Haut Comité Juridique
de la Place financière de Paris

RAPPORT SUR LES IMPACTS JURIDIQUES ET REGLEMENTAIRES DE L'INTELLIGENCE ARTIFICIELLE EN MATIÈRE BANCAIRE, FINANCIÈRE ET DES ASSURANCES

du Haut Comité Juridique
de la Place Financière de Paris

20 juin 2025

9 rue de Valois 75001 Paris - Tél.: 33 (0)1 42 92 20 00 - hautcomite@hcjp.fr - www.hcjp.fr

TABLE DES MATIÈRES

INTRODUCTION / RÉSUMÉ

L'intelligence artificielle (l'**IA**) n'est pas une innovation récente. Elle remonte aux origines mêmes de l'informatique – il y a plus de 70 ans – lorsque le mathématicien britannique Alan Turing se demandait dans un article publié en 1950[1] si les machines pouvaient penser (« *Can machines think ?* ») et à la conférence de Dartmouth en 1956 qui a réuni une vingtaine de chercheurs pour poser les bases de l'IA comme une discipline scientifique, sous l'impulsion de John McCarthy[2].

L'IA a connu une croissance exponentielle ces dernières années grâce au développement de la *big data* et à sa démocratisation auprès du grand public, notamment avec l'émergence des systèmes d'IA générative à partir de 2022. Les développements de l'IA devraient se poursuivre et tendre à représenter un marché de plusieurs centaines de milliards de dollars et d'un demi-milliard d'utilisateurs à l'horizon 2027[3]. L'Union européenne ambitionne de devenir le continent leader en matière d'IA[4] et a annoncé un plan de 200 milliards d'euros investissement via l'initiative « *InvestAI* » dans cette perspective[5].

L'IA touche tous les secteurs, y compris le secteur bancaire et financier. Elle apparaît comme « *le principal moteur de croissance de la transformation numérique* »[6] pour les entreprises de cette industrie, telles que les établissements de crédit, les entreprises d'investissement, les entreprises d'assurance, les établissements de paiement, les établissements de monnaie électronique et les sociétés de gestion (les **Institutions Financières**).

Le recours à l'IA par les Institutions Financières a conduit les autorités de supervision françaises à solliciter le Haut Comité Juridique de la Place Financière de Paris (le HCJP) pour étudier les impacts juridiques et réglementaires de l'IA en matière bancaire, financière et assurantielle en constituant un groupe de travail rassemblant des experts métiers, des représentants des autorités, des professeurs de droit et des avocats fin 2023 (le **groupe de travail**)[7].

---

[1] *A. M. Turing, Computing Machinery and Intelligence, Mind, 49, 1950, p.433-460.*

[2] *J. Henno, 1956 : et l'intelligence artificielle devint une science, Les Echos, 21 août 2017.*

[3] *BPI France, Marché de l'intelligence artificielle : où en sommes-nous ?, 4 juin 2024 (https://bigmedia.bpifrance.fr/nos-actualites/marche-de-lintelligence-artificielle-ou-en-sommes-nous) ; BPI France, Les chiffres 2023-2024 du marché de l'IA dans le monde, 23 juin 2024 (https://lehub.bpifrance.fr/les-chiffres-2023-2024-du-marche-de-lia-dans-le-monde/).*

[4] *Commission européenne, Communication from the commission to the European parliament, the council, the European economic and social committee and the committee of the regions – AI Continent Action Plan, 9 avril 2025, p. 1: « The European Union is committed and determined to become a global leader in Artificial Intelligence, a leading AI continent. »*

[5] *Ursula von der Leyen, Présidente de la Commission européenne, Speech by President von der Leyen at the Artificial Intelligence Action Summit, 11 février 2025.*

[6] *Denis Beau, Premier sous-gouverneur de la Banque de France, L'intelligence artificielle : bénédiction ou malédiction pour la transformation du secteur financier ?, Discours, Singapour, 8 novembre 2024.*

[7] *Cf. annexe 1 – Participants au groupe de travail.*

La mission confiée au groupe de travail exclut du champ de l'analyse l'usage de l'IA à des fins de supervision et de contrôle des Institutions Financières, notamment en matière de lutte contre le blanchiment et le financement du terrorisme ou encore les enjeux de responsabilité disciplinaire pour les Institutions Financières quant à l'IA. Elle écarte également du champ de son analyse les enjeux d'assurabilité des risques en matière d'IA.

À l'issue d'une année de travaux, le groupe de travail a élaboré le présent rapport (le **Rapport**).

Il a été rapidement constaté que les Institutions Financières recourent à l'IA depuis plusieurs années pour des cas d'usage variés. La technologie offre de plus en plus de possibilités, créant de nouvelles opportunités. Le groupe de travail a ainsi observé que l'IA est devenue un outil incontournable pour la fourniture de services réglementés dans ce secteur (e.g. le *credit scoring*, les *robo-advisers*, les *chatbots*, etc.)[8]. Cette évolution a établi une dichotomie naturelle entre les « *IA assistant* », qui assistent les humains dans leurs tâches et les « *IA exécutant* », qui disposent d'un degré d'autonomie plus élevé. Cette transformation numérique, alimentée par l'IA, promet de redéfinir les pratiques traditionnelles et d'ouvrir de nouvelles perspectives pour l'industrie financière.

Mais face à la multiplication des cas d'usage de l'IA par les Institutions Financières, le groupe de travail s'est interrogé sur le cadre réglementaire existant de l'IA dans le secteur financier, notamment en analysant la réglementation sectorielle applicable. L'association Paris Europlace dans sa réponse[9] à la consultation lancée par la Commission européenne sur l'IA dans le secteur financier[10] a pu déjà porter le message de l'existence d'une réglementation sectorielle qui couvre déjà – au moins pour partie – la technologie de l'IA[11].

Le groupe de travail s'est alors penché sur la manière dont la règlementation sectorielle existante et encadrant les Institutions Financières pouvait prendre en compte les nouveaux risques générés par l'IA (e.g. biais algorithmiques, hallucinations etc.) et a examiné les questions de gouvernance pour chaque type d'Institution Financière et le cadre de contrôle pouvant être défini.

---

[8] *International Organisation of Securities Commission (IOSCO), Artificial Intelligence in Capital Markets: Use Cases, Risks, and Challenges, mars 2025.*

[9] *Paris Europlace, Target consultation on AI in the financial sector, Paris Europlace AI Working Group response, 13 septembre 2024.*

[10] *Commission européenne, Consultation document – Target consultation on artificial intelligence in the financial sector, 18 juin 2024.*

[11] *Paris Europlace, op. cit. n° 9, « In itself, AI is not new, having indeed quite a long history in the financial services industry (for credit risk scoring, high-frequency trading, and robo-advice) and being already subject to existing risk frameworks. Specifically, AI applications in finance are already subject to regulation through sectoral or cross-sectoral specific rules, such as consumer data privacy regulation, consumer protection regulation in lending operations, or prudential requirements concerning data governance, cyber risk, third-party risk, information systems outsourcing, or operational risk. We thus consider that the financial industry is already more heavily regulated than other sectors. We stand for that reason against an additional, sectoral regulation », p. 1.*

Certains sujets traités par les réglementations spécifiques aux Institutions Financières tels que la protection de la clientèle, la protection des données clients (notamment le secret professionnel), les exigences prudentielles ou encore la relation avec les prestataires tiers, en particulier en cas d'externalisation, définissent d'ores et déjà un régime réglementaire permettant d'appréhender l'usage de l'IA.

L'analyse du cadre réglementaire de l'IA pour les Institutions Financières a bien entendu tenu compte de la toute nouvelle réglementation sur l'IA produite par l'Union européenne avec le règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle (le **RIA**).

Le RIA constitue un cadre juridique novateur qui régit la conception, le développement, le déploiement et l'utilisation des systèmes d'IA, afin de garantir leur bonne utilisation tout en minimisant les risques pour le bien-être humain et la société. Encore faut-il pouvoir identifier quels outils d'IA sont concernés. La délimitation entre IA et simple système logiciel est difficile en raison de la complexité des IA et de l'évolution technique continue. La Commission l'admet elle-même : il n'est pas possible de déterminer automatiquement ou d'établir une liste exhaustive des systèmes qui entrent ou non dans la définition d'un système d'IA[12].

Pour rédiger le Rapport, le HCJP s'est fondé sur la définition européenne de l'IA, elle-même tirée de la définition de l'OCDE[13]. Selon l'article 3.1 du RIA, un « *système d'IA* » (**Système d'IA** ou **SIA**) est un système automatisé, conçu pour générer des sorties, à partir des entrées qu'il reçoit, tels que des recommandations, des prédictions ou des décisions influençant son environnement.

Ces systèmes incluent ainsi le raisonnement logique, l'analyse prédictive, les techniques de *machine learning* et son sous-ensemble le *deep learning*. Les technologies de *natural language processing* (NLP), permettant aux algorithmes de traiter des données encodées en langage humain, sont également comprises comme des SIA. Aux côtés des IA génératives co-existent les IA déterministes. Ces dernières sont souvent qualifiées de « *basiques* » car elles suivent des règles prédéfinies pour traiter des tâches répétitives[14]. Techniquement moins avancée que l'IA générative, l'IA déterministe est surtout utilisée pour l'automatisation de tâches administratives ou des analyses de données simples. Ces IA sont toutefois suffisamment poussées pour ne pas être considérées comme la simple automatisation d'un procédé habituellement exécuté par un humain.

---

[12] Commission européenne, Guidelines on the definition of an artificial intelligence system established by Regulation (EU) 2024/1689 (AI Act), lignes directrices, 6 février 2025, paragraphe 62.

[13] OCDE, Recommendation of the Council on Artificial Intelligence, adoptée le 22 mai 2019, modifiée le 3 mai 2024.

*[14] Association Française de la Gestion d'Actifs (**AFG**), Guide Professionnel Principes et bonnes pratiques pour une utilisation responsable de l'IA par les sociétés de gestion, janvier 2025, p. 7.*

La Commission européenne exclut néanmoins les méthodes de régression linéaire, logistique[15] ou heuristique classique[16] en ce que ces dernières ne se distinguent pas des traitements de données basiques.

Les simples modèles de prédiction ne seront pas non plus soumis au RIA[17]. Cela inclut les systèmes utilisant les règles d'apprentissage statistique de base à l'image des modèles de prévisions financières, y compris ceux prédisant les cours futurs des actions. Ces outils sont cités à titre d'exemple par la Commission et ne sauraient constituer une liste exhaustive compte tenu de la rapidité des évolutions technologiques. En tout état de cause, la frontière entre les outils d'IA et les simples systèmes logiciels est ténue mais lourde de conséquences. Ainsi, les Institutions Financières ne pourront pas s'épargner un exercice de définition poussé afin de savoir si leur outil relève du champ d'application du RIA ou non (cf. paragraphe A).

Enfin, une précision sémantique s'avère nécessaire : le RIA régule les Systèmes d'IA dans leur ensemble. Ces derniers sont constitués d'un « *modèle d'IA* », le composant essentiel, augmenté d'autres composants tel qu'une interface utilisateur, pour former un Système d'IA. Ainsi, le modèle IA fait partie du Système d'IA. Cette segmentation, même si parfois délicate en pratique, est essentielle car elle permettra aux Institutions Financières de mieux identifier les obligations réglementaires applicables selon le type de système utilisé.

Outre l'intérêt d'une définition précise des Systèmes d'IA pour l'élaboration de ce Rapport, le RIA adopte une approche fondée sur les risques, déjà familière aux les Institutions Financières et qui impactera les nouvelles obligations liées à cette technologie pour les acteurs.

Les Institutions Financières se trouvent ainsi confrontées à deux ensembles de règles distincts : les règles transversales issues du RIA et celles issues de la réglementation sectorielle. Une question d'articulation entre ces deux ensembles de règles se pose, car des interactions entre ces deux régimes réglementaires sont perceptibles à plusieurs niveaux. Il convient de souligner toutefois que les législateurs ont suivi une approche générale de complémentarité entre ces deux ensembles de

[15] Il est communément admis que les méthodes de régression linéaire et régression logistique sont des techniques de machine learning qui calculent des prédictions à partir de données précédentes. Par exemple, en examinant les tendances d'achat passées des clients, l'analyse de régression estime les ventes futures.

[16] Une heuristique est une méthode de calcul qui utilise une approche basée sur des règles, la reconnaissance de formes ou des stratégies d'essais et d'erreurs plutôt que l'apprentissage basé sur les données. Cette méthode manque ainsi d'adaptabilité par rapport aux IA qui apprennent par l'expérience. (Voir Commission européenne, Guidelines on the definition of an artificial intelligence system established by Regulation (EU) 2024/1689 (AI Act), Lignes directrices, 6 février 2025, paraghraphe 48).

[17] Ibid, p. 8.

règles, comme l'a rappelé la Commission européenne dans sa consultation[18] et que des ponts ont été établis entre ces deux corps de normes.

Le Rapport a ainsi pour objectif de présenter et proposer une méthodologie pour appréhender ces questions d'articulation entre le RIA et la réglementation sectorielle des Institutions Financières. Il aborde également les sujets d'application pouvant se poser avec d'autres ensembles de textes, tels que ceux relatifs aux données (notamment DORA et RGPD), à la protection de l'environnement et la propriété intellectuelle et fournit des clés de lecture concernant les normes en matière de protection environnementale et les dispositifs de protection de la propriété intellectuelle.

Enfin, l'IA ne saurait être appréhendée dans un tel Rapport sans une attention particulière aux enjeux de responsabilité pour les Institutions Financières, même si le projet de directive sur la responsabilité a été retiré des priorités actuelles de l'Union européenne.

Le Rapport examinera donc l'encadrement existant de l'IA par les réglementations sectorielles (I). Les contours, notamment les champs d'application matériel et territorial du RIA et la classification par les risques, propre au RIA, seront exposés à l'aune des usages de l'IA par les Institutions Financières. Les différents statuts des opérateurs de SIA – fournisseur, déployeur, importateur et distributeur – seront également abordés parallèlement à leurs obligations spéciales (II). Le groupe de travail entend apporter des éléments de réponse et de réflexion sur l'articulation entre le RIA et les réglementations sectorielles ou transversales régissant les Institutions Financières (III) et aborder enfin les enjeux de responsabilité afférents aux Institutions Financières dans leurs rapports avec l'IA (IV).

[18] *Commission européenne, op. cit. n° 10, « The AI Act is designed to complement the already existing financial services acquis, that, while not explicitly targeted at regulating AI, is an important framework to manage the related risks in specific applications and includes several relevant requirements for financial entities when providing financial services. ».*

I. L'encadrement existant de l'IA par les réglementations sectorielles

La réglementation des Institutions Financières est technologiquement neutre. Elle appréhende toutes les formes de technologies sans élaborer des contraintes spécifiques à tout ou partie d'entre elles. Pour autant, l'usage de l'IA comme toute technologie utilisée pour la fourniture de prestations de services financiers engendre de nouveaux risques qu'il faut savoir cartographier et encadrer.

En sus des organismes internationaux[19], les superviseurs nationaux et européens des Institutions Financières ont d'ores et déjà milité pour encadrer l'usage qui est fait de l'IA par les Institutions Financières[20]. Cet encadrement devrait pouvoir prendre appui sur la réglementation existante, qui prévoit déjà un corpus de règles sectorielles fourni, applicables dans une large mesure en cas d'usage de l'IA et de Systèmes d'IA par les Institutions Financières, notamment en matière de gouvernance, de gestion des risques, d'externalisation ou de protection des données clients.

A. L'IA apparaît comme un outil pour la prestation de services financiers réglementés

Les Institutions Financières sont libres en principe de recourir à l'IA dans le cadre de la fourniture de services réglementés à leurs clients, que cela soit des services bancaires, de paiement, d'investissement ou d'assurance.

Chaque industrie recourt à l'IA comme une assistance dans l'exécution de prestations réglementées, comme un outil d'exécution, doté d'une certaine autonomie, de certaines prestations ou encore comme un instrument d'appréciation, de gestion et/ou de contrôle des risques induits. Les cas d'usage de l'IA par les Institutions Financières se multiplient d'ailleurs depuis plusieurs années, l'IA comme outil d'exécution autonome de prestations réglementées demeurant pour l'instant l'usage le moins développé.

---

[19] Cf. notamment le rapport du « Financial Stability Board » (FSB) dénommé « Financial Stability Implications of Artificial Intelligence », en date de novembre 2024 ; à la suite d'un premier rapport en 2021, « International Organisation of Securities Commission » (IOSCO) a publié en mars 2025 un nouveau rapport relatif à l'usage de l'IA dans les marchés de capitaux décrivant les cas d'usage, les risques et les enjeux associés (le Rapport IOSCO), soumis à consultation jusqu'au 11 avril 2025.

[20] ACPR, Le développement des big techs dans le secteur financier: quels risques, quelles réponses réglementaires ?, Dossier, octobre 2024 ; ACPR, Intelligence artificielle : quel impact à l'ACPR ?, Revue de l'ACPR, juillet 2024; ACPR, La transformation numérique dans le secteur français de l'assurance, Analyses et synthèses n° 132, 14 janvier 2022 ; ACPR, Gouvernance des algorithmes d'intelligence artificielle dans le secteur financier, Document de réflexion, juin 2020 ; EIOPA, Factsheet on the regulatory framework applicable to AI systems in the insurance sector, Facthseet, 15 juillet 2024 ; EIOPA, Artificial intelligence governance principles : towards ethical and trustworthy artificial intelligence in the European insurance sector, 17 juin 2021 ; EIOPA, Consultation Paper on Opinion on Artificial Intelligence Governance and Risk Management, 10 février 2025 ; Commission européenne, Livre blanc – Intelligence artificielle : une approche axée sur l'excellence et la confiance, 19 février 2020 ; ESMA, Public statement – on the use of Artificial Intelligence in the provision of retail investment services, 30 mai 2024, ESMA35-335435667-5924.

1. L'IA assistant

Une fonction importante de l'IA est d'assister les personnes physiques en automatisant des tâches complexes, en analysant rapidement de larges quantités de données ou encore en proposant des suggestions ou des solutions issues de ces analyses. Les Institutions Financières gagnent à y avoir recours.

Dans le domaine bancaire, l'IA peut notamment jouer ce rôle en permettant d'identifier un marché cible sur la base des données disponibles concernant les clients potentiels (*mapping*), de répondre à des questions simples de clients, d'assister dans l'appréciation du risque de crédit (*credit scoring*) d'un emprunteur potentiel ou l'analyse documentaire requise lors de l'ouverture du compte (*i.e.* analyse *know-your-customer*) ou encore, d'optimiser les flux de transactions et de détecter les usages frauduleux des moyens de paiement.

L'IA peut aussi avoir un véritable rôle d'assistant en matière de prestations de services d'investissement. L'IA fait d'ailleurs déjà partie des outils des entreprises d'investissement. Des outils basés sur l'IA ont en effet été développés pour fournir, par exemple, des conseils financiers.

En matière de prestation de services d'investissement, l'IA joue notamment ce rôle à l'aide des *robo-advisers*, qui automatisent la gestion des portefeuilles d'investissement (sous la forme de gestion conseillée et/ou de gestion discrétionnaire sous mandat). Ces systèmes reposent sur des algorithmes, et utilisent des techniques de *machine learning*, permettant de personnaliser les stratégies d'investissement en fonction des objectifs et du profil de risque des clients[21]. Grâce à cette personnalisation, les *robo-advisers* peuvent fournir des services d'investissement adaptés aux besoins individuels des clients, tout en facilitant, voire démocratisant, l'accès à des conseils financiers et/ou stratégies potentiellement sophistiqués. Cette personnalisation se manifeste également dans les critères que les investisseurs peuvent définir en amont de tout investissement. Dans un contexte où les critères ESG (critères Environnementaux, Sociaux et de Gouvernance) revêtent une importance croissante, ce degré de personnalisation répond à un besoin. L'IA peut ainsi être proposée par les entreprises d'investissement comme un outil au bénéfice des investisseurs, afin de mieux aligner leurs décisions d'investissement sur leurs convictions. On rappellera que seuls les prestataires de services d'investissement peuvent utiliser l'IA ou des Systèmes d'IA qui participent de manière essentielle à la fourniture de services d'investissement. Le simple usage de l'IA ne permet pas de se soustraire à l'application des règles encadrant l'exercice de ce type de services (y compris en matière d'agrément), si l'IA devient l'instrumentum de tels services.

[21] *Rapport IOSCO, op. cit., p. 26.*

De façon similaire, l'usage de l'IA dans le cadre d'activités de gestion collective impliquant la gestion de fonds d'investissement par des sociétés de gestion croît progressivement, faisant ainsi évoluer les processus d'investissement mis en œuvre par les gestionnaires, comme le souligne l'ESMA dans le cadre d'une analyse relative aux tendances, risques et vulnérabilités inhérents au recours à l'IA dans le domaine de la gestion de fonds[22]. Si l'usage de l'IA n'y est pas encore perçu comme se substituant au rôle décisif des gérants dans le cadre de nombre de stratégies d'investissement, son utilisation dans le processus décisionnel mis en œuvre par ces sociétés de gestion n'en demeure pas moins croissante, l'IA étant ainsi perçue par les gestionnaires comme un moyen d'améliorer leur efficacité opérationnelle en facilitant leurs prises de décision.

Par ailleurs, aussi bien dans le domaine bancaire, financier, assurantiel que celui des services de paiements, les *chatbots* et assistants virtuels alimentés par l'IA aident les investisseurs ou les clients, selon le cas, à accéder rapidement à des informations sur leurs comptes, à poser des questions sur le fonctionnement de leur contrat et à recevoir des orientations initiales. Ces outils optimisent également les processus de réclamation, alors même que les Institutions Financières rapportent que les équipes dédiées peuvent recevoir plusieurs milliers de sollicitations par semaine. Celles-ci s'en trouvent ainsi libérées, ce qui leur permet de se concentrer sur les dossiers nécessitant une attention particulière ou présentant un degré de complexité supérieur. Reste à démontrer que l'efficacité et l'interaction client s'en trouvent ainsi améliorées[23], tout cela avec un coût réduit pour le prestataire, avec notamment l'application des règles en matière de traitement des réclamations (le champ d'application de ces dernières n'étant pas exclu par le seul recours à une technologie d'IA).

Dans une vision prospective, on peut anticiper qu'au stade de la souscription de produits financiers, l'utilisation de *chatbots* pour répondre aux questions des souscripteurs potentiels permettrait de les orienter vers des produits correspondant à leurs besoins. Dans différents domaines tels que celui des assurances et/ou des services financiers, il conviendrait alors que leur utilisation s'inscrive pleinement dans le cadre réglementaire existant du devoir d'information et de conseil.

En assurance-vie, l'utilisation de l'IA permet de procéder à l'analyse en nombre des clauses bénéficiaires, afin d'identifier, en cours de contrat, celles qui manquent de clarté dans leur rédaction ou ne sont plus à jour afin de solliciter les souscripteurs et les inviter à procéder à une vérification puis une modification de la clause, facilitant ainsi l'identification des bénéficiaires. Elle permet également, lors du dénouement du contrat, en cas de décès de l'assuré, de procéder à l'analyse de documents en masse, notamment ceux disponibles en *open source*, afin de faciliter la recherche des bénéficiaires et d'améliorer ainsi la lutte contre les contrats en déshérence.

---

[22] ESMA TRV Risk Analysis, Artificial intelligence in EU investment funds: adoption, strategies and portfolio exposures, ESMA50-43599798-9923, 25 février 2025.

[23] ESMA, TRV Risk Monitor n° 2, 2023, p. 36: « One area of concern is the transparency and quality of consumer interactions if generative AI is deployed in tools such as virtual assistants and robo-advisers ».

2. L'IA exécutant

Aujourd'hui, l'IA ne se limite plus à son rôle traditionnel d'assistant. Elle devient désormais un véritable exécutant, capable de prendre des décisions et de les mettre en œuvre de manière autonome.

Par exemple, le *trading* algorithmique repose sur l'utilisation d'algorithmes qui passent automatiquement des ordres d'achat ou de vente en fonction de paramètres prédéfinis et de signaux de marché. Le *trading* à haute fréquence, un sous-ensemble du *trading* algorithmique, exécute des transactions à une vitesse extrêmement rapide, souvent en l'espace de millisecondes, voire de nanosecondes. L'IA peut permettre d'améliorer la capacité à anticiper les mouvements de marché, voire à tirer parti des fluctuations de prix, le cas échéant en fournissant une liquidité au marché.

De manière similaire, le recours aux *robo-advisers* – tant pour une activité de conseil en investissement que de gestion sous mandat – permettrait une automatisation significative voire complète d'activités de conseil et/ou de gestion des portefeuilles d'investissement, les arbitrages et le cas échéant l'exécution des transactions reposant sur l'utilisation d'algorithmes combinée à une analyse automatique des données par le Système d'IA, sans intervention de l'équipe de gestion ou d'un conseiller en investissement.

Les Systèmes d'IA pourraient aussi permettre une amélioration de la relation client au stade de la gestion des contrats, notamment d'assurance. On pense tout d'abord à la simplification de la gestion des réclamations, via une résolution automatisée et quasi autonome d'une grande partie des réclamations reçues des clients. On pense également à l'accélération de la gestion des sinistres, que ce soit au stade de leur déclaration, via l'analyse des pièces justificatives transmises, de leur évaluation, en évitant par exemple le déplacement d'experts grâce à l'utilisation de la reconnaissance d'images (notamment en assurance auto ou habitation) ou encore de leur indemnisation, en réduisant les délais de versement des indemnités d'assurance (notamment dans le cas de l'assurance paramétrique), limitant de plus en plus l'intervention humaine.

3. L'IA instrument d'amélioration de l'appréhension des risques

L'IA peut aussi être utilisée par les établissements de crédit, prestataires de services d'investissement, établissements de paiement et établissements de monnaie électronique aux fins de satisfaire aux exigences réglementaires qui s'appliquent à eux. L'IA peut par exemple être utilisée dans le cadre des calculs de fonds propres pour optimiser l'identification et la gestion des risques auxquels les établissements sont exposés (risques informatiques, opérationnels, de fraude, etc.).

La réglementation bancaire, en ce compris prudentielle, ayant été rédigée de façon neutre technologiquement afin de s'adapter aux évolutions techniques et technologiques du secteur bancaire, encourage dans une certaine mesure et sous certaines conditions, l'usage de l'IA par les établissements assujettis aux fins du calcul de leurs exigences de fonds propres. Comme le relève l'Autorité de contrôle prudentiel et de résolution (**ACPR**), un certain nombre d'établissements de crédit utilise déjà l'IA pour la conception des modèles internes d'évaluation de risque de crédit

qu'ils utilisent dans le cadre du calcul de leurs exigences de fonds propres[24]. En outre, le recours à l'IA peut permettre de prendre en compte, de manière plus rapide, pertinente et granulaire, certains risques opérationnels, de liquidité et de concentration.

L'IA peut aussi, dès aujourd'hui, jouer un rôle dans la conformité, la gestion des risques et l'efficacité opérationnelle au sein des Institutions Financières. Les Systèmes d'IA peuvent, le cas échéant, surveiller et analyser certaines réglementations financières, détecter les comportements non conformes (ou potentiellement violant certaines réglementations) et évaluer les risques associés aux différentes options d'investissement. L'IA peut aussi détecter des schémas inhabituels dans les données transactionnelles et les communications, contribuant ainsi à prévenir les fraudes. Eu égard à la masse des données et à la rapidité d'exécution d'ordres de bourse, l'IA peut s'avérer être un outil permettant d'analyser les données et de détecter des comportements irréguliers ou situations douteuses par rapport à la réglementation.

L'automatisation de tâches répétitives telles, par exemple, la saisie de données et la génération de rapports, sont aujourd'hui possibles grâce à l'IA ; ceci devrait pouvoir améliorer l'efficacité opérationnelle, tout en réduisant les erreurs dues à l'intervention humaine et, réciproquement, pouvoir permettre aux salariés de se concentrer sur des missions à plus forte valeur ajoutée.

Dans le domaine de l'assurance, la quantité croissante de données à la disposition des assureurs leur permet d'appréhender avec beaucoup plus de justesse les risques et, en conséquence, d'ajuster la tarification des produits de manière plus précise. Selon l'ACPR, « *les technologies de Big Data associées à l'IA permettent d'augmenter la finesse et le champ d'appréciation des risques et d'en améliorer la modélisation et la maîtrise* »[25]. Par exemple, l'IA permet désormais une identification des zones à risques de façon automatique et évolutive, via l'analyse en temps réel des données météorologiques. Les Systèmes d'IA contribuent également à lutter plus efficacement contre la fraude à l'assurance, elle-même de plus en plus sophistiquée en raison de l'utilisation croissante de l'IA par les fraudeurs.

B. Les nouveaux risques liés à l'usage de l'IA

L'introduction de l'IA dans les services financiers entraîne l'apparition d'une série de risques[26] que les Institutions Financières doivent appréhender.

---

[24] *Henri Fraisse et Christophe Hurlin, Modèles internes des banques pour le calcul du capital réglementaire (IRB) et intelligence artificielle, ACPR, Débats économiques et financiers n° 44, mars 2024.*

[25] *ACPR, Transformation numérique dans le secteur français de l'assurance, Analyses et Synthèses n° 132, 14 janvier 2022.*

[26] *Voir aussi ESMA, Public Statement on the use of Artificial Intelligence (AI) in the provision of retail investment services, 30 mai 2024, ESMA35-335435667-5924, spéc. n° 5 et s.*

Tout d'abord, l'automatisation des processus participant de la prestation des services financiers par l'IA expose les Institutions Financières à des risques opérationnels accrus. La réduction progressive de l'intervention humaine dans certaines tâches essentielles peut entraîner des défaillances techniques, des erreurs algorithmiques, voire des cyberattaques, mettant éventuellement en péril la continuité des activités des Institutions Financières et interrogeant sur la place de l'intervention humaine dans les opérations impliquant l'usage de l'IA.

Par ailleurs, si l'IA promet des gains d'efficacité pour les Institutions Financières, elle présente aussi des risques pour la stabilité des marchés financiers. En effet, l'IA pourrait exacerber la volatilité des marchés, notamment en amplifiant des mouvements déjà existants, ce qui pourrait créer des déséquilibres de liquidité, voire une mauvaise interprétation de certains signaux de marché entraînant une réponse excessive à certaines tendances ou encore une réponse, par une Institution Financière, à ses propres signaux de marché.

Un autre risque réside dans les éventuels biais algorithmiques susceptibles de survenir, avec pour conséquence un risque de discrimination. Les Systèmes d'IA peuvent en effet générer des biais suivant la qualité et la fiabilité des données sur lesquelles ils sont entraînés. Un modèle basé sur des données biaisées reproduira, voire accentuera, ces biais. Ces biais peuvent en outre subsister, même avec des données de qualité, en raison d'approximations ou de corrélations propres aux ensembles de données historiques. Les critères du genre, l'âge ou l'origine ethnique posent évidemment question.

Au-delà des biais algorithmiques, il existe un risque, dans la mesure où les Systèmes d'IA se fondent sur une multitude de données, qu'il devienne impossible d'expliquer quelles données ont permis d'apporter l'information recherchée ou de prendre la décision concernée (problématique de l'explicabilité limitée de certains Systèmes d'IA, également connue sous le nom de « *black box* » ou boîte noire).

En outre, la surreprésentation d'un nombre restreint de prestataires technologiques fournissant des solutions d'IA est de nature à poser des problèmes de concentration et de dépendance pouvant avoir des conséquences systémiques[26bis]. Le manque de concurrence entre ces fournisseurs[27], dû notamment aux coûts élevés du développement des modèles d'IA, accentue ce risque. Cette concentration pourrait non seulement rendre les Institutions Financières utilisatrices vulnérables en cas de défaillance, mais aussi entraîner une homogénéité des données et des modèles,

[26bis] *ESMA, Institut Louis Bachelier, The Alan Turing Institute, Leveraging Large Language Models in Finance: Pathways to Responsible Adoption, Working papers, 2025, p. 28.*

[27] *Sur les risques concurrentiels à l'amont de la chaîne de valeur, voir Autorité de la concurrence, Intelligence artificielle générative : l'Autorité rend son avis sur le fonctionnement concurrentiel du secteur de l'intelligence artificielle générative, 28 juin 2024.*

limitant la diversité des sources d'apprentissage et amplifiant les biais. L'émergence de prestataires d'IA et les potentiels phénomènes de consolidation qui pourraient apparaître autour de ces acteurs afin de leur permettre de disposer d'une taille critique nécessaire à leur viabilité économique pose également la question des enjeux découlant de leurs éventuelles défaillances ou faillites et des conséquences que de tels évènements pourraient avoir sur les activités des Institutions Financières. Au-delà, une telle concentration entraînerait un risque non-négligeable en termes de cybersécurité et pourrait par ailleurs entraîner des problématiques de souveraineté, les fournisseurs majeurs de Systèmes d'IA n'étant pas toujours européens.

De surcroît, la fiabilité des résultats générés par l'IA est une autre source de préoccupation. Certains modèles d'IA peuvent produire des erreurs, communément appelées « *hallucinations* », c'est-à-dire fournir des informations fausses, mais cohérentes, ce qui peut nuire à la fiabilité des résultats. Des conséquences graves sur les décisions de souscription de produits financiers peuvent en résulter si elles ne sont pas corrigées à temps.

Le risque d'utilisation de données sensibles et protégées des clients est également un défi important lié à l'IA. Le secret bancaire ou plus généralement le secret professionnel auquel sont astreintes les Institutions Financières encadre très strictement l'usage des données des clients[28].

Le traitement automatisé de vastes quantités de données, notamment via des algorithmes externes ou des plateformes de cloud, expose les entreprises à des risques accrus de fuites de données. L'externalisation et la sous-traitance peuvent également engendrer un risque accru pour les acteurs financiers. Néanmoins, la règlementation sur la résilience opérationnelle numérique du secteur financier n° 2022-2554 du 14 décembre 2022 (**DORA**) permet de réduire ces risques en intégrant des obligations de sécurité liées aux prestataires. Ces risques soulèvent également des questions de conformité avec les règles strictes imposées par le Règlement Général de Protection des Données n° 2016-69 en date du 27 avril 2016 (**RGPD**).

Enfin, la confiance excessive dans les algorithmes, sans supervision humaine adéquate, peut entraîner des décisions imprévisibles ou inadaptées, en particulier dans des contextes de marché volatile. Maintenir une supervision humaine suffisante pour corriger les erreurs éventuelles et s'assurer que l'utilisation de l'IA ne remplace pas entièrement le jugement humain, notamment dans des situations imprévues où les algorithmes pourraient échouer à prédire des résultats adéquats, s'avère être une nécessité[29].

---

[28] *Cf. article L. 511-33 du Code monétaire et financier (**CMF**) pour les établissements de crédit, Article L. 522-19 du CMF pour les établissements de paiement, article L. 531-12 du CMF pour les entreprises d'investissement et les sociétés de gestion de portefeuille.*

[29] *Cf. ce facteur de risque souligné par l'ESMA dans Public statement – on the use of Artificial Intelligence in the provision of retail investment services, 30 mai 2024, ESMA35-335435667-5924.*

D'une manière générale, le recours accru à des leviers technologiques par les Institutions Financières, quel que soit le procédé automatisé utilisé (et que celui-ci repose ou non sur des technologies liées à l'IA), peut certes avoir pour effet de réduire les risques relatifs au facteur humain mais également, corrélativement, d'accroître les risques opérationnels résultant de l'utilisation de tels procédés technologiques : anomalies, piratages informatiques, mauvaises configurations etc. Un Système d'IA mal calibré ou insuffisamment entrainé peut ainsi dégrader la qualité des services proposés par une Institution Financière, influencer négativement ses processus décisionnels, et exposer l'établissement à des risques juridiques et réputationnels[29bis]. Il semblerait donc requis pour les Institutions Financières de mettre en balance les risques associés aux facteurs humains avec ceux découlant d'une solution basée sur l'IA. Par cette approche par les risques, elles pourraient ainsi déterminer si, à quel moment, et dans quelle mesure, une intervention humaine est plus appropriée qu'une intervention algorithmique.

C. Une gouvernance propre aux usages de l'IA s'impose

La mise en place d'un cadre de gouvernance pour l'exploitation et la conception de l'IA par les Institutions Financière est essentielle. Ce cadre doit inclure les parties prenantes via une comitologie appropriée pour notamment comprendre les relations avec les fournisseurs d'IA, gérer l'exploitation, la propriété et le traitement des données d'entrée de sortie du système et, *a fortiori*, établir un cadre de contrôle rigoureux sans oublier des programmes de formation continue mis en place[30] pour s'adapter aux évolutions de l'IA.

Des grands principes de gouvernance s'articulant autour de la transparence, de la responsabilité, du maintien de l'intervention humaine ou encore de la protection des données ont été relevés par les superviseurs internationaux[31].

1. La gouvernance de l'IA requise pour les établissements de crédit

L'utilisation de l'IA ne doit pas conduire les établissements de crédit à se dégager de leurs responsabilités au seul motif qu'ils ont eu recours à un algorithme.

Le recours à l'IA doit donc s'intégrer notamment dans l'organisation et le contrôle interne des établissements de crédit tel que prévu par, notamment, les articles L. 511-55 et s. du CMF et l'arrêté du 3 novembre 2014 relatif au contrôle interne des entreprises du secteur de la banque, des services de paiement et des services d'investissement soumises au contrôle de l'ACPR (l'Arrêté du **3 novembre 2014**), ayant vocation à transposer les articles 74 et s. de la Directive 2013/36/UE du 26 juin 2013 concernant l'accès à l'activité des établissements de crédit et la surveillance prudentielle des établissements de crédit (**CRD**).

[29bis] *ESMA, Institut Louis Bachelier, The Alan Turing Institute, Leveraging Large Language Models in Finance: Pathways to Responsible Adoption, Working papers, 2025, p. 12.*

[30] *Article 4 du RIA.*

[31] *Rapport IOSCO, op. cit., p. 49.*

Ces exigences relatives à l'élaboration d'une gouvernance portant sur la détection, maîtrise, gestion et surveillance des risques se trouvent incluses dans l'évaluation d'un établissement de crédit au stade d'une demande d'agrément et dans le cadre de sa supervision continue par les autorités. Le déploiement de solutions IA nécessite une gouvernance appropriée, reposant notamment sur une maîtrise et un suivi spécifique des risques induits engendrés par cette technologie, auprès du responsable de la gestion des risques de l'établissement.

L'article 215 de l'Arrêté du 3 novembre 2014 impose la validation d'un dispositif de gestion de la continuité d'activités, en ce compris en matière informatique, par l'organe de surveillance de l'établissement de crédit. Les établissements de crédit devront inclure dans leurs politiques, procédures et contrôles de surveillance et de maîtrise des risques, y compris informatique, le recours à l'IA. Cela pourrait par exemple impliquer de recruter des personnes compétentes pour mener ces contrôles et le cas échéant mettre en œuvre les mesures correctrices nécessaires telles que la vérification du bon fonctionnement de l'algorithme, de la cohérence des résultats qu'il fournit, de la qualité et de la pertinence des données utilisées. Il faudra notamment que les établissements de crédit déterminent la fréquence et l'étendue des contrôles des algorithmes selon la sensibilité du cas d'usage concerné. Par exemple, le recours à l'IA pour répondre à des questions des clients devrait être en mesure d'identifier une « *réclamation* » et d'y apporter le traitement correspondant : renvoi vers un conseiller ou application des règles prévues en la matière (délai de traitement de la demande, etc. conformément à la Recommandation 2022-R-01 du 9 mai 2022 sur le traitement des réclamations émise par l'ACPR).

L'intégration de l'IA dans le cadre du contrôle interne des établissements de crédit reste soumise au principe de proportionnalité applicable de manière générale en la matière. Cette exigence de proportionnalité étant par essence relative, elle doit s'apprécier de manière continue, dans le temps, conduisant l'établissement de crédit à revoir ses exigences en la matière à l'aune, d'un côté, des nouveaux risques induits par l'IA (requérant une veille et une gouvernance appropriées) et, de l'autre côté, des opportunités offertes par l'IA en termes de maîtrise des risques et de développement des activités.

À ces règles, s'ajoutent les nouvelles exigences en matière de sécurité et de résilience opérationnelle numérique introduites par DORA, dont l'objectif est d'atteindre un niveau commun élevé de résilience opérationnelle numérique. Les établissements de crédit devront donc également veiller à ce que les Systèmes d'IA entrant dans le champ d'application de ce règlement en respectent les exigences.

Ils nécessitent d'être documentés notamment par des procédures et politiques internes et d'être intégrés dans le cycle de revue des risques et de conformité, requérant ainsi, par exemple, la tenue de comités de nouveaux produits (NAP).

L'IA consiste à analyser un grand nombre de données : la qualité et l'efficacité des Systèmes d'IA utilisés par les établissements de crédit dépend donc de la qualité et de la mise à jour de ces données.

L'utilisation de données trop anciennes ou inadaptées résulterait dans l'introduction de biais, voire même d'erreurs, dans les Systèmes d'IA. Il est donc essentiel que les banques mettent en place un cadre de la gestion des données utilisées par leurs algorithmes tout en respectant notamment la réglementation sur le traitement des données personnelles et le secret professionnel.

La technicité des algorithmes requiert également un investissement important des établissements de crédit, qui doivent former leur personnel, créer de nouveaux postes et/ou faire appel à des prestataires externes en mesure de développer des algorithmes adaptés à leurs besoins, d'en contrôler le bon fonctionnement, de les mettre à jour et d'y apporter des corrections le cas échéant. Outre l'investissement financier requis, les établissements de crédit doivent pouvoir répondre aux exigences d'explicabilité de leurs Systèmes d'IA : la complexité de certains algorithmes peut donc constituer un frein à leur utilisation par les établissements de crédit, s'ils ne sont pas en mesure d'expliquer clairement aux régulateurs le fonctionnement de ces outils et les décisions qu'ils prennent ou suggèrent à l'établissement de prendre. La responsabilité des établissements peut se trouver accrue à ce titre.

2. La gouvernance de l'IA pour les établissements de paiement et établissements de monnaie électronique

D'un point de vue général, les établissements de paiement et les établissements de monnaie électronique doivent veiller, au même titre que les établissements de crédit, à ce que leur gouvernance s'adapte à l'IA afin de garantir une utilisation conforme aux réglementations en vigueur. S'ils intègrent l'IA, les établissements de paiement et les établissements de monnaie électronique doivent respecter l'ensemble des normes de gouvernance et de contrôle interne qui leur sont imposées en raison de leur agrément[32] et notamment en application de l'Arrêté du 3 novembre 2014.

En termes de standard et d'approche, les établissements de paiement et établissements de monnaie électronique doivent s'assurer que l'intégration de l'IA dans leur contrôle interne tient compte du principe de proportionnalité et que les exigences en matière de sécurité et de résilience opérationnelle sont respectées. La qualité des données et l'explicabilité des algorithmes sont aussi essentielles pour éluder les biais algorithmiques et erreurs du Système d'IA.

Un investissement en formation et en ressources humaines est nécessaire pour répondre aux exigences réglementaires. Cela peut représenter un défi pour les établissements de plus petite taille, qui disposent de ressources limitées. La question de l'implication humaine dans les prises de décision est particulièrement cruciale pour ces plus modestes établissements. En effet, face à un manque de ressources et dans un souci de « *surefficience* », il existe un risque potentiel de dépendance à l'IA.

[32] *Article L. 522-6 du CMF pour les établissements de paiement et article L. 526-8 du CMF pour les établissements de monnaie électronique.*

Cela pourrait également entrainer une dépendance vis-à-vis de la société fournissant ce service, soulevant ainsi des questions sur leur capacité à agir de manière saine et prudente, conformément à leurs exigences réglementaires.

Les établissements de paiement et de monnaie électronique, en particulier ceux qui traitent avec des consommateurs, devront aussi veiller à garantir la transparence de leurs algorithmes d'IA et de l'utilisation qu'ils en font.

3. La gouvernance de l'IA requise pour les entreprises d'investissement

Les entreprises d'investissement doivent mettre en place une gouvernance de l'IA adaptée, garantissant que les Systèmes d'IA sont soumis à des contrôles réguliers et que des mécanismes d'audit sont en place pour vérifier leur bon fonctionnement[33].

Les dirigeants sociaux auront à mettre en œuvre un processus décisionnel et de surveillance adapté à la nature de l'outil qu'est l'IA. D'ailleurs, l'ESMA a insisté sur la nécessité pour les dirigeants sociaux de développer une compréhension approfondie des outils d'IA qu'ils déploient[34]. Les dirigeants sociaux devraient veiller à ce que les algorithmes respectent non seulement les exigences réglementaires applicables aux entreprises d'investissement (en ce compris notamment celles résultant de l'Arrêté du 3 novembre 2014), mais aussi les principes de bonne conduite, en garantissant que les décisions prises servent toujours l'intérêt supérieur du client, conformément aux exigences de la Directive 2014/65/UE du 15 mai 2014 concernant les marchés d'instruments financiers (**MiFID II**). Pour ce faire, la mise en place de processus de supervision humaine et des contrôles réguliers afin de s'assurer du bon fonctionnement des Systèmes d'IA s'imposent aux entreprises d'investissement.

La supervision des systèmes automatisés doit être appréhendée. La nécessité d'audits fréquents et de contrôles réguliers pour s'assurer que les Systèmes d'IA sont conformes aux objectifs de gestion des risques et aux exigences réglementaires semble ainsi fondée. En outre, les entreprises d'investissement devraient adopter des mécanismes rigoureux pour évaluer la qualité et la fiabilité des résultats générés par leurs Systèmes d'IA, en particulier lorsque ces résultats influencent des décisions d'investissement.

---

[33] *Article L. 533-29 du CMF.*

[34] *ESMA, Public Statement on the use of Artificial Intelligence (AI) in the provision of retail investment services, 30 mai 2024, ESMA35-335435667-5924, n° 10.*

Des programmes de formation continue auront à être mis en place et à évoluer en fonction des changements de cette technique. Cette formation aurait à couvrir non seulement l'utilisation des outils d'IA, mais aussi les risques associés, comme le biais algorithmique et la sécurité des données, etc. Un personnel bien formé est essentiel pour faire face aux défis posés par l'intégration de l'IA dans les services d'investissement et pour assurer le respect des obligations réglementaires.

4. La gouvernance de l'IA requise pour les entreprises d'assurance

L'EIOPA soulignait dans son Rapport sur les principes de gouvernance en matière d'IA, publié en 2021, que « *les solutions fournies par l'IA aux compagnies d'assurance présentent des risques qui nécessiteront une surveillance réglementaire et prudentielle* »[35].

Ce rapport préparé par un groupe d'experts a pour objet de présenter leurs travaux relatifs à des bonnes pratiques de gouvernance pour les entreprises d'assurance sans écarter d'autres approches possibles. Il est à cet égard intéressant de relever que l'EIOPA prépare actuellement une Opinion sur la gouvernance et la gestion des risques liés à l'IA dans le secteur de l'assurance, afin de conférer davantage de portée à ses recommandations en matière d'IA[36].

Si l'article L. 354-1 du Code des assurances rappelle que les entreprises d'assurance et de réassurance mettent en place un système de gouvernance garantissant une gestion saine et prudente de leur activité et faisant l'objet d'un réexamen interne régulier, le RIA quant à lui rappelle que ces règles continuent à s'appliquer lorsqu'elles font usage de systèmes d'IA.

La législation existante devrait en effet constituer la base de tout cadre de gouvernance de l'IA, mais il faut savoir ce que cela signifie dans le contexte de l'IA.

L'EIOPA rappelle les principes de gouvernance pour une IA éthique et digne de confiance dans le secteur de l'assurance, laquelle reposerait sur les principes suivants : principe de proportionnalité, principe d'équité et de non-discrimination, principe de transparence et d'explicabilité, principe de

[35] *EIOPA, Artificial Intelligence governance principles: towards ethical and trustworthy artificial intelligence in the European insurance sector, 17 juin 2021. Ce document représente les points de vue des membres du groupe consultatif d'experts de l'EIOPA sur l'éthique numérique dans le secteur de l'assurance, sans nécessairement représenter la position de l'EIOPA elle-même sur ces sujets.*

[36] *À propos de laquelle une consultation a été lancée début 2025, les réponses des acteurs (assureurs, intermédiaires, syndicats, fédérations, régulateurs etc.) étaient attendues pour le 12 mai 2025 ; EIOPA is seeking feedback on its Opinion on Artificial Intelligence governance and risk management, 12 février 2025.*

surveillance humaine, principe de gouvernance des données et de conservation des données, et le principe de robustesse et de performance.

L'EIOPA vient également préciser que le système de gouvernance des assureurs devrait en principe appréhender les impacts de l'IA au regard des compétences dont doivent disposer les membres du conseil d'administration (ou du conseil de surveillance) ainsi que les responsables de fonctions clés.

Aussi, tout en rappelant le principe de proportionnalité, elle invite les entreprises d'assurance à définir dans leurs politiques internes les différents rôles et responsabilités du personnel impliqué dans les processus d'IA et pose à cet égard certaines bonnes pratiques en matière de gouvernance. Ainsi, les organes d'administration, de gestion ou de contrôle devraient avoir une compréhension suffisante de la manière dont l'IA est utilisée dans leurs organisations respectives et des risques qu'elle comporte.

Quant aux différents responsables de fonctions clés, leurs missions évolueront nécessairement à l'aune de l'utilisation de l'IA au sein de l'entreprise d'assurance. Par exemple, l'EIOPA souligne que[37] :

- la fonction de vérification de la conformité s'assure que l'utilisation de l'IA au sein de l'entité est conforme aux règles applicables ;

- la fonction d'audit interne évalue la qualité et l'efficacité des algorithmes et met en place des contrôles appropriés ;

- la fonction de gestion des risques renforce les contrôles des données sous-jacentes aux Systèmes d'IA en veillant notamment à ce qu'elles demeurent exemptes de biais interdits ;

- la fonction actuarielle est responsable des contrôles appliqués aux Systèmes d'IA utilisés dans le cadre de ses missions (calcul des provisions techniques, opinion sur la politique de souscription etc.).

En outre, et sur la base de l'article 260 du règlement délégué (UE) 2015/35[38] qui prévoit que le système de gestion des risques doit inclure des politiques relatives à la suffisance et à la qualité des données à prendre en considération dans les processus de souscription et de provisionnement, l'EIOPA prévoit que les entreprises d'assurance devraient mettre en œuvre une politique de gouvernance des données alignée avec l'impact potentiel des cas d'usage de l'IA sur les clients ou l'entreprise et conforme à la législation applicable en matière de protection des données[39].

---

[37] *EIOPA, consultation paper on its Opinion on Artificial Intelligence governance and risk management, 10 février 2025.*

[38] *Complétant la directive (UE) n° 2009/138 sur l'accès aux activités de l'assurance et de la réassurance et leur exercice (***Solvabilité II***).*

[39] *Ibid.*

5. La gouvernance de l'IA requise pour les sociétés de gestion

Les directives et réglementations sectorielles spécifiques à la gestion d'actifs ne prévoient pas de dispositifs particuliers d'encadrement des risques susceptibles de résulter du recours à l'IA.

Cela étant dit, certains moyens de contrôle résultant de ces réglementations permettent, en raison de leur généralité et transversalité, d'encadrer le recours à de telles technologies IA. Ces dispositifs, qui s'ajoutent à ceux résultant de réglementations transverses distinctes (DORA, RGPD etc. – voir paragraphe III *infra*) peuvent être de différentes natures.

À titre illustratif, l'agrément des sociétés de gestion donne lieu en France à une revue, par l'AMF, de la présentation des procédés d'investissements et autres outils et moyens technologiques mis en œuvre par toute société de gestion française dans le cadre de ses activités de gestion.

L'AMF dispose ainsi déjà de la faculté d'être informée, non seulement durant la phase d'agrément des sociétés de gestion mais aussi durant toute la durée de vie de ces dernières (par le biais de l'actualisation obligatoire de leur programme d'activité via l'interface ROSA au gré des évolutions de ce dernier), des outils technologiques – en ce inclus ceux fondés sur l'IA – mis en œuvre par toute société de gestion, et des moyens mis en œuvre par ces sociétés de gestion pour contrôler ces outils et leur paramétrage.

L'AMF peut ainsi déjà approfondir et le cas échéant encadrer le recours à l'IA par toute société de gestion française, de sorte qu'aucun mécanisme additionnel d'agrément distinct relatif à tout Système d'IA ne semble dans ce contexte requis.

De façon similaire, l'agrément d'une société de gestion française requiert déjà la démonstration par cette dernière d'un plan de continuité d'activité (« *back-up plan* ») destiné à établir sa capacité à gérer d'éventuels incidents et/ou défaillances technologiques et ainsi permettre la continuité des activités qu'elle exerce[40]. Un tel plan doit ainsi détailler les moyens concrets envisagés par une société de gestion en vue d'éviter toute interruption de ses activités, peu important la nature des technologies susceptibles d'être affectées par toute éventuelle défaillance (en ce incluse donc toute technologie le cas échéant fondée sur l'IA).

Ces aspects sont par ailleurs renforcés par des développements à inclure en matière de cybersécurité, lesquels font l'objet d'une vigilance accrue de la part de l'AMF comme en attestent les synthèses des différents contrôles SPOT AMF relatifs aux dispositifs de cybersécurité publiées en décembre 2019, avril 2021 et décembre 2023 (lesquelles identifient tout un ensemble de bonnes et mauvaises

[40] *Voir article 321-25 du Règlement général de l'AMF (OPCVM), article 57(3) du Règlement délégué (UE) n° 231/2013 (dit Règlement AIFM) et article 21(3) du Règlement délégué n° 2014/65/UE (si fourniture de services d'investissement) ainsi que position – recommandation AMF n° 2012-19.*

pratiques en ce domaine, tant en matière de gouvernance, de *reporting* que de cartographie des prestataires et de gestion des incidents) mais également la doctrine AMF précitée, laquelle précise qu'une société de gestion doit détailler le dispositif mis en place par elle en matière de cybersécurité[41].

Enfin, un nouveau guide professionnel de l'AFG propose des principes militant pour une utilisation responsable de l'IA par les sociétés de gestion qui passe notamment par l'instauration d'une gouvernance adaptée pour s'assurer de la conformité des usages de l'IA avec la réglementation des sociétés de gestion[42].

Cet environnement réglementaire doit par ailleurs être intégré par la société de gestion dans le cadre de son dispositif de contrôle interne.

D. La protection de la clientèle doit être assurée

Les clients seront en tout état de cause protégés par la nécessité d'un agrément pour qu'un acteur délivre une prestation de service réglementée : peu importe le support ou le moyen mis en œuvre – IA ou autre – dès lors que la prestation fournie au client répond à la qualification de service d'investissement, bancaire, de paiement, d'assurance ou s'inscrit dans le cadre d'une activité de gestion collective, un agrément devra par principe être obtenu et les règles de bonne conduite applicables respectées.

Au-delà du respect des règles de bonne conduite inhérentes à la prestation de services réglementés, lorsque l'IA est utilisée pour la fourniture de ces services, d'autres problématiques liées à l'usage de cette technologie sont mises en exergue.

1. L'explicabilité et la transparence sont les principales préoccupations

La réponse apportée au client par l'algorithme doit satisfaire à toutes les exigences applicables à l'Institution Financière dans le cadre de sa communication avec des clients ou des clients potentiels (transparence, clarté, secret professionnel), mais également à l'égard de leurs superviseurs.

L'utilisation de l'IA, si elle est dûment maîtrisée, peut donc permettre aux Institutions Financières de gagner en efficacité et de réduire leurs coûts, mais présente également une source de risque potentiel qui doit être maîtrisée. Cela implique de manière générale que les Institutions Financières

---

[41] Ainsi que des ateliers dédiés à ces thématiques, notamment dans le cadre des journées de formations RCCI-RCSI en mars 2023 avec la présence de l'ANSSI.

[42] AFG, op. cit., Guide Professionnel Principes et bonnes pratiques pour une utilisation responsable de l'IA par les sociétés de gestion, janvier 2025.

restent en mesure d'expliquer le fonctionnement du modèle utilisé ainsi que le produit de l'analyse fournie par l'algorithme (par exemple, une analyse de risque de crédit d'un emprunteur potentiel). Ceci nécessite de documenter l'explicabilité et de définir par des procédures et processus appropriés, une gouvernance adéquate qui doit être revue de manière régulière[43].

En tout état de cause, l'Institution Financière utilisant l'IA doit garder le contrôle des décisions qui sont prises à l'aide de cet outil, et doit pouvoir s'en écarter en cas d'analyse difficilement explicable ou interprétable, voire incohérente. Cette exigence est susceptible de constituer une difficulté pratique additionnelle pour l'Institution Financière.

Les règles de bonne conduite issues de la directive MiFID II appréhendent déjà, quant à elles, les enjeux d'information et de transparence vis-à-vis des investisseurs[44]. En application de son obligation générale de primauté de l'intérêt du client et de son obligation générale d'information, une Institution Financière fournissant un service d'investissement au sens de la directive MiFID II doit veiller à informer sa clientèle de son utilisation de l'IA dans la prestation de ses services. Cette transparence nous semble particulièrement importante compte tenu des risques associés à l'utilisation de l'IA dans ce contexte. À titre d'exemple, une Institution Financière offrant un service de conseil en investissement, dont les recommandations sont optimisées par une solution d'IA, doit en informer sa clientèle, car les risques inhérents à l'utilisation de cette technologie peuvent influencer les conseils prodigués[45].

De même, l'IA doit faire l'objet d'une communication claire, exacte et non trompeuse de la part des Institutions Financières et notamment des sociétés de gestion de portefeuille et prestataires de services d'investissement, conformément à leurs obligations réglementaires respectives[46]. Plus spécifiquement, cette obligation devrait imposer aux Institutions Financières de s'abstenir d'« *AI washing* », c'est-à-dire présenter l'utilisation de l'IA de manière disproportionnée par rapport à l'usage réel qui en est fait, de sorte à induire le client/investisseur en erreur sur la valeur ajoutée ou la performance du service fourni. À notre connaissance, aucune sanction n'a été prononcée pour de tels agissements en France ; mais le régulateur américain (*U.S. Securities and Exchange*

[43] *ESMA, Public Statement on the use of Artificial Intelligence (AI) in the provision of retail investment services, 30 mai 2024, ESMA35-335435667-5924, n°25 "By fostering transparency, implementing robust risk management practices, and compliance with legal requirements, ESMA would aim to help firms ensure they harness the potential of AI while safeguarding investors' confidence and protection".*

[44] *Ibid, spéc. n° 7 et s.*

[45] *ESMA, Orientations concernant certains aspects relatifs aux exigences d'adéquation de la directive MiFID II, ESMA35-43-3172, 3 avril 2023, paragraphe 17.*

[46] *Article L.533-22-2-1 du CMF pour les sociétés de gestion de portefeuille ; Article L. 533-15 du CMF pour les prestataires de service d'investissement.*

Commission) a d'ores et déjà sanctionné deux sociétés de conseil en investissement début 2024 pour communication fausse et trompeuse sur base d'*AI washing*[47]. L'ESMA reste attentive à ce phénomène et a publié un document d'information public à ce sujet[48].

Les Institutions Financières devraient faire leurs meilleurs efforts pour s'assurer que les données utilisées pour entraîner leurs Systèmes d'IA soient exemptes de biais, en appliquant en tout état de cause les exigences issues de la réglementation MiFID II, notamment en s'assurant de la qualité de leurs procédures[49].

2. L'encadrement des responsabilités des Institutions Financières

Les chaînes de responsabilité devront également clairement intégrer l'utilisation de l'IA. Les risques induits à ce titre nécessitent également d'être cantonnés via les conventions, la documentation contractuelle ainsi que les politiques et procédures internes[50].

Face à la place croissante que prend l'IA dans les opérations journalières des Institutions Financières mais aussi plus globalement de tout autre acteur (e.g. fournisseurs, prestataires etc.), un encadrement contractuel spécifique de cette technologie semble requis. Ceci s'avère nécessaire non seulement quand le prestataire est spécialisé dans la fourniture d'une solution IA mais aussi lorsque cette technologie est utilisée par un prestataire non spécialisé. La mise en place par les Institutions Financières d'un clausier spécifique à l'IA pourrait être envisagée, couvrant divers aspects tels que la transparence des algorithmes, la protection des données clients et confidentielles, ou encore le respect du secret professionnel.

Pour les relations spécifiques avec les prestataires d'IA et sous réserve de règlementations techniques européennes sur le sujet, des clauses contractuelles additionnelles sont requises par DORA dans le cadre de l'utilisation des services de technologies de l'information et de la communication[51] (**TIC**). Par exemple, une clause de réversibilité pourra être incluse pour garantir la continuité des services de l'Institution Financière en cas de changement de prestataire ou résiliation des accords contractuels ; ou encore des dispositions plus strictes concernant le traitement des données clients et la confidentialité, eu égard à la sensibilité des informations traitées par ces acteurs.

---

[47] *SEC v. Global Predictions, Inc, N° 3-21894 (SEC, 18 mars 2024) ; SEC v. Delphia (USA) Inc., N° 3-21894 (Sec, 18 mars 2024).*

[48] *ESMA, Using Artificial Intelligence for Investing: What you should consider, 2025.*

[49] *ESMA, op. cit., Public Statement On the use of Artificial Intelligence (AI) : "Investment firms should implement rigorous quality assurance processes for their AI tools. This should include thorough testing of algorithms and their outcomes for accuracy, fairness, and reliability in various market scenarios."*

[50] *Cf. le paragraphe IV du Rapport.*

[51] *Article 30 de DORA.*

E. L'encadrement des utilisations de l'IA passe aussi par la réglementation prudentielle

1. L'encadrement prudentiel de l'utilisation de l'IA aux fins de la fourniture de services financiers

Le recours aux Systèmes d'IA par les Institutions Financières est susceptible d'avoir un impact sur les exigences de fonds propres pour risque opérationnel, telles que prévues par le cadre prudentiel applicable aux établissements de crédit (composé de la directive sur la surveillance prudentielle des établissements de crédit (CRD) et du règlement sur les exigences prudentielles (règlement (UE) 575/2013 du 26 juin 2013 concernant les exigences prudentielles applicables aux établissements de crédit (**CRR**)), celui applicable aux entreprises d'investissement (composé de la directive (UE) 2019/2034 du 27 novembre 2019 sur la surveillance prudentielle des entreprises d'investissement (**IFD**) et du règlement (UE) 2019/2033 du 27 novembre 2019 sur les exigences prudentielles applicables aux entreprises d'investissement (**IFR**)) ainsi que, pour ce qui concerne les entreprises d'assurance, Solvabilité II et le règlement délégué (UE) 2015/35 qui la complète.

L'utilisation de l'IA doit ainsi être intégrée dans les dispositifs d'appréciation des risques encourus par les Institutions Financières comme tous les risques liés à l'usage des technologies. L'utilisation des Systèmes d'IA est ainsi d'ores et déjà supervisée par les autorités compétentes sous l'angle des risques opérationnels susceptibles d'en découler.

2. L'encadrement de l'utilisation de l'IA à des fins prudentielles

La réglementation prudentielle est considérée, dans son ensemble, comme technologiquement neutre dans le sens où elle n'interdit, n'impose, ne privilégie ou ne pénalise pas en principe le recours à une technologie plutôt qu'une autre pour son application, sous réserve que la technologie utilisée n'induise pas de nouveaux risques qui ne seraient pas précisément identifiés et maîtrisés[52]. Elle ne s'oppose ainsi pas, en principe, à ce que les Institutions Financières recourent à l'IA pour satisfaire aux exigences prudentielles qui leur sont applicables, que ce soit en matière de contrôle interne et conformité ou pour la détermination de leurs exigences de fonds propres. L'IA peut en effet s'avérer un outil particulièrement utile pour permettre aux Institutions Financières (au premier

[52] *Selon la BCE, "the EU financial services regulatory framework is already broadly technology neutral" (ESCB/European banking supervision response to the European Commission's public consultation on a new digital finance strategy for Europe/ FinTech action plan, août 2020, p. 17). Cette approche technologiquement neutre est également mise en oeuvre par la BCE dans le cadre de la supervision bancaire ("The ECB follows a technology-neutral approach to its areas of competence, including banking supervision and the oversight of payment systems, in accordance with the SSM Regulation and the Treaty on the Functioning of the European Union" ou "The ECB supports a technology-neutral approach to regulation, supervision and oversight" (même réponse de la BCE, p. 11). La position du régulateur bancaire européen à cet égard est constante et régulièrement réaffirmée « In my view, supervisors should essentially be technology-neutral" (Panel remarks by Andrea Enria, Chair of the Supervisory Board of the ECB, at the Financial Stability Institute 20th anniversary conference, Basel, 12 mars 2019).*

rang desquels les établissements de crédit) de faire face à l'accroissement continu et à la complexité grandissante de la réglementation prudentielle.

D'une part, les règles applicables en matière de contrôle interne et de conformité n'excluent pas, *a priori*, la possibilité pour les Institutions Financières assujetties d'utiliser l'IA dans le cadre du dispositif global de contrôle interne et de conformité qu'elles mettent en place pour s'y conformer[53]. Toutefois, comme le souligne l'ACPR, les règles en matière de contrôle interne ont été rédigées « *dans l'idée que les contrôles étaient effectués par des humains* »[54]. Contrôle permanent et contrôle périodique doivent en effet être effectués par des personnes physiques, que celles-ci soient dédiées à ces contrôles ou engagées par ailleurs dans des activités opérationnelles, selon le cas. Cette exigence de l'implication de l'humain n'exclut pas pour autant l'usage de l'IA. En revanche, elle tend à cantonner l'IA dans un rôle d'assistant de l'humain ou tout au moins à minimiser son recours en tant qu'exécutant. L'utilisation de l'IA en matière de contrôle interne et de conformité appelle ainsi à une revue minutieuse des exigences applicables, de manière à déterminer la part des contrôles qui peut être réalisée en utilisant des Systèmes d'IA et celle qui doit impérativement être confiée à des humains pour respecter les exigences applicables.

D'autre part, la réglementation prudentielle applicable aux établissements de crédit (i.e. CRR/CRD) ne s'oppose pas non plus à l'utilisation de l'IA pour satisfaire à ses exigences, lorsque cela apparaît possible. Au contraire, elle encourage, dans une certaine mesure et sous certaines conditions, l'usage de l'IA par les établissements de crédit aux fins du calcul des exigences de fonds propres. Cette utilisation, via les modèles mis en place par les établissements dans le cadre des approches internes, fait toutefois l'objet d'un encadrement très rigoureux.

Les établissements de crédit sont en effet tenus de se conformer aux exigences prévues par CRR pour les approches internes, ce qui peut soulever des difficultés et une certaine complexité en présence de Systèmes d'IA complexes (dits « *boîtes noires* ») en particulier pour satisfaire à l'exigence d'interprétabilité et d'explicabilité posée par CRR. Des publications récentes des autorités de supervision (notamment de l'Autorité bancaire européenne (**EBA**) et de l'ACPR) indiquent que les superviseurs, conscients de la difficulté mais également des enjeux que représente l'utilisation de l'IA pour les établissements de crédit (du fait notamment de son potentiel d'amélioration des capacités prédictives d'évaluation du risque de crédit), se sont orientés vers un encadrement fondé sur des recommandations de principe (*principle-based recommendations*) destinées à affiner l'application de la réglementation CRR encadrant les modèles internes en cas de recours à l'IA.

---

[53] *Aucune disposition de l'Arrêté du 3 novembre 2014 n'interdit le recours à l'utilisation de l'IA dans les dispositions de contrôle interne mis en place par les assujettis.*

[54] *ACPR, Document de réflexion, Intelligence artificielle – Enjeux pour le secteur financier, décembre 2018, paragraphe 3.1.3 p. 25.*

L'EBA a ainsi élaboré une série de recommandations[55], invitant les établissements à notamment s'assurer que les modèles fondés sur l'IA qu'ils utilisent sont compris par leurs utilisateurs aux différents niveaux requis, n'excèdent pas le degré de complexité nécessaire à leur objectif, sont interprétables et correctement documentés, régulièrement contrôlés et mis à jour, et impliquent un contrôle par l'humain qui doit être en mesure de comprendre les hypothèses et le comportement du modèle par rapport aux prédictions qu'il effectue (aussi bien au stade de son développement que de son application).

Les récentes modifications apportées à CRR par le règlement dit CRR3[56], en vigueur depuis le 1er janvier 2025, ne remettent pas en cause la possibilité pour les établissements assujettis de recourir à l'IA aux fins de la détermination de leurs exigences de fonds propres[57] mais pourraient dans une certaine mesure, compte tenu de leur objectif (à savoir réduire les possibilités d'arbitrage offertes par l'utilisation des approches internes), rendre moins attractif le recours à l'IA dans ce domaine pour certains établissements de crédit[58] ou conduire à repenser/réorienter son utilisation dans ce contexte[59]. À cet égard, les nouvelles formes d'IA en gestation (notamment les Systèmes d'IA dits nativement interprétables (*natively interpretable AI*) en ce qu'ils permettent de relier les prévisions du modèle aux variables utilisées par celui-ci[60]) pourraient faciliter la conformité aux exigences réglementaires dans le cadre du recours à l'IA aux fins de la détermination des exigences de fonds propres, en réduisant considérablement les difficultés d'interprétabilité (i.e. grâce à la réduction voire l'élimination de l'effet « *boîte noire* »), sans pour autant perdre en performance prédictive[61].

---

[55] EBA, Machine Learning for IRB models – Follow-up report from the consultation on the discussion paper on machine learning for IRB models, (EBA/REP/2023/28), 4 août 2023.

*[56] Règlement (UE) 2024/1623 du Parlement européen et du Conseil du 31 mai 2024 modifiant CRR en ce qui concerne les exigences pour risque de crédit, risque d'ajustement de l'évaluation de crédit, risque opérationnel et risque de marché et le plancher de fonds propres (**CRR3**).*

[57] On notera à cet égard l'introduction d'une définition du risque de modèle par CRR3 (article 4(1)52 ter de CRR) qui par sa généralité, permet d'appréhender les diverses formes d'IA et de ce fait semble confirmer la non-opposition de principe à recourir à l'IA aux fins de satisfaire aux exigences prudentielles prévues par CRR/CRD (CRD incluait déjà, depuis son adoption le 26 juin 2013, une définition souple assez similaire du risque lié au modèle capable d'appréhender l'IA sous ses diverses formes – transposée à l'article 10(aa) de l'Arrêté du 3 novembre 2014).

[58] Les modifications apportées par CRR3 imposent des contraintes supplémentaires en matière d'utilisation des modèles internes aux fins de la détermination des exigences de fonds propres (notamment en imposant le recours à l'approche standard pour certaines expositions et en introduisant des valeurs minimales (« planchers » ou « input floors ») pour les estimations propres faites par les établissements de crédit des paramètres de risques, qu'il s'agisse de la probabilité de défaut, de la LGD ou des facteurs de conversion, ainsi qu'un plancher de fonds propres global (« output floor »)).

[59] Par exemple, CRR3 affine et rend plus sensible au risque l'approche standard pour le risque de crédit et rend contraignante l'approche alternative par les modèles internes (A-IMA), aux côtés de l'approche alternative standard (A-SA) et de l'approche standard simplifiée, pour le risque de marché.

[60] Tel est le cas par exemple des modèles fondés sur une régression logistique ou un arbre de décision (par opposition aux modèles du type « forêts aléatoires » dont l'interprétabilité est pratiquement impossible).

[61] Voir notamment, sur cette proposition, la publication intitulée « Modèles internes des banques pour le calcul du capital réglementaire (IRB) et intelligence artificielle » d'Henri Fraisse et Christophe Hurlin, parue dans les Débats économiques et financiers (n° 44) de l'ACPR et la Banque de France en mars 2024.

En tout état de cause, que ce soit pour la détermination des exigences de fonds propres pour risque de crédit, risque de crédit de contrepartie, risque opérationnel ou risque de marché, l'utilisation de modèles internes – et donc de l'IA – à des fins prudentielles est systématiquement soumise à l'autorisation préalable des autorités compétentes. Cette autorisation, rendue nécessaire par le fait que l'utilisation des approches internes permet aux établissements de crédit de dévier des exigences standard pour définir leur propre méthodologie de calcul du capital réglementaire, n'est accordée qu'une fois que les autorités compétentes ont été en mesure de vérifier que le modèle envisagé satisfait à l'ensemble des exigences quantitatives et qualitatives prévues par la réglementation (en l'occurrence pour l'essentiel CRD/CRR et l'Arrêté du 3 novembre 2014), en ce compris la mise en place d'une solide gouvernance pour la gestion du risque lié au modèle (i.e. un partage clair des responsabilités, des politiques et procédures claires de détection, gestion, suivi, déclaration, etc).

Logiquement, et pour les mêmes raisons, les modifications apportées aux modèles internes mis en place par les établissements de crédit sont également soumises à autorisation des autorités compétentes. En outre, en cas de non-respect des conditions requises ou d'insuffisances constatées dans la précision du modèle, les autorités compétentes sont habilitées à révoquer l'autorisation d'utilisation accordée ou imposer des mesures appropriées d'amélioration dans un bref délai.

L'usage de l'IA est également permis aux fins du calcul des exigences de fonds propres des entreprises d'investissement. Cette approche s'inscrit dans le cadre du régime prévu par le cadre IFD/IFR pour les exigences de fonds propres, qui permet aux entreprises d'investissement d'utiliser des modèles internes pour calculer le facteur K reflétant le risque de position nette (K-NPR), d'une manière alignée avec le cadre prudentiel des établissements de crédit (CRD/CRR). Cette utilisation de l'IA à des fins prudentielles demeurera probablement marginale pour les entreprises d'investissement dans la mesure où elle ne touchera que celles qui négocient pour compte propre et qui optent pour l'utilisation des modèles internes aux fins du calcul de K-NPR (au lieu de l'approche standard ou l'approche standard alternative). Le cas échéant, cette utilisation de l'IA sera, comme pour les établissements de crédit, soumise à l'agrément des autorités compétentes qui s'assureront de la satisfaction des exigences quantitatives et qualitatives requises, *ab initio*, puis dans le cadre d'un contrôle régulier.

De même, les compagnies d'assurance soumises à Solvabilité II peuvent *a priori* recourir à l'IA pour calculer leur capital de solvabilité requis lorsqu'elles effectuent ce calcul à l'aide d'un modèle interne (intégral ou partiel), sous réserve que ce modèle interne ait été approuvé par les autorités de contrôle[62]. L'usage que peuvent faire les compagnies d'assurance de l'IA aux fins de déterminer

[62] *Articles 112 et 113 de Solvabilité II, tels que transposés aux articles L. 352-1 et s. et R. 352-2 et s. du Code des assurances, et complétés par les articles 228 et s. du règlement délégué (UE) 2015/35.*

leurs exigences de fonds propres lorsqu'elles utilisent les modèles internes est ainsi non seulement encadré par la réglementation, qui impose la satisfaction de nombreuses exigences (y compris en ce qui concerne les données utilisées et en matière d'explicabilité des modèles) mais également soumis à une supervision continue de la part des autorités qui pourront, en cas de non-respect des exigences applicables, imposer des exigences de capital supplémentaires voire retirer l'autorisation accordée.

D'autres types d'Institutions Financières, lorsqu'elles sont tenues de déterminer tout ou partie de leurs exigences de fonds propres en fonction par exemple des risques qu'elles encourent, pourraient aussi, potentiellement, recourir à l'usage de l'IA aux fins d'effectuer cette détermination, sous réserve que la réglementation qui leur est applicable ne s'y oppose pas. Le cas échéant, le recours à l'IA ne devrait pas être générateur de risques non identifiés et non maîtrisés et devrait s'effectuer dans le respect de l'ensemble de la réglementation applicable à l'Institution Financière concernée. Un usage de l'IA dans ce cadre pourrait par exemple être envisagé par les sociétés de gestion de portefeuille agréées au titre de la directive AIFM aux fins de déterminer les exigences de fonds propres supplémentaires qu'elles doivent respecter pour couvrir les risques éventuels de mise en cause de leur responsabilité professionnelle à l'occasion de la gestion de FIA en fonction des risques qu'elles supportent[63].

Comme lorsqu'elle est utilisée aux fins de l'exécution de prestations de services réglementées en faveur de la clientèle, le recours à l'IA aux fins de la satisfaction des exigences réglementaires prudentielles par les Institutions Financières doit être intégré dans les dispositifs d'appréciation des risques encourus comme tous les risques liés à l'usage des technologies (voir sur ce point notamment le paragraphe B ci-dessus).

F. L'encadrement de la protection des données clients doit intégrer le recours à l'IA

Le secret bancaire n'appartient pas aux dispositions faisant l'objet d'une harmonisation au niveau européen. En droit français, il est prévu qu'en principe, les membres de l'organe de surveillance d'un établissement règlementé[64] et toute personne qui a un titre quelconque participe à la

[63] *Conformément à l'article 317-2, IV du règlement général de l'AMF, les fonds propres supplémentaires d'une société de gestion de portefeuille agréée pour gérer des FIA doivent être « d'un montant suffisant pour couvrir les risques éventuels de la mise en cause de sa responsabilité pour négligence professionnelle ». Le taux de 0,01% prévu par l'article 14(2) du règlement (UE) 231/2013 étant un taux minimum, « le taux retenu par la société de gestion de portefeuille doit résulter d'une analyse menée régulièrement par cette dernière concernant les risques qu'elle supporte et leur quantification et le montant ainsi défini doit correspondre aux risques supportés et être d'un niveau suffisant pour permettre de prendre les mesures de remédiations rendues nécessaires » (Position - recommandation AMF - DOC-2012-19 - Guide d'élaboration du programme d'activité des sociétés de gestion de portefeuille et des placements collectifs autogérés, à jour au 18 décembre 2024, p. 57). Le recours à l'IA pour estimer les fonds propres supplémentaires nécessaires à cet égard (au titre notamment des risques opérationnels supportés par la société de gestion de portefeuille) paraît envisageable, bien qu'il ne s'agisse pas là d'un cas d'usage déjà répertorié.*

[64] *Article L. 511-33 du CMF pour les établissements de crédit et les sociétés de financement ; Article L. 522-19 du CMF pour les établissements de paiement ; Article L. 526-35 du CMF pour les établissements de monnaie électronique ; Article L. 531-12 du CMF pour les entreprises d'investissement et les sociétés de gestion de portefeuille ; Article L. 421-8 du CMF pour les entreprises de marché ; Article L. 440-8 du CMF pour les chambres de compensation ; etc.*

direction ou à la gestion d'un tel établissement ou qui est employée par celui-ci, sont tenus au secret professionnel. Des dérogations sont prévues, notamment face à certaines autorités (ACPR, Banque de France, autorité judiciaire dans le cadre de procédures pénales, etc.) ou dans certains cas (cessions et transferts de contrats, prises de participation ou de contrôle, contrats de prestations de services, etc.), à certaines conditions[65]. En tout état de cause, le bénéficiaire de la protection peut expressément y renoncer.

Le secret bancaire français est non seulement relativement strict par rapport à d'autres juridictions de l'UE mais soulève en plus de nombreuses interrogations, comme en témoigne la jurisprudence : les clients d'un établissement soumis à l'obligation de confidentialité sont-ils les seuls bénéficiaires du secret ? L'obligation de confidentialité survit-elle à la fin de la relation d'affaires ? Quelles informations doivent être considérées comme couvertes par le secret ? Quelle forme doit prendre la renonciation expresse du bénéficiaire ? La liste des personnes à qui il n'est pas opposable est-elle exhaustive ? À ces questions s'ajoute également celle de l'articulation des dispositions relatives au secret bancaire avec celles relatives au secret professionnel prévu par le Code pénal, dont le secret bancaire serait une déclinaison.

Ces questions se posent à l'évidence dans le cadre de l'adoption par les Institutions Financières de l'IA et ce avec d'autant plus de force que la donnée est un élément clé de l'efficacité des algorithmes. Il est donc crucial pour les Institutions Financières de déterminer quelles sont les données qu'elles peuvent utiliser et, le cas échéant, dans quelle mesure, pour « *nourrir* » les Systèmes d'IA auxquels elles recourent. En effet, les données considérées comme couvertes par le secret professionnel pourraient ne pas pouvoir être utilisées par l'Institution Financière dans certains Systèmes d'IA, en fonction de leur finalité et des personnes susceptibles d'y avoir accès, en particulier lorsque ces derniers sont conçus par un tiers, soulevant ainsi des enjeux de confidentialité et de maîtrise des informations traitées. De sorte qu'en cas de collaboration avec des partenaires extérieurs, les Institutions Financières devront être en mesure de démontrer que les données utilisées ne quittent pas leur périmètre, afin de garantir le respect du secret.

L'enjeu est d'autant plus important dans le contexte européen : le RIA étant d'application directe au sein de l'UE, les Institutions Financières de juridictions autres que la France, pourraient bénéficier d'un avantage concurrentiel si elles peuvent utiliser des données considérées en droit français comme confidentielles dans leurs Systèmes d'IA ou à tout le moins plus facilement que les Institutions Financières françaises. Leurs Systèmes d'IA pourraient alors tourner avec des

[65] *L. 511-33 du CMF pour les établissements de crédit et les sociétés de financement ; Article. L. 522-19 du CMF pour les établissements de paiement ; Article L. 526-35 du CMF pour les établissements de monnaie électronique ; Article L. 531-12 du CMF pour les entreprises d'investissement et les sociétés de gestion de portefeuille ; Article L. 440-10 du CMF pour les chambres de compensation ; etc.*

données plus précises, plus à jour, plus pertinentes, etc., et produire en conséquence des analyses plus adaptées que les systèmes nourris avec des données davantage « *filtrées* ». À titre d'exemple, la renonciation au secret bancaire par son bénéficiaire semblerait pouvoir être valablement prévue dans des conditions générales dans certaines juridictions européennes, alors même que les exigences françaises semblent l'exclure, le consentement devant être donné « *au cas par cas* ».

Nous n'évoquerons pas ici la question des exceptions légales au secret bancaire mentionnées ci-dessus (qui ont déjà fait l'objet de travaux et d'un rapport du HCJP) mais nous souhaitons présenter une première grille d'analyse du sujet de la conformité aux dispositions relatives au secret bancaire dans le contexte de l'usage de Systèmes d'IA par les Institutions Financières assujetties à ces dispositions de Systèmes d'IA.

Il ne fait pas de doute que ces Institutions Financières ne pourraient faire usage des données de leurs clients au moyen des Systèmes d'IA offerts au grand public dans le respect des dispositions précitées. Les conditions d'usage de ces systèmes sont, en effet, explicites quant à la réutilisation des données des utilisateurs qui constitue donc une communication à des tiers devant faire l'objet d'un consentement exprès des clients concernés.

Toutefois, il nous semble que l'usage de Systèmes d'IA déployés dans le cadre d'infrastructures informatiques sécurisées (soit dans les propres serveurs de l'établissement, soit via des environnements externalisés non mutualisés et présentant des engagements de sécurité et de confidentialité satisfaisants), ne serait pas constitutif d'une divulgation à des tiers d'informations protégées, soumise à ce titre aux dispositions applicables au secret bancaire.

Le dispositif de protection des données confidentielles applicable aux Institutions Financières assujetties en France tel que prévu par le CMF, ne semble donc pas constituer un obstacle de principe au déploiement de Systèmes d'IA sous réserve de la mise en place de certains garde-fous que maîtrisent bien les Institutions Financières (mesures tant techniques qu'organisationnelles et contractuelles), notamment lorsque des données sensibles sont partagées/transférées pour alimenter un Système d'IA tiers. Dans cette perspective, l'IA serait pour les Institutions Financières une nouveauté technique à appréhender conformément au cadre règlementaire déjà existant, sans qu'il n'y ait lieu de lui réserver un traitement spécifique.

G. L'encadrement de l'IA au travers du recours à des prestataires tiers

1. La réglementation de l'externalisation

Comme a pu l'indiquer l'ACPR dans un document de réflexion de juin 2020[66], les Institutions Financières ont recours à différents types de tiers prestataires pour développer leur IA : la conception

[66] *ACPR, Gouvernance des algorithmes de l'intelligence artificielle dans le secteur financier, document de réflexion, juin 2020.*

et la réalisation peuvent être confiées une société externe et l'hébergement et l'exploitation de services d'IA peuvent être externalisés chez un hébergeur traditionnel ou un fournisseur de solutions de services en nuage (*cloud*)[67].

L'ACPR souligne à cet égard que la mise en œuvre d'une sous-traitance suppose de prévoir la réversibilité des solutions d'IA externalisées et doit être précédée par une analyse de risques *ex-ante*. En outre, l'Institution Financière doit pouvoir accéder au code source et aux modèles et offrir la même garantie au superviseur afin de rendre possible un audit couvrant les systèmes, le code logiciel et les données.

À l'aune des articles 231 et suivants de l'Arrêté du 3 novembre 2014 et des orientations de l'EBA sur l'externalisation[68], se pose la question d'une éventuelle qualification de la contractualisation avec ces prestataires externes de prestations de services essentiels externalisées (**PSEE**) ou « *Prestation de services ou autres tâches opérationnelles essentielles ou importantes* » pour reprendre l'expression usitée dans l'Arrêté du 3 novembre 2014[69].

En matière d'assurance, l'ACPR pourrait ainsi qualifier la sous-traitance de solutions d'IA comme une externalisation d'activité opérationnelle importante ou critique, au sens des articles L. 354-3 et R. 354-7 du Code des assurances, lesquels imposent une information préalable de l'ACPR via un formulaire dédié (cf. Instruction 2020-I-09, modifiée récemment pour inclure l'externalisation auprès d'un prestataire de services en nuage).

Dans son *Factsheet* sur le cadre réglementaire de l'IA en assurance publié le 15 juillet 2024, l'EIOPA rappelle que « *le recours à des systèmes d'IA tiers pourrait être considéré comme une sous-traitance*

---

[67] *Le groupe de travail renvoie vers les travaux menés par le HCJP dans son rapport sur le cloud bancaire en date de mai 2021 ; HCJP, Rapport sur le cloud bancaire : état des lieux et propositions, Mai 2021.*

[68] *EBA, Guidelines on outsourcing arrangements, EBA/GL/2019/02, 25 février 2019.*

[69] *Pour mémoire, l'article 10, r) de l'Arrêté du 3 novembre 2014 définit les prestations de services ou d'autres tâches opérationnelles essentielles ou importantes comme : « (i) les opérations de banque au sens de l'article L. 311-1 du Code monétaire et financier, l'émission et la gestion de monnaie électronique au sens de l'article L. 315-1 du même code, les services de paiement au sens du II de l'article L. 314-1 du même code et les services d'investissement au sens de l'article L. 321-1 du même code, pour lesquels l'entreprise assujettie a été agréée ; (ii) les opérations connexes mentionnées aux 1, 2 ,3, 7 et 8 du I de l'article L. 311-2, aux 1, 2, 5 et 6 de l'article L. 321-2 et aux articles L. 522-2 et L. 526-2 du Code monétaire et financier ; (iii) les prestations participant directement à l'exécution des opérations ou des services mentionnés aux deux premiers tirets ; (iv) ou toute prestation de services lorsqu'une anomalie ou une défaillance dans son exercice est susceptible de nuire sérieusement à la capacité de l'entreprise assujettie de se conformer en permanence aux conditions et obligations de son agrément et à celles relatives à l'exercice de son activité, à ses performances financières ou à la continuité de ses services et activités. »*
Sont ainsi expressément exclus : « (i) la fourniture à l'entreprise assujettie de services de conseil et d'autres services ne faisant pas partie des activités couvertes par son agrément ou par son habilitation, y compris la fourniture de conseils juridiques, la formation de son personnel, les services de facturation et la sécurité des locaux et du personnel de l'entreprise ; et (ii) l'achat de prestations standard, y compris des services fournissant des informations de marché ou des flux de données sur les prix ».

au sens de Solvabilité II »[70], avec toutes les conséquences que cela implique (notamment en termes de responsabilité, etc.). Dans une telle hypothèse, l'assureur ainsi que l'ACPR jouiront d'un accès effectif à toutes les informations relatives aux fonctions et activités sous-traitées, en ce compris la possibilité d'effectuer des inspections sur place, dans les locaux du prestataire de services (article 274(4) du règlement délégué (UE) 2015/35 complétant Solvabilité II).

Il est précisé que les entreprises d'assurance s'abstiennent d'externaliser des activités ou des fonctions opérationnelles importantes ou critiques, lorsque cette externalisation serait susceptible de nuire à la prestation continue d'un niveau de service satisfaisant à l'égard des assurés, souscripteurs et bénéficiaires de contrats et entreprises réassurées.

Les dispositifs en matière d'externalisation des Institutions Financières peuvent s'avérer complexes à mettre en œuvre face à des fournisseurs d'IA très concentrés refusant toute forme de contrôle voire d'audit de leur système par les superviseurs.

L'externalisation induite par le recours à l'IA peut emporter des enjeux réglementaires conséquents pour les sociétés de gestion. Plusieurs schémas peuvent théoriquement être envisagés et leur pertinence est susceptible d'évoluer au fur et à mesure de l'émergence et/ou de l'arrivée à maturité de nouvelles technologies articulées autour de l'IA :

- les prestataires peuvent simplement offrir des solutions d'IA s'imbriquant dans le processus décisionnel (et/ou autres procédures) mis en œuvre par les sociétés de gestion, auquel cas différents moyens de contrôle semblent d'ores-et-déjà exister en vue de couvrir ce cas de figure (voir régime de l'externalisation *infra* ou encore la description des moyens techniques mis en œuvre par la société de gestion et contrôlée par l'AMF lors de son agrément) ; ou

- les prestataires pourraient également, le cas échéant, offrir de véritables « *outils de gestion* » que l'IA pourrait potentiellement rendre dans une certaine mesure autonomes et auto-suffisants. Dans un tel schéma, qui ne nous semble pas encore d'actualité à ce jour[71], des prestataires offriraient des solutions technologiques fondées sur l'IA et intégrant déjà un processus décisionnel relatif à des activités de gestion sur certaines stratégies. Cette hypothèse poserait alors la question de l'encadrement de tels prestataires mais également du rôle de la société de gestion qui pourrait ainsi se voir reléguer au rang de simple chambre d'enregistrement des décisions issues du logiciel d'IA ainsi élaboré par le prestataire d'IA. À défaut de véritable activité de paramétrage de cet outil par la société de gestion et/ou d'intégration de données pertinentes nécessaires à son fonctionnement

[70] *EIOPA, Regulatory framework applicable to AI systems in the insurance sector, juillet 2024.*

[71] *ESMA TRV Risk Analysis, Artificial intelligence in EU investment funds: adoption, strategies and portfolio exposures, ESMA50-43599798-9923, 25 février 2025.*

effectif, le rôle « *discrétionnaire* » de la société de gestion pourrait être remis en question, voire déporté vers le prestataire offrant de tels outils clés en main, ce dernier devenant alors le véritable maître d'œuvre de la stratégie de gestion ainsi envisagée. En cas d'absence d'agrément en qualité de société de gestion de portefeuille (ou agrément équivalent dans un pays tiers) d'un tel prestataire tiers, un tel scénario pourrait par ailleurs être assimilable à une forme de contournement des règles applicables en matière de monopole relatif aux services de gestion d'actifs à raison de l'usage d'une technologie, ce qui s'avérerait contraire au principe de neutralité technologique de la règlementation.

En d'autres termes, plus les solutions technologiques offertes par les prestataires d'IA s'avéreront pointues et autonomes, plus les enjeux relatifs au recours à de tels prestataires s'avéreront importants et susceptibles d'impliquer des schémas d'externalisation de prestations essentielles (voir *infra*), lesquels font déjà en pratique l'objet d'une interprétation extensive, mais également potentiellement de qualification d'une activité de gestion au niveau des prestataires eux-mêmes et ce alors même que ces derniers ne disposent *a priori* pas d'un quelconque statut réglementé en matière de gestion d'actifs (voir enjeux d'agrément et risques de contournement évoqués *supra*). La démonstration du caractère discrétionnaire des prérogatives exercées par les sociétés de gestion, notamment par le biais du paramétrage de tels outils d'IA mais également du maintien d'un contrôle sur leur fonctionnement, s'avérera alors un élément clé du maintien de la discrétion de gestion inhérente à leur statut.

Au-delà de l'intervention humaine requise en matière de traitement automatisé, l'IA d'un prestataire tiers utilisée comme l'instrumentum de la fourniture d'une prestation réglementée pourrait remettre en cause l'agrément de l'Institution Financière mais aussi soumettre le prestataire aux exigences d'agrément des Institutions Financières.

2. Vers un encadrement des *Big Techs*

Dans une publication d'octobre 2024[72], l'ACPR envisage un nouveau cadre prudentiel pour les entreprises technologiques communément appelées les *Big Techs*.

Comme le note l'ACPR dans sa publication, DORA a introduit un cadre nouveau dans l'Union européenne pour encadrer le recours par des Institutions Financières à des TIC (y compris potentiellement des solutions d'IA – voir paragraphe G) et à leurs prestataires de services. À cet égard, DORA introduit un cadre de supervision spécifique pour les prestataires de services TIC considérés comme critiques pour les Institutions Financières[73]. Ce dispositif a ainsi pour ambition d'apporter une première réponse réglementaire à l'implication croissante de certaines entreprises technologiques avec le secteur bancaire et financier.

[72] *ACPR, Le développement des Big Techs dans le secteur financier : quels risques, quelles réponses réglementaires ? Octobre 2024.*

[73] *Articles 31 et suivants de DORA.*

Toutefois, plus largement, l'ACPR souligne que la place jusque-là limitée des « *Big Techs* » dans l'industrie financière continue de croître, portée par « *des innovations technologiques qui leur offrent un avantage comparatif important* »[74]. Parmi les avantages compétitifs de ces acteurs, l'autorité française rappelle leur « *capacités de collecte, d'analyse et d'exploitation de données à grande échelle, couplées à la maîtrise de technologies avancées en intelligence artificielle (IA) et en machine learning* »[75], qui leur permettent potentiellement de « *proposer des services présumés plus adaptés, à partir de l'identification des besoins clients et ainsi capturer des parts de marché et générer de nouvelles sources de revenus* »[76]. Face à cette importance croissante et aux risques afférents, l'ACPR s'interroge sur le besoin de faire évoluer le cadre applicable à ces acteurs.

Cette initiative se fonde notamment sur un constat : la règlementation européenne ne prévoit pas de surveillance consolidée pour les groupes d'établissements de paiement ou de monnaie électronique. Cette situation empêche les autorités de surveillance de développer une vision exhaustive des risques portés par de tels groupes, dans un contexte où l'usage croissant des Systèmes d'IA pourrait donner naissance à des « *Big Techs* ». Afin de répondre à cette lacune, une exigence de surveillance consolidée pourrait être introduite dans la directive sur les services de paiement (**DSP**), dès lors qu'un groupe financier, qui ne serait pas déjà soumis à la surveillance prudentielle au titre de CRR, compterait au moins un établissement de paiement ou de monnaie électronique. Une telle surveillance pourrait reposer sur l'introduction d'une notion de compagnie *holding* de paiement, similaire à celle de compagnie financière *holding*.

Au-delà des aspects de consolidation, d'autres renforcements du cadre DSP pourraient également se justifier dans un contexte de développement des « *Big techs* ». Ceux-ci pourraient impliquer notamment l'application d'exigences supplémentaires de fonds propres (« pilier II ») et l'introduction d'exigences de liquidité pour les établissements de paiement et de monnaie électronique, ainsi que l'encadrement des prestations techniques de type X-Pay (par exemple Apple Pay, Google Pay) et de la fourniture de services en marque blanche, notamment en imposant une plus grande transparence et des mesures visant à assurer la protection des fonds de la clientèle.

L'ACPR envisage également d'imposer aux groupes d'activités mixtes le regroupement de leurs activités financières et auxiliaires significatives au sein d'une structure dédiée, afin de permettre une supervision consolidée et le cas échéant, lorsque les activités financières combinées du groupe présentent des risques de nature similaire à ceux d'un établissement de crédit, l'application des règles bancaires à l'ensemble du sous-groupe financier[77]. L'ACPR constate en effet que la structure

[74] *ACPR, op. cit., Le développement des Big Techs dans le secteur financier : quels risques, quelles réponses réglementaires ?, p. 1.*

[75] *Ibid.*

[76] *Ibid.*

[77] *Ibid.*

complexe des grands conglomérats technologiques et plus généralement des grands groupes d'activités mixtes combinée à la prépondérance des activités non financières peuvent faire obstacle à une supervision consolidée en application des règles actuelles. La mise en place d'une telle holding permettrait aux superviseurs de mieux appréhender les activités de chaque groupe, leur interconnexion avec les activités non financières et, partant, leur caractère systémique.

Enfin, l'ACPR envisage de prévoir dès à présent la possibilité pour le superviseur d'imposer l'application des règles prudentielles bancaires à l'ensemble d'un sous-groupe financier, dès lors que les activités financières combinées du groupe présenteraient des risques de nature similaire à une activité d'établissement de crédit ou lorsque qu'un risque pour la stabilité financière serait identifié comme insuffisamment couvert par les exigences individuelles applicables, afin de tenir compte de l'innovation permanente des technologies.

II. Les apports du RIA pour les Institutions Financières

Les Institutions Financières recourent aux outils d'IA depuis bien avant le déploiement du RIA. Dès lors, il faudra que ces outils, pour certains en place depuis des années, s'adaptent à la nouvelle règlementation. À cela, s'ajoute également l'obligation pour les fournisseurs de SIA de maintenir leur système en conformité durant toute la période d'utilisation, ce qui implique des mécanismes de surveillance et d'alerte en continu. Face à ces nouveaux défis, les Institutions Financières, comme l'ensemble des acteurs auxquels le RIA s'applique, bénéficient d'une entrée en application du RIA échelonnée qui permettra aux autorités de réaliser un travail de pédagogie. Ainsi, ce n'est qu'au 2 août 2026 que les dispositions du RIA deviendront applicables dans leur ensemble (à l'exception des règles relatives aux SIA à haut risque de l'annexe 1)[78].

Afin de pouvoir anticiper l'impact du RIA, il est essentiel, pour les acteurs financiers, d'en comprendre précisément le champ d'application pour cette industrie, le contenu des principales obligations, et le rôle qui serait dévolu en la matière aux autorités de surveillance sectorielles.

A. La clarification du champ d'application de l'IA aux secteurs financiers

Le RIA a vocation à réguler les Systèmes d'IA dans le but premier de sauvegarder les droits consacrés dans la Charte des droits fondamentaux de l'Union européenne. Il apparait alors normal que ce règlement ne s'applique pas de la même façon à tous les SIA, mais vise plutôt à encadrer ceux pouvant poser le plus de risques au regard des objectifs poursuivis par le RIA.

De même, ce nouveau règlement a vocation à définir un cadre général compatible avec les évolutions technologiques futures. Il a dû définir les solutions techniques qu'il régit sans reposer uniquement sur les pratiques et techniques développées jusqu'alors. À cet effet, la définition retenue par le RIA, reprend l'approche générale de l'OCDE et pose ainsi des critères précis de caractérisation des SIA, sans viser de méthode ou de techniques spécifiques.

Les Institutions Financières devront alors mener un travail d'analyse au cas par cas pour déterminer si leurs solutions d'IA entrent ou non dans le champ d'application du RIA.

Notons à titre liminaire que le RIA vient aussi encadrer la fourniture de modèle d'IA à usage général[79]. Toutefois, dans la mesure où les Institutions Financières devraient, *a priori*, rarement être qualifiées de fournisseurs de tels modèles, les dispositions du RIA qui s'y rapportent ne seront pas analysées en détail dans le présent rapport.

---

[78] *CNIL, Entrée en vigueur du règlement européen sur l'IA : les premières questions-réponses de la CNIL, 12 juillet 2024.*

[79] *Articles 51 et suivants du RIA.*

1. Une définition centrée sur la génération de sortie

Le RIA adopte une définition spécifique de l'IA qui vise à distinguer les technologies capables de générer des sorties à partir des entrées qu'elles reçoivent des autres types de systèmes logiciels. Les autres éléments caractéristiques fondamentaux d'un Système d'IA sont : (i) le niveau d'autonomie avec lequel il fonctionne (lui permettant de bénéficier « *d'un certain degré d'indépendance dans leur action par rapport à une ingérence humaine et de capacités à fonctionner sans intervention humaine* ») et (ii) sa possible faculté d'adaptation après son déploiement « *liée à des capacités d'auto-apprentissage, qui permettent au système d'évoluer en cours d'utilisation* »[80, 80bis]. Sont ainsi exclus les systèmes de prédiction simples. Par exemple, certains systèmes automatisés de prévision des cours futurs des actions s'appuient sur des méthodes trop simplistes pour être considérées par le RIA, notamment à cause de leur capacité limitée à analyser les tendances et à ajuster leurs résultats de façon autonome[81]. Le même raisonnement s'applique aux systèmes d'estimation statistique qui prédisent, par exemple, un temps de réponse moyen du service client en se basant sur des données passées[82]. Ces deux modèles ne sont finalement pas suffisamment autonomes ou adaptables pour avoir besoin d'être régulés.

Les lignes directrices de la Commission susmentionnées rappellent également les autres critères de qualification à prendre en compte dans la caractérisation des Systèmes d'IA au sens du RIA, à savoir : la nature automatisée du système, les objectifs implicites ou explicites qu'il poursuit, la capacité d'inférence, la nature de ces sorties et leurs capacités à influencer leur environnement[83].

Ces lignes directrices permettent de mieux préciser les caractéristiques que des systèmes doivent satisfaire pour être assujettis au RIA, la Commission soulignant à la fois : la largeur du spectre de solutions potentiellement captées mais aussi le besoin d'une analyse au cas par cas et *in concreto* pour déterminer si le RIA trouve ou non à s'appliquer. Cette évaluation est particulièrement signifiante pour les acteurs financiers, qui ont largement intégré ce type de solutions bien avant l'adoption du RIA. *In fine*, cette définition centrée sur la génération de sorties constitue un cadre de référence essentiel pour déterminer quelles solutions d'IA relèvent du champ d'application du RIA, tout en clarifiant les responsabilités des acteurs dans ces secteurs.

---

[80] *Considérant 12 du RIA.*

[80bis] *Ces termes techniques ont vocation à être précisés par une prochaine publication de la Commission européenne suivant les résultats de la consultation sur les lignes directrices de la définition des SIA et des IA interdites. Voir European Commission releases analysis of stakeholder feedback on AI definitions and prohibited practices public consultations, 12 mai 2025.*

[81] *Commission européenne, Guidelines on the definition of an artificial intelligence system established by Regulation (EU) 2024/1689 (AI Act), lignes directrices, 6 février 2025, paragraphe 50.*

[82] *Ibid, paragraphe 51.*

[83] *Ibid.*

2. Une application extraterritoriale

L'application territoriale du RIA constitue une caractéristique fondamentale du règlement.

Le RIA s'applique à tout système ou modèle d'IA utilisé dans l'Union européenne, indépendamment du lieu où il a été développé ou fourni. Cela signifie que les Systèmes d'IA étrangers produisant des sorties utilisées dans l'UE seront soumis aux exigences du RIA[84]. Tel sera le cas par exemple d'un client français achetant un Système d'IA auprès d'un fournisseur canadien mais utilisant le SIA pour ses opérations internes en France ou encore d'une entreprise en Chine qui utilise une IA pour filtrer les CV et envoie les résultats filtrés à sa filiale luxembourgeoise, qui a l'intention d'utiliser les résultats du SIA pour ses activités dans l'Union européenne.

Si le RIA prévoit explicitement son application aux fournisseurs et aux déployeurs de Systèmes d'IA établis ou situés dans un pays tiers dès lors que les sorties produites par le Système d'IA sont utilisées dans l'Union[85], le considérant n° 22 semble introduire un critère d'intention. Celui-ci précise en effet que le champ du RIA devrait inclure les fournisseurs et déployeurs établis dans un pays tiers, dans la mesure où « *les sorties produites par ces systèmes sont destinées à être utilisées dans l'Union* ». Cette disposition pourrait ainsi justifier que les acteurs de pays tiers ne soient pas assujettis au RIA, même s'ils sont liés à un Système d'IA dont les sorties sont utilisées dans l'UE, si ces systèmes n'étaient pas destinés à cette fin. Toutefois, pour assurer une parfaite sécurité juridique pour les acteurs, en l'absence de clarification dans les dispositions contraignantes du RIA, une telle restriction du champ géographique fondée sur le critère de l'intention pourrait être apportée par la Commission sur les critères de l'application extraterritoriale du RIA.

Le caractère extraterritorial du RIA pourrait également compliquer l'utilisation de solutions développées dans des juridictions non alignées sur les standards européens, ce qui soulève des défis pour les Institutions Financières souhaitant adopter des Systèmes d'IA innovants provenant de l'étranger. Ces contraintes nécessiteront des ajustements contractuels ainsi que des mécanismes de *due diligence* approfondis pour garantir la conformité tout au long de la chaîne d'approvisionnement. À ce titre, la Commission européenne a récemment publié des modèles de clauses contractuelles types pour les marchés publics relatifs à l'IA par les organismes publics. Bien que destinées aux organismes publics qui achètent des Systèmes d'IA développés ou à développer par un fournisseur externe, ces clauses favorables aux acheteurs peuvent également être une source d'inspiration pour les Institutions Financières[86].

3. Une classification par les risques

L'approche retenue par le RIA est fondée sur les risques. Le RIA prévoit de ce fait un régime progressif d'obligations selon le degré de risque posé par le Système d'IA pour la santé, la sécurité et les droits fondamentaux.

---

[84] *Article 2.1 du RIA.*

[85] *Article 2 du RIA.*

[86] *Commission européenne, Procurement of AI, Updated EU AI model contractual clauses, 5 mars 2025.*

Les Systèmes d'IA utilisés par les Institutions Financières seront catégorisés selon que le risque est inacceptable, élevé, spécifique ou minimal. Un important travail de cartographie des solutions d'IA intégrées dans les organisations des Institutions Financières devra être mis en place pour distinguer les niveaux de risques et les exigences spécifiques leur étant applicables, suivant les usages considérés.

3.1 - Systèmes d'IA à risque inacceptable

Le RIA énumère limitativement les Systèmes d'IA prohibés car faisant courir un risque jugé inacceptable en raison de leur nature[87].

Aucun cas d'usage dans le secteur bancaire et financier ne semble être expressément visé au sein de cette catégorie. Cependant, la mise en œuvre de certaines catégories de systèmes peut s'avérer délicate pour l'industrie financière. Notamment, le RIA interdit les Systèmes d'IA qui exploitent les éventuelles vulnérabilités dues à l'âge, au handicap ou à la situation sociale ou économique spécifique d'une personne d'une manière qui est raisonnablement susceptible de causer un préjudice important à cette personne[88].

À cet égard, les lignes directrices de la Commission européenne publiées en février 2025[89] précisent que les Systèmes d'IA utilisés pour fournir des services bancaires, tels que des hypothèques et des prêts, utilisant l'âge ou la situation socio-économique spécifique du client, dans le respect de la législation de l'Union européenne, ne constituent pas une pratique interdite « *lorsqu'elles sont conçues pour protéger et soutenir les personnes identifiées comme vulnérables en raison de leur âge, de leur handicap ou de leur situation socio-économique spécifiques et sont bénéfiques pour ces groupes, contribuant également à des services financiers plus équitables et plus durables pour ces groupes* » (traduction non-officielle).

En revanche, un Système d'IA qui ciblerait les personnes âgées avec des offres d'assurance en exploitant leur capacité cognitive réduite pourrait relever des pratiques interdites par le RIA et être de fait prohibé[90].

De même, une autre pratique interdite par le RIA vise les Systèmes d'IA qui reposeraient sur des collectes de données sur le comportement social ou les caractéristiques personnelles utilisées à des fins décorrélées du contexte de collecte desdites données (aussi appelée « *social scoring* »),

[87] *Article 5 du RIA.*

[88] *Article 5(1)b du RIA.*

[89] *Commission européenne, Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act), 4 février 2025, paragraphe 133.*

[90] *Ibid, paragraphe 117.*

par exemple dans le cadre de certaines prestations financières. L'intégration de ces données par un Système d'IA pourrait relever de la catégorie des Systèmes d'IA à risque inacceptable si le système en déduit un « *traitement préjudiciable ou défavorable* » dans un contexte autre que celui dans lequel les données ont été collectées ou si ce traitement est « *préjudiciable ou défavorable* » de manière disproportionnée ou injustifiée[91]. Si le RIA rappelle que cette disposition n'est pas censée avoir « *d'incidence sur les évaluations licites des personnes physiques qui sont pratiquées dans un but précis, dans le respect du droit de l'Union et du droit national* »[92], le périmètre des cas d'usage qui seront désormais interdits n'est pas précisément défini au sein du texte. Une clarification concernant l'appréciation de ces situations visées aux articles 5.1.c (i) et (ii) du RIA permettrait de donner une meilleure visibilité sur les cas d'utilisation dans le secteur bancaire et financier entrant ou non dans leurs champs.

À cet égard, les lignes directrices susmentionnées de la Commission apportent des précisions utiles. Elles indiquent par exemple que sur ce fondement, doivent être interdits :

- l'utilisation par une compagnie d'assurance d'un Système d'IA recommandant de refuser un contrat ou de fixer des primes d'assurance-vie plus élevées pour une personne pour laquelle ladite compagnie aurait collecté des informations sur les dépenses et d'autres informations financières qui ne sont pas liées à la détermination de l'éligibilité de ce candidat à l'assurance-vie et la détermination de la prime pour cette assurance[93] ; et

- le recours par établissement de crédit à un Système d'IA pour déterminer la solvabilité des personnes et l'accès à un crédit immobilier sur la base de caractéristiques personnelles non liées[94].

En revanche, cette disposition du RIA ne remet pas en cause les Systèmes d'IA permettant l'évaluation de personnes à des fins légitimes spécifiques entraînant un traitement potentiellement préjudiciable ou défavorable si celui-ci est justifié et proportionné et que des données provenant de contextes sociaux connexes sont utilisées[95].

Typiquement, les informations collectées par des appareils embarqués sur un véhicule, qui démontreraient qu'un conducteur ne respecte pas des pratiques de conduite sûres, pourraient être utilisées par l'assureur pour augmenter la prime de cet assuré en raison du risque plus élevé d'accident, à condition que l'augmentation de la prime soit proportionnée au comportement à risque du conducteur.

---

[91] *Article 5(1)c (i) et (ii) du RIA.*

[92] *Considérant 31 du RIA*

[93] *Commission Européenne, op. cit., Guidelines on prohibited artificial intelligence practices, paragraphe 170.*

[94] *Ibid.*

[95] *Ibid.*

Malgré les clarifications de la Commission européenne, les cas d'usage susceptibles d'être considérés comme interdits restent définis très largement. Une approche plus restrictive des dispositions du RIA permettrait de ne pas trop entraver significativement la capacité des Institutions Financières d'explorer les opportunités que l'IA peut générer dans leur secteur.

3.2 - Systèmes d'IA à risque élevé

Le RIA dresse une liste exhaustive des cas d'usage de SIA devant être considérés comme à haut risque. Certains de ces cas d'usage sont spécifiques au secteur financier. Ces derniers bénéficient potentiellement du mécanisme d'exemption prévu par le RIA. À défaut, ils devront se soumettre à des exigences particulièrement renforcées.

(i) Les systèmes de credit scoring et de tarification en matière d'assurance-vie et d'assurance maladie

Le RIA autorise, mais soumet à un régime strict, le recours à des Systèmes d'IA à haut risque, définis expressément dans le texte.

Deux cas d'usages visent particulièrement les acteurs du secteur bancaire et financier :

- Les Systèmes d'IA permettant l'évaluation de la solvabilité des personnes physiques ou l'établissement de leur note de crédit[96]

Ces Systèmes d'IA déterminent entre autres l'accès des personnes physiques aux ressources financières ou à d'autres services essentiels (logement, électricité et services de télécommunication) pouvant conduire à créer ou perpétuer des schémas de discrimination entrant dans la catégorie des Systèmes d'IA à haut risque[97].

Le champ d'application du RIA n'est pas limité par une référence spécifique au statut règlementaire de l'acteur qui aurait vocation à déployer de telles solutions. Le régime prévu par le RIA pourrait donc devoir être respecté par les établissements de crédit mais aussi par l'ensemble des acteurs intervenant dans l'octroi de crédit à des personnes physiques et susceptibles d'intégrer ce type d'outil (qu'il s'agisse des prêteurs mais également de tout intermédiaire dans la chaîne d'octroi de prêt à l'instar des intermédiaires en opérations de banque et de servies de paiement, voire potentiellement des prestataires technologiques).

[96] *Article 5(b) Annexe III du RIA.*

[97] *Considérant 58 du RIA.*

- Pour les assurances, les Systèmes d'IA destinés à être utilisés pour l'évaluation des risques et la tarification en ce qui concerne les personnes physiques en matière d'assurance-vie et d'assurance maladie[98]

En raison de leur potentielle incidence significative sur les conditions de vie des bénéficiaires d'assurances-vie et d'assurances santé, la conception, le développement et l'utilisation de ces Systèmes d'IA peuvent porter atteinte à leurs droits fondamentaux, entrainant ainsi des risques d'exclusion financière ou de discrimination nécessitant une vigilance accrue du régulateur.

À noter que dans son « *Factsheet* » sur le cadre réglementaire de l'IA en assurance, l'EIOPA rappelle que si le RIA introduit des exigences supplémentaires pour les fournisseurs ou les déployeurs de Systèmes d'IA à risque élevé, « *l'ensemble de la législation assurantielle continuera de s'appliquer à tous les cas d'usage, quelle que soit leur qualification au titre du RIA* »[99].

Notons que le RIA prévoit expressément la faculté pour la Commission européenne de réviser la liste des cas d'utilisation de Systèmes d'IA à haut risque lorsque le Système d'IA en question est destiné à être utilisé dans un des domaines spécifiés à l'Annexe III du RIA[100]. Puisque le *credit scoring* et la tarification en matière d'assurance-vie et d'assurance-maladie sont bel et bien des domaines spécifiés à l'annexe III du RIA, la Commission pourrait potentiellement étendre la liste à d'autres cas d'usage qui pourraient apparaître dans l'univers financier et qui se révèleraient particulièrement risqués, par exemple du point de vue de la protection des clients ou pour la stabilité des marchés, dans l'hypothèse où la Commission parviendrait à rattacher cette dernière notion à la protection de la santé, de la sécurité et des droits fondamentaux[101].

(ii) Les exemptions et le mécanisme de l'opt out

Certains Systèmes d'IA, soit compte tenu de leur objectif, soit parce qu'ils font déjà l'objet d'un encadrement précis par une autre réglementation, devraient en principe être exclus de la catégorie des Systèmes d'IA à haut risque au titre du RIA, alors même qu'ils auraient pu être qualifiés comme tels au sens du RIA. Tel est le cas des Systèmes d'IA utilisés aux fins de détecter les fraudes dans l'offre de services financiers et à des fins prudentielles pour calculer les besoins en fonds propres des établissements de crédit et des compagnies d'assurance, dans la mesure où ils sont encadrés par le droit de l'Union[102].

---

[98] *Article 5(c), annexe III du RIA.*

[99] *EIOPA, Regulatory framework applicable to AI systems in the insurance sector, juillet 2024.*

[100] *Article 7.1 du RIA.*

[101] *Article 1(1) du RIA.*

[102] *Considérant 58 du RIA.*

Toutefois, le champ exact de l'exemption pour la détection de la fraude financière demeure flou[103]. En particulier, il serait utile de confirmer dans quelle mesure les Systèmes d'IA utilisés aux fins de la lutte contre le blanchiment de capitaux et le financement du terrorisme ou aux fins de prévention des abus de marché bénéficient d'une telle exemption. La portée de l'exclusion des Systèmes d'IA utilisés à des fins prudentielles pour calculer les exigences de fonds propres de certaines Institutions Financières prévue par le considérant n° 58 du RIA manque également de clarté dans la mesure où elle n'est pas davantage précisée par d'autres dispositions du RIA. Son articulation avec l'inclusion des « *systèmes d'IA destinés à être utilisés pour évaluer la solvabilité des personnes physiques ou pour établir leur note de crédit* » dans la liste des Systèmes d'IA à haut risque prévue à l'annexe III du RIA soulève également des questions (voir sur ce point le paragraphe 5 ci-après relatif à l'articulation du RIA avec la réglementation prudentielle).

De plus, à travers le mécanisme de l'*opt out*, un Système d'IA visé à l'annexe III du RIA n'entre pas dans la catégorie des Systèmes d'IA à haut risque lorsqu'il ne présente pas de risques importants de préjudice pour la santé, la sécurité ou les droits fondamentaux des personnes physiques[104]. Si les conditions déterminant l'application du mécanisme de l'*opt-out* sont clairement et limitativement énumérées, il subsiste des incertitudes quant aux cas d'usage concrets pouvant bénéficier de cette exemption dans le secteur bancaire et financier.

Ainsi, s'agissant d'un système permettant l'évaluation de la solvabilité du client par le Système d'IA d'une banque, selon le dispositif dans lequel il s'insère, il pourrait ne pas se contenter de réaliser une « *tâche procédurale étroite* »[105] ni d'« *améliorer le résultat d'une activité humaine préalablement réalisée* »[106]. Dans ce cas, il ne pourrait pas être exempté sur la base de ces fondements. En revanche, s'il est utilisé uniquement pour « *exécuter une tâche préparatoire* »[107] en vue de déterminer le risque de défaillance potentiel du client, ou encore permettre de « *détecter les constantes en matière de prise de décision ou les écarts par rapport aux constantes habituelles antérieures* »[108]

---

[103] *L'annexe III du RIA qui répertorie les Systèmes d'IA à haut risque visés l'article 6(2) du RIA (sous réserve que ne trouve à s'appliquer la dérogation prévue à l'article 6(3) du RIA ou mécanisme d'opt-out)) prévoit au paragraphe 5(b) que sont considérés comme des Systèmes d'IA à haut risque les « systèmes d'IA destinés à être utilisés pour évaluer la solvabilité des personnes physiques ou pour établir leur note de crédit, à l'exception des systèmes d'IA utilisés à des fins de détection de fraudes financières ». Tel que prévu à l'annexe III du RIA, l'exclusion des Systèmes d'IA utilisés aux fins de la détection des fraudes financières de la catégorie des Systèmes d'IA à haut risque contribue à entretenir le flou sur la portée exacte de l'exclusion plus qu'il ne l'éclaire compte tenu de la syntaxe du paragraphe 5(b) (qui pourrait laisser envisager une lecture dans la perspective de la proposition incise qui précède).*

[104] *Article 6(3) du RIA.*

[105] *Article 6(3)(a) du RIA.*

[106] *Article 6(3)(b) du RIA.*

[107] *Article 6(3)(d) du RIA.*

[108] *Article 6(3)(c) du RIA.*

pour dresser un profil type de note de crédit acceptable pour l'Institution Financière en question il serait alors exempté du régime applicable aux Systèmes d'IA à haut risque. Cette appréciation devra être menée in concreto selon les besoins exacts pour lesquels le Système d'IA est utilisé.

On peut espérer une clarification prochaine du mécanisme d'*opt-out* afin de mieux apprécier le périmètre des Systèmes d'IA à haut-risque à considérer.

(iii) Des contraintes spécifiques pour les Systèmes d'IA à risque élevé dans le secteur bancaire et financier

Les cas d'usage visés ci-dessus, considérés comme présentant un risque élevé, font partie des seules hypothèses où le déployeur d'un Système d'IA doit, avant le premier déploiement, procéder à une analyse d'impact de ces systèmes concernant les droits fondamentaux avant de les mettre en service[109]. On peut s'interroger sur les raisons pour lesquelles seul le secteur bancaire et assurantiel, parmi l'ensemble des cas d'usage régis par le texte et déployés sans lien avec le secteur public, s'est vu assujettir à cette obligation. On peut certainement y déceler une vigilance particulière de la part des autorités financières sur l'accès aux prestations fournies par ces industries.

3.3 - Systèmes d'IA dit « *à risque spécifique* » interagissant directement avec des personnes physiques

S'ils ne sont pas considérés comme présentant des risques inacceptables ou élevés, de nombreux cas d'usage dans le domaine bancaire et financier entreront dans la catégorie des systèmes présentant un risque spécifique car interagissant directement avec des personnes physiques ou générant des contenus de synthèse[110]. Notons que la notion de « *Système d'IA à risque spécifique* » n'est pas définie en tant que telle dans le RIA mais désigne ici la catégorie de systèmes qui ne seraient pas captés par les cas d'usage à risques inacceptables ou élevés mais qui présentent des risques d'usurpation d'identité ou de tromperie à cause de leurs interactions directes avec l'utilisateur[111]. Sous l'égide du Bureau de l'IA, des bonnes pratiques pourraient être également développées pour respecter ces exigences[112], par exemple au niveau de l'industrie via des chartes professionnelles.

Les Institutions Financières déployant par exemple des *chatbots*, des systèmes d'analyse du langage ou encore des systèmes d'analyse des habitudes et de l'amélioration de l'expérience client devront,

[109] *Article 27 du RIA.*

[110] *Article 50 du RIA.*

[111] *Considérant 132 du RIA.*

[112] *Article 50(4) du RIA.*

dès la conception du produit, permettre d'informer l'utilisateur afin qu'il comprenne qu'il interagit avec un Système d'IA et/ou que les informations lui étant présentées ont été générées et manipulées par un Système d'IA.

3.4 - Systèmes d'IA à risque minimal ou nul

Enfin, le RIA autorise la libre utilisation de l'IA à risque minimal. C'est une catégorie résiduelle des Systèmes d'IA. Sont inclus ici tous ceux ne correspondant à aucune autre classification. Ces IA ne nécessitent pas de se conformer à des exigences particulières et représentent la grande majorité des systèmes actuellement utilisés dans l'UE. En font partie les jeux vidéo ou les filtres anti-spam. Des bonnes pratiques pourraient là encore être également développées au niveau de l'industrie via des chartes professionnelles pour aider les acteurs à se structurer.

B. Création de nouvelles obligations liées aux usages de l'IA

1. Quatre statuts possibles pour les Institutions Financières

Le RIA envisage plusieurs catégories auxquelles sont attachées des obligations différentes. Une analyse approfondie et au cas par cas sera ainsi nécessaire pour déterminer le statut et les obligations afférentes. Il définit quatre statuts d'acteurs principaux[113] :

Le fournisseur d'IA est le premier acteur dans la chaîne de valeur des SIA régulé par le RIA. Il est « *une personne physique ou morale, une autorité publique, une agence ou tout autre organisme qui développe ou fait développer un système d'IA ou un modèle d'IA à usage général et le met sur le marché ou met le système d'IA en service sous son propre nom ou sa propre marque, à titre onéreux ou gratuit* ». Il semblerait que les Institutions Financières, même si elles ne relèvent pas à titre principal de ce statut puisque leur activité principale ne consiste pas a priori à développer des Systèmes d'IA, peuvent assez facilement entrer dans cette catégorie par exemple si elles font développer un Système d'IA par un prestataire pour le mettre en service. De plus, un distributeur, importateur ou déployeur (tels que défini ci-dessous) pourra être considéré comme un fournisseur d'IA à haut risque s'il apporte « une modification substantielle à un système d'IA à haut risque qui a déjà été mis sur le marché ou a déjà été mis en service » ou bien s'il en modifie la destination[114].

Le déployeur d'IA est « *une personne physique ou morale, une autorité publique, une agence ou un autre organisme utilisant sous sa propre autorité un système d'IA […]* ». Autrement dit, il s'agit de

[113] *Article 3 du RIA.*

[114] *Article 25(1)(b) et (c) du RIA.*

l'utilisateur usant de l'IA à des fins professionnelles. Les Institutions Financières devraient relever plus généralement de cette catégorie, sauf si elles choisissent plus fréquemment de développer ou de faire développer le Système d'IA pour un usage sur mesure. Par exemple, les Institutions Financières seront déployeurs de leur outil de gestion RH si celui-ci est un Système d'IA et qu'elles l'utilisent dans leurs organisations pour gérer, par exemple, leur masse salariale.

L'importateur d'IA est toute personne établie dans l'UE qui met sur le marché un Système d'IA portant le nom ou la marque d'une personne établie en dehors de l'UE. Il peut être une banque française qui achète un logiciel d'IA développé en Chine pour le mettre sur le marché européen.

Le distributeur d'IA est une personne physique ou morale qui met à disposition un Système d'IA dans la chaîne d'approvisionnement, sans en modifier les propriétés. Il peut être une société française qui rachète puis distribue un logiciel d'IA déjà présent dans l'UE à ses succursales. Il met à disposition le produit sans le modifier. On peut aussi considérer que pourrait être qualifiée de distributeur la maison mère d'un groupe financier européen qui acquiert un Système d'IA auprès d'un fournisseur pour que ce SIA soit déployé par les filiales européennes du groupe.

Les différentes obligations contenues dans le RIA dépendant, pour partie, de la catégorie à laquelle appartient l'opérateur d'IA, la qualification est en effet importante afin de déterminer la nature et l'étendue des exigences qui devront être satisfaites. L'exercice de qualification du rôle qu'occupe une Institution Financière doit être mené avec précision, en notant que les différentes catégories mentionnées ci-dessus ne sont pas exclusives. Ainsi une même entité peut par exemple être à la fois distributeur et déployeur, dès lors qu'elle met un Système d'IA à disposition sur le marché de l'Union et qu'elle l'utilise simultanément sous sa propre autorité. Dans cette hypothèse, les exigences afférentes à chaque statut devraient s'appliquer de manière cumulative. Au-delà, notons que le RIA n'introduit aucun régime dérogatoire pour la fourniture de système ou de modèle d'IA au sein d'un même groupe.

Ainsi, le recours à des solutions d'IA au sein d'un même groupe financier pourrait entraîner la caractérisation de différents statuts au sens du RIA pour les entités du groupe, avec un ensemble d'obligations variables selon le statut applicable à chaque entité.

2. Des obligations et régimes de responsabilité spécifiques propres à chaque statut

Des obligations de transparence et de conformité au RIA doivent être observées par les Institutions Financières lorsqu'elles développent et fournissent, importent ou déploient de l'IA.

Les obligations sont nombreuses et, comme indiqué plus haut, dépendent de la qualification retenue pour l'Institution Financière concernée. Il est à noter que le RIA contient un certain nombre de

dispositions destinées à intégrer les obligations qu'il édicte dans le cadre et les obligations déjà prévues pour les établissements fournissant des services financiers.

Les obligations des fournisseurs et/ou déployeurs d'IA à haut risque figurent aux articles 8 et s. du RIA (maîtrise de l'IA, existence d'un système de gestion des risques, exigences quant aux données employées et quant à la gouvernance desdites données, documentation technique, enregistrement, transparence et fourniture d'informations aux déployeurs, contrôle humain, exactitude, robustesse et cybersécurité…, conservation de documents, journaux générés automatiquement, mesures correctives et devoir d'information…).

Les obligations définies pour chaque statut répondent à celles imposées aux autres catégories d'acteurs de la chaîne de valeur des SIA définies dans le RIA. Ainsi, par exemple, si l'interdiction de certaines pratiques en application de l'article 5 du RIA vise de manière évidente les déployeurs, les lignes directrices de la Commission européenne précisent qu'il est attendu des fournisseurs qu'ils prennent des mesures raisonnables pour que leur SIA, y compris les SIA à usage général dont on peut raisonnablement penser qu'ils peuvent être utilisés pour un cas d'usage interdit, ne puissent être déployés pour de telles finalités[115].

En outre, tout manquement d'un des acteurs de la chaîne de valeur des SIA à ses obligations au titre du RIA pourrait ainsi impacter la capacité des autres, impliqués dans le développement, la mise sur le marché ou le déploiement d'un même SIA, à satisfaire les leurs. La responsabilité encourue pour manquement aux exigences du RIA (entraînant des sanctions pouvant aller jusqu'à 7% du chiffre d'affaires annuel mondial ou 35 millions d'euros selon le manquement[116]) devra, dans cette hypothèse, être articulée avec la responsabilité contractuelle et extracontractuelle susceptible d'être engagée par l'acteur impliqué.

C. Reconnaissances des autorités de surveillance existantes

Pour assurer une mise en œuvre harmonisée et efficace des obligations du RIA, un réseau d'autorités compétentes, nationales et européennes, a été institué.

1. Les autorités compétentes au titre du RIA

Le RIA prévoit lui-même différentes institutions publiques, nationales et européennes, en charge de la mise en œuvre du nouveau règlement.

Le RIA creé deux organismes européens chargés de l'interprétation et de la mise en place du RIA, tous deux possédant des pouvoirs et une autorité variable.

---

[115] *Commission Européenne, op. cit., Guidelines on prohibited artificial intelligence practices, paragraphe 40.*

[116] *Article 99(3) du RIA.*

- Le Bureau européen de l'IA (« *AI Office* ») est un organe dépendant de la Commission. Il contribue à la mise en œuvre stratégique, cohérente et efficace du RIA et possède à ce titre un certain nombre de pouvoirs, notamment d'enquête[117], surtout en termes de SIA à usage général[118]. Au Bureau de l'IA sera greffé le « *AI Act Service Desk* », un centre d'information sur le RIA, permettant aux parties de demander de l'aide et de recevoir des réponses sur mesure[119].

- Enfin, le Comité IA (« *AI Board* ») fournira des recommandations sur l'application du RIA. Y siègent des représentants de tous les États membres. Il s'assure ainsi principalement de l'harmonisation de l'application du RIA à travers l'Europe.

Le RIA impose également à chaque État membre de désigner différentes autorités nationales compétentes[120], incluant l'autorité de contrôle nationale, responsable de l'application générale du RIA et agissant en tant que point de contact avec les différentes autorités nationales ; l'autorité de surveillance des marchés, chargée de vérifier la conformité des Systèmes d'IA mis sur le marché ; et l'autorité « *notifiante* », qui joue un rôle clé dans la désignation et la notification des organismes d'évaluation de la conformité des Systèmes d'IA.

La désignation de ces nouvelles compétences doit s'articuler avec le rôle existant des autorités sectorielles en charge de la supervision du secteur financier. Par exemple, la Banque centrale européenne conserve ses fonctions de surveillance prudentielle concernant les processus de gestion des risques et les mécanismes de contrôle interne des établissements de crédit[121].

L'un des enjeux majeurs de ce cadre global et des différentes compétences ainsi définies est l'harmonisation des approches entre les autorités ayant la compétence de principe avec celles compétentes pour le secteur financier, ce au niveau national comme au niveau européen. Cela est particulièrement critique pour les Institutions Financières, car les divergences entre régulateurs pourraient compliquer les opérations transfrontalières et les exigences spécifiques au RIA doivent être intégrées aux régulations sectorielles sans créer de conflits ou de doublons.

2. Le cas de la France

Pour l'instant, la France ne semble pas avoir désigné la ou les autorités compétentes pour superviser l'usage de l'IA par les Institutions Financières à l'aune également des réglementations sectorielles. Il convient de se référer au considérant n° 158 et à l'article 74(6) du RIA. Afin d'assurer la cohérence

[117] *Voir article 64 RIA et Décision de la Commission, Decision establishing the European Artificial Intelligence Office C(2024) 390, 24 janvier 2024 pour une vision plus détaillée des pouvoirs du Bureau Européen de l'IA.*

[118] *Considérant 163 et article 75 du RIA.*

[119] *Dévoilé par la Commission européenne dans son AI Continent Action Plan, 9 avril 2025, p. 21.*

[120] *Article 59 du RIA.*

[121] *Considérant 158 RIA.*

et le respect du RIA par les services financiers, les États devront désigner les autorités compétentes, dans les limites de leurs compétences respectives, y compris pour les activités de surveillance de marché[122].De plus, y sont explicitement mentionnées les autorités financières compétentes au titre du règlement sur les exigences prudentielles applicables aux établissements de crédit (CRR) et des directives sur le crédit à la consommation (2008/48/CE), sur l'accès à l'activité des établissements de crédit (CRD) et sur les contrats de crédit aux consommateurs relatifs aux biens immobiliers à usage résidentiel (2014/17/UE).

Les prérogatives de ces autorités devraient comprendre « *le pouvoir d'effectuer des activités de surveillance du marché ex post qui peuvent être intégrées, le cas échéant, dans leurs mécanismes et procédures de surveillance existants au titre du droit de l'Union en matière de services financiers* ».

De plus, pour les SIA à haut risque du secteur financier, « *l'autorité de surveillance du marché aux fins du présent règlement est l'autorité nationale responsable de la surveillance financière de ces établissements* »[123]. Il est néanmoins possible pour les Etats membres de déroger à cette disposition et de désigner une autre autorité compétente[124].

À ce jour, la France semble opter pour une répartition des pouvoirs entre plusieurs autorités existantes plutôt que d'en créer une nouvelle. À ce titre, l'ACPR sera chargée de superviser l'application du RIA pour le secteur financier, y compris pour les banques de taille significatives. Cette dernière se prépare donc à développer des mécanismes d'audit *ad hoc* pour les SIA[125].

Un des objectifs majeurs de la répartition des compétences devrait être de concilier le besoin d'harmonisation des approches des autorités, comme suggéré ci-dessus, avec l'impératif de ne pas complexifier le cadre institutionnel accompagnant la mise en œuvre du RIA pour les Institutions Financières. La priorité devrait être de confier la mise en œuvre du RIA par les Institutions financières aux autorités dotées de ressources et de compétences techniques appropriées, proches des enjeux spécifiques du secteur financier, et capables de répondre rapidement aux interrogations des acteurs sur des problématiques souvent sophistiquées.

[122] *Ibid.*

[123] *Article 74(6) du RIA.*

[124] *Article 74(7) du RIA.*

[125] *ACPR, Intelligence Artificielle : quel impact à l'ACPR ? Revue de l'ACPR, 5 juillet 2024.*

III. La nécessité d'articuler le RIA avec les autres réglementations des Institutions Financières

Le législateur européen, par le RIA, vise à instaurer un cadre juridique harmonisé à l'échelle européenne pour promouvoir le développement, l'utilisation et l'adoption de l'IA sur l'ensemble du marché intérieur[126]. Cependant, ce cadre juridique transversal est susceptible de se superposer avec les réglementations existantes applicables aux Institutions Financières à plusieurs égards. Il en résulte une problématique concernant l'articulation et l'interaction entre ce nouveau corpus de règles et les réglementations préexistantes, notamment celles régissant les données (e.g. DORA, NIS 2, RGPD)[127], ainsi que les règles spécifiques aux Institutions Financières.

A. Interactions entre la réglementation sur l'IA et les réglementations sectorielles

1. Une approche générale de complémentarité du RIA aux réglementations sectorielles

Le législateur européen souhaite, à travers le RIA, établir un cadre et une articulation cohérente du RIA avec les règles sectorielles. Plus précisément, le législateur précise, dans le considérant n° 158 du RIA, sur certaines exigences du RIA, qu' « *il convient d'intégrer certaines des obligations [du RIA]* », tandis que pour d'autres, il appelle à « *éviter les chevauchements* » notamment par la mise en place de dérogations[128].

Ce dernier considérant vise spécifiquement le secteur bancaire et financier mais cette volonté de cohérence du législateur semble plus globale car nous constatons également que le considérant n° 64 du RIA envisage l'hypothèse où le présent règlement suppose à ce qu'il « *implique d'appliquer conjointement et de manière complémentaire les divers actes législatifs* »[129] ; tandis que le considérant n° 81 évoque une « *complémentarité entre le présent règlement et le droit sectoriel existant de l'Union [qui] devrait également être prise en compte dans les futures activités ou orientations de normalisation de la Commission*. »[130].

Cette volonté législative était également manifeste dans la consultation ciblée lancée par la Commission européenne sur l'IA dans le secteur financier. La Commission européenne explique expressément en introduction que le RIA est conçu pour compléter l'acquis existant en matière de services bancaires et financiers – même si la réglementation sectorielle ne vise pas spécifiquement

[126] *Considérant 8 du RIA.*

[127] *Veuillez-vous référer au paragraphe B du présent Rapport.*

[128] *Considérant 158 du RIA.*

[129] *Considérant 64 du RIA.*

[130] *Considérant 81 du RIA.*

à régir cette technologie – notamment en posant un cadre pour la gestion du risque lié à l'IA et certaines exigences spécifiques à l'IA que les Institutions Financières devraient prendre en compte pour l'exploitation de cette technologie[131].

L'approche retenue par le RIA nous semble ainsi relativement claire : le corps de règles trans-sectoriel posé par le RIA doit tenir compte des spécificités du secteur bancaire et financier pour leur mise en œuvre au sein des Institutions Financières. En d'autres termes, le RIA complète le cadre législatif existant en matière bancaire et financière et n'entend pas s'y substituer.

2. Des exigences spécifiques en matière de gouvernance à intégrer

De cette approche de complémentarité, nous relevons que le RIA reconnaît soit l'équivalence entre ses dispositions et celles de la réglementation sectorielle, soit précise comment concilier l'obligation du RIA avec celle issue de la réglementation sectorielle.

Le RIA complète, à d'autres égards, les réglementations sectorielles en imposant des exigences de gouvernance.

2.1 - Les reconnaissances d'équivalence ou de complémentarité en matière de gouvernance

(i) Les formes de reconnaissance d'équivalence

Nous constatons que le RIA initie des reconnaissances d'équivalences entre certaines de ses exigences et les règles établies par la réglementation sectorielle. En plusieurs dispositions et termes similaires, le RIA dispose, par un jeu de double condition, que si les fournisseurs/déployeurs sont (i) des « *établissements financiers* » et (ii) qu'à ce titre, ils sont « *soumis à des exigences relatives à leur gouvernance, à leurs dispositifs ou à leurs processus internes prévues par la législation de l'Union sur les services financiers* », alors la conformité à ce dernier ensemble de règles sectorielles « *vaut respect de l'obligation* » posée par le RIA.

Cette reconnaissance d'équivalence appelle deux remarques préliminaires :

- sur la définition d'« *établissement financier* » : d'aucuns pourraient, de prime abord, considérer que la qualification d'« *établissement financier* » fait directement référence à celle posée par l'article 4, paragraphe 1, point 26) du CRR. Cependant, il ne nous semble pas que les établissements de crédit

[131] *Commission européenne, Consultation document – Targeted consultation on artificial intelligence in the financial sector, 18 juin 2024, p. 3.*

et les entreprises d'investissement de classe 1 soient exclus du champ de cette reconnaissance d'équivalence. Cela contredirait la philosophie d'harmonisation et de complémentarité voulue par le législateur européen qui, à plus forte raison, vise directement cette idée de reconnaissance d'équivalence dans le considérant n° 158, en disposant que le RIA devrait permettre « *des dérogations limitées* » pour les établissements de crédit et autres établissements financiers ;

- sur l'interprétation donnée de la « *législation de l'Union sur les services financiers* » : l'expression usitée par le RIA de « *législation de l'Union sur les services financiers* », ne devrait pas être interprétée comme excluant les services bancaires, pour les mêmes raisons évoquées au point précédent.

En conséquence, il nous semble que le sens des dispositions sur les reconnaissances d'équivalence doit permettre qu'une Institution Financière, déjà soumise à un certain nombre de règles de gouvernance, dispositifs ou processus internes aux termes de son statut réglementaire, soit réputée répondre aux dispositions visées par le RIA.

Il convient également de préciser que le RIA semble bien admettre des reconnaissances d'équivalence par ces dispositions et non une subordination à ces dispositions. En effet, admettre que les dispositions permettent une subordination du RIA par les règles sectorielles reviendrait à écarter totalement certaines règles spécifiques du RIA. Cela ne semble pas être le cas ici, car même si le cadre réglementaire sectoriel permet aux Institutions Financières de se conformer favorablement aux exigences du RIA, il ne s'y substitue pas. Les Institutions Financières devront en tenir compte lorsqu'elles répondent aux exigences de leur propre réglementation sectorielle jugée équivalente. En d'autres termes, l'adage *specialia generalibus derogant* voulant que les lois spéciales (i.e. la réglementation sectorielle) dérogent aux lois générales (i.e. le RIA) ne devrait pas trouver directement à s'appliquer.

Une pleine et entière reconnaissance d'équivalence est ainsi notable s'agissant de l'obligation de surveillance du fonctionnement du Système d'IA à haut risque sur la base de la notice d'utilisation[132]. L'obligation d'information en cas d'incident grave[133] lors de l'utilisation de ce Système d'IA pourrait être remplie par la notification des incidents opérationnels majeurs à l'ACPR par les dirigeants effectifs[134], sous réserve de notifier les autres personnes visées par la disposition du RIA.

[132] *Article 26(5) du RIA.*

[133] *Ibid.*

[134] *Article 249-1 de l'Arrêté du 3 Novembre 2014 et Article L. 521-10 du CMF.*

(ii) Des reconnaissances de complémentarité des règles

S'agissant de la complémentarité des règles du RIA avec celles de la réglementation sectorielle, le RIA la reconnaît d'abord en matière de conservation des documents. Les Institutions Financières fournissant des Systèmes d'IA à haut risque peuvent ainsi s'appuyer sur leurs systèmes existants pour satisfaire à leurs obligations de conservation des documents en vertu du RIA. Les Institutions Financières devront, à ce titre, tenir à jour leur documentation technique sur l'IA[135]. Pour les établissements de crédit, cette documentation technique pourrait être intégrée dans les manuels de procédures qui décrivent les activités de l'entité[136].

Pour ces mêmes entités, le RIA admet également une reconnaissance de complémentarité de la réglementation sectorielle concernant les journaux générés automatiquement[137], les systèmes de surveillance et les plans de surveillance après commercialisation[138].

(iii) Les reconnaissances d'équivalence partielle

L'article 17 du RIA dispose que les fournisseurs de Systèmes d'IA à haut risque doivent mettre en place des systèmes de gestion de la qualité, impliquant la rédaction de politiques et procédures précises afin de respecter les prescriptions du RIA. Toutefois, les Institutions Financières fournissant un tel système bénéficient d'une reconnaissance d'équivalence de leur réglementation sectorielle, à l'exception des prescriptions développées aux points g), h) et i) du paragraphe 1 de cet article 17. La reconnaissance d'équivalence n'est alors que partielle.

Ainsi, en ce qui concerne le système de gestion des risques[139], l'élaboration, la mise en œuvre et le fonctionnement des systèmes de surveillance post-commercialisation[140] (étant précisé que, comme précédemment expliqué, l'article visant cette obligation permet aux Institutions Financières d'intégrer les obligations en matière de surveillance pré-commercialisation dans les systèmes et plans déjà existants de l'entité, sous réserve qu'ils présentent un niveau de protection équivalent), et les procédures d'incident grave[141] (étant précisé que l'article 73 paragraphe 9 du RIA dispose que

[135] *Article 18(3) du RIA.*
[136] *Article 254 de l'Arrêté du 3 Novembre 2014.*
[137] *Article 19(2) du RIA.*
[138] *Article 72(4) du RIA.*
[139] *Article 17(1), g) du RIA.*
[140] *Article 17(1), h) du RIA.*
[141] *Article 17(1), i) du RIA.*

pour les systèmes à haut risque visés à l'annexe III mis sur le marché par un fournisseur soumis à une obligation de signalement équivalente, alors seule la violation d'une obligation visant à protéger les droits fondamentaux doit être signalée), les Institutions Financières devront les mettre en place, la reconnaissance d'équivalence n'étant que partielle [142].

2.2 - Nouvelles obligations du RIA complétant la réglementation sectorielle des Institutions Financières

Outre les dispositions du RIA posant des reconnaissances d'équivalence ou de complémentarité à la réglementation sectorielle, le règlement introduit de nouvelles obligations pour les Institutions Financières, selon le rôle qu'elle occupe tel qu'expliqué dans le paragraphe 1 et la classification du Système d'IA, comme détaillé dans le paragraphe 3.

À ce titre et dans l'esprit du RIA, il nous semble que ces obligations spécifiques à l'IA ne devraient pas entrer en contradiction avec celles de la réglementation sectorielle mais plutôt les compléter.

Les Institutions Financières seront ainsi tenues, de manière non exhaustive, de répondre à des obligations en matière de gouvernance des données[143], préparation de documentation technique[144], enregistrement[145] et préparation d'un système de journaux automatisés[146] ou encore de contrôle humain[147]. Ces prescriptions viendront s'ajouter à celles déjà établies par la réglementation sectorielle en vigueur, et elles s'y intégreront de manière cohérente.

3. Un raffinement de la gestion des risques inhérents à l'usage de l'IA

Le RIA adopte une approche par les risques, conceptuellement proche de celle qui prévaut traditionnellement dans la réglementation bancaire et financière (bien que le référentiel soit différent)[148]. Cette approche implique que les Institutions Financières doivent effectuer un double travail d'identification et de qualification : d'une part, la qualification du modèle ou Système d'IA (par exemple, interdit, à haut risque, usage général, etc.) et, d'autre part, la qualification des acteurs impliqués (par exemple, fournisseur, déployeur, etc.), en sus d'un travail de cartographie des risques.

---

[142] *Veuillez-vous référer au paragraphe 3 du présent Rapport.*

[143] *Article 10 du RIA.*

[144] *Article 11 du RIA.*

[145] *Article 12 du RIA.*

[146] *Article 19 du RIA.*

[147] *Article 14 du RIA.*

[148] *Ceci a notamment été mis en évidence par un auteur : B. Bréhier, L'application du règlement européen sur l'intelligence artificielle (IA Act) aux activités bancaires et financières, RDBF n° 6, novembre-décembre 2024, paragraphe 20.*

Parallèlement, l'article 9 paragraphe 1, i) du RIA prévoit la mise en place d'un système de gestion des risques pour les Systèmes d'IA à haut risque. Aucune reconnaissance d'équivalence n'a été admise pour ces dispositions (cf. paragraphe (iii)). Toutefois, il est nécessaire de se poser la question de l'éventuel chevauchement ou de l'imbrication de ce système avec le cadre réglementaire existant pour les Institutions Financières.

Bien qu'aucune reconnaissance d'équivalence ne soit formellement instaurée dans le RIA, force est de constater que le système de gestion des risques prévu par le RIA ne pourra pas prévaloir, il devra venir en complément de celui issu de la réglementation bancaire et financière comme évoqué par l'article 17(4) du RIA. Une articulation des deux régimes nous semble inéluctable.

En effet, il semble important de noter que le système de gestion des risques en place dans les Institutions Financières répond aux particularités du secteur en prenant en compte de multiples aspects et enjeux qui ne sont pas considérés dans le RIA, lequel ne vise qu'à la préservation des droits fondamentaux. Le système de gestion des risques établi dans le cadre de la réglementation sectorielle bénéficie également de son autorisation par l'autorité compétente de supervision bien ancrée dans le paysage réglementaire européen, alors que celui posé par le RIA est encore balbutiant.

Enfin, les règles établies par la réglementation sectorielle sont conçues pour être flexibles et neutres, de sorte que l'intégration d'une nouvelle technologie comme l'IA ne devrait pas créer d'obstacles pour les Institutions Financières. Ces dernières devront néanmoins adapter leur système de gestion des risques pour répondre aux nouveaux risques créés par cette technologie.

Dès lors, le système de gestion des risques du RIA devrait naturellement s'intégrer dans celui existant pour les Institutions Financières. Toutefois, ces institutions ne seront pas exemptes de devoir effectuer certains ajustements pour répondre aux exigences spécifiques du RIA.

4. L'articulation incertaine en matière de règles de bonne conduite

Le RIA ne prévoit pas expressément de dispositif d'équivalence entre des règles de bonne conduite à mettre en œuvre vis-à-vis des clients bénéficiant d'une prestation de service réglementé utilisant l'IA et les règles de bonne conduite issues des règles sectorielles.

Il reviendra en effet à chaque Institution Financière de respecter pour chaque service réglementé les règles de bonne conduite pour prendre en compte les effets ou les risques attachés à l'IA qui serait utilisée pour leur prestation. Par exemple, l'article 50 du RIA dispose que les fournisseurs doivent s'assurer que les Systèmes d'IA destinés à interagir directement avec des personnes physiques soient conçus et développés de manière à ce que ces personnes soient informées qu'elles interagissent avec un Système d'IA, sauf à ce qu'il ressorte du point de vue de cette personne physique normalement informée, raisonnablement attentive et avisée qu'elle interagit avec un tel Système d'IA. Cette obligation de transparence devrait être intégrée dans les règles de bonne conduite imposées aux Institutions Financières.

Il n'en demeure pas moins que le niveau qualitatif mais aussi quantitatif d'information à donner aux clients / investisseurs en aval et en amont de la fourniture de la prestation de service réglementé relative à l'utilisation de l'IA et les risques associés relèvera de la politique interne de chaque Institution Financière.

5. L'articulation avec la réglementation prudentielle

L'articulation entre le RIA et la réglementation prudentielle repose sur le considérant n° 58 du RIA qui pose en la matière un principe d'exclusion dont la portée exacte demeure toutefois incertaine.

Selon le considérant n° 58, « *les systèmes d'IA prévus par le droit de l'Union […] à des fins prudentielles pour calculer les besoins en fonds propres des établissements de crédit et des compagnies d'assurance ne devraient pas être considérés comme étant à haut risque au titre du présent règlement* ». Autrement dit, les Systèmes d'IA utilisés à des fins prudentielles par les Institutions Financières qui font déjà l'objet d'un encadrement par une réglementation sectorielle spécifique (à l'instar de CRR pour les établissements de crédit ou de Solvabilité II tel que complétée par le règlement délégué (UE) 2015/35 pour les compagnies d'assurance) ne devraient pas, en principe, être soumis aux exigences prévues par le RIA pour les Systèmes d'IA à haut risque, dans la mesure où le considérant n° 58 exclut *a priori* cette qualification en ce qui concerne ces systèmes – à la différence des Systèmes d'IA destinés à être utilisés pour évaluer la solvabilité des personnes physiques ou pour établir leur note de crédit (*credit scoring*) qui sont, quant à eux, expressément catégorisés parmi les Systèmes d'IA à haut risque (conformément à l'annexe III point 5(b) du RIA).

Cependant, la portée exacte de cette exclusion comporte des incertitudes. En effet, la réglementation prudentielle encadrant l'utilisation par les Institutions Financières des Systèmes d'IA intégrés à leurs modèles internes aux fins du calcul de leurs exigences de fonds propres ne fait pas complètement abstraction du rôle que joue la notation interne attribuée par ces modèles dans l'approbation des crédits octroyés – y compris aux particuliers.

Tel est le cas par exemple de l'article 144(1)(b) de CRR qui soumet l'autorisation d'utiliser l'approche fondée sur les modèles internes à la démonstration par les établissements de crédit[149] que « *les notations internes et estimations de défauts et de pertes utilisées dans le calcul des exigences de fonds propres et les systèmes et processus liés jouent un rôle essentiel […] dans le processus décisionnel, ainsi que dans les fonctions d'approbation des crédits […]* ».

[149] *À la satisfaction de l'autorité compétente.*

Cette évaluation du rôle essentiel joué par la notation interne attribuée par le système de l'établissement de crédit dans la décision d'octroi du crédit est connue sous le nom de « *use-test* »[150]. Un modèle interne intégrant un Système d'IA permettant d'évaluer la solvabilité des personnes physiques en vue de leur attribuer une notation interne et les assigner à un échelon de crédit[151] aux fins du calcul des exigences de fonds propres pourrait-il être considéré comme incluant un système de *credit scoring* entrant dans le champ des Systèmes d'IA à haut risque (en vertu de l'annexe III, point 5(b)) et déclencher de ce fait, dans une certaine mesure, l'application des règles prévues par le RIA pour les Systèmes d'IA à haut risque ? La question reste ouverte n'ayant pas fait, à ce stade, l'objet de clarifications de la part des autorités compétentes.

Ainsi, bien que le considérant n° 58 du RIA pose un principe d'exclusion des Systèmes d'IA utilisés à des fins prudentielles pour calculer les exigences de fonds propres de la catégorie des Systèmes d'IA à haut risque, les exigences du RIA auront probablement un impact sur le développement des modèles internes et l'évaluation des critères encadrant leur utilisation par les autorités compétentes, dans la mesure où ces systèmes participent à l'évaluation de la solvabilité des personnes physiques et impliquent l'attribution d'une note de crédit « *interne* » en vue de l'octroi de crédit à l'égard de ces personnes.

En outre, il convient de noter que cette exclusion du champ des Systèmes d'IA à haut risque des Systèmes d'IA utilisés à des fins prudentielles pour le calcul des besoins en fonds propres des établissements de crédit et des compagnies d'assurances (déjà encadrés par une réglementation sectorielle existante) n'est pas reprise (ou autrement précisée) dans le corps même du RIA.

Une clarification de l'articulation du RIA et de la réglementation prudentielle (en particulier de cette exclusion prévue par le considérant n° 58) serait certainement bénéfique afin de permettre aux Institutions Financières pour lesquelles le droit de l'Union prévoit la possibilité d'utiliser l'approche fondée sur les modèles internes pour le calcul de leurs exigences de fonds propres d'identifier clairement les règles qui leur sont applicables en fonction de l'utilisation qu'elles font de l'IA en lien avec leurs modèles internes.

Au-delà, il convient de noter que le principe d'exclusion des Systèmes d'IA utilisés à des fins prudentielles pour calculer les exigences de fonds propres de la catégorie des Systèmes d'IA à haut risque au titre du RIA posé par le considérant n° 58 ne vise que deux catégories d'Institutions

[150] *Julien Uri (ACPR) et François Guebs (Banque Nationale de Belgique), présentation « AI Act et réglementation sectorielle : interactions et conséquences sur la supervision » - accessible ici : chrome-extension ://efaidnbmnnnibpcajpcglclefindmkaj/ https://www.telecom-paris.fr/wp-content-EvDsK19/uploads/2024/12/lundi-ia-finance-11-supervision-f-guebs-j-uri.pdf.*

[151] *Conformément aux prescriptions des articles 172 et 173 de CRR.*

Financières, à savoir les établissements de crédit et les compagnies d'assurances, précisément celles pour lesquelles le droit de l'Union permet aujourd'hui l'utilisation de Systèmes d'IA à des fins prudentielles dans le cadre notamment de l'utilisation des modèles internes.

Or, comme indiqué précédemment (cf. paragraphe 2), d'autres types d'Institutions Financières pourraient envisager de recourir à l'IA à des fins prudentielles pour calculer leurs besoins en fonds propres, par exemple les entreprises d'investissement déterminant leurs fonds propres sur la base des facteurs K ou les sociétés de gestion de portefeuille soumises à des exigences de fonds propres supplémentaires en vertu de la directive AIFM. Le cas échéant, le considérant n° 58 du RIA, tel que rédigé actuellement, ne permettrait pas de faire bénéficier les Systèmes d'IA mis en place aux fins de calculer leurs besoins en fonds propres par ces Institutions Financières de l'exclusion de principe de la catégorie des Systèmes d'IA à haut risque au titre du RIA qu'il prévoit (et cela, *a priori*, que le droit de l'Union prévoit[152] ou ne prévoit pas[153] d'encadrement spécifique pour l'utilisation que pourraient avoir ces Institutions Financières de l'IA à des fins prudentielles).

Les Systèmes d'IA utilisés par les Institutions Financières autres que des établissements de crédit ou des compagnies d'assurances à des fins prudentielles pour calculer leurs besoins en fonds propres pourraient donc être qualifiés de Systèmes d'IA à haut risque, alors même qu'ils poursuivent un objectif similaire, si les conditions de l'article 6 du RIA se trouve remplies. Une clarification quant à l'interprétation de la portée du principe d'exclusion posé par le considérant n° 58 s'agissant des Institutions Financières susceptibles d'en bénéficier, sur la base notamment des objectifs qui ont présidé à son insertion dans le RIA, pourrait donc également s'avérer bénéfique, afin d'apporter une sécurité juridique à l'usage qui pourrait être fait par d'autres Institutions Financières de l'IA à des fins prudentielles.

6. L'articulation avec les règles d'externalisation sectorielles

Le RIA ne pose pas de règles spécifiques en matière d'externalisation[154] qui pourraient se chevaucher ou poser des difficultés d'articulation avec les règles préexistantes dans la réglementation bancaire

[152] *La réglementation IFD/IFR opérant un renvoi à la réglementation CRD/CRR pour le calcul du facteur K reflétant le risque de position nette (K-NPR), les entreprises d'investissement sont a priori autorisées à utiliser les modèles internes pour calculer les exigences de fonds propres y afférents en vertu du droit de l'Union. Pourtant, les entreprises d'investissement ne sont pas mentionnées parmi les Institutions Financières visées par le considérant n° 58 du RIA comme bénéficiant de l'exclusion de principe qu'il pose, s'agissant des Systèmes d'IA utilisés aux fins du calcul des exigences de fonds propres qu'elles utilisent.*

[153] *La réglementation encadrant la détermination des exigences de fonds propres supplémentaires pour les sociétés de gestion de portefeuille soumises à la directive AIFM ne prévoit pas de dispositions relatives à l'utilisation de l'IA à cette fin.*

[154] *Pour rappel, l'externalisation est définie par la réglementation sectorielle comme le fait pour une Institution Financière de décider qu'une activité ou un service qu'elle aurait elle-même effectué (ou qu'il serait raisonnable de concevoir qu'elle l'aurait effectué) soit réalisé par un tiers (Cf. le paragraphe 26 des « EBA Guidelines on outsourcing arrangements », EBA/GL/2019/02, 25 février 2019).*

et financière (cf. paragraphe 1). Cependant, bien qu'un tel chevauchement ne soit pas explicitement observé, on peut s'interroger sur des scénarios où une Institution Financière prendrait alternativement le rôle de fournisseur ou de déployeur d'IA.

Ces statuts de fournisseur ou déployeur au sens du RIA emportent-ils pour l'Institution Financière une qualification d'entité externalisatrice ou réalisant une prestation externalisée ?

Les rôles de fournisseur et de déployeur définis par le RIA se fondent sur la relation de chaque acteur avec le Système d'IA, plutôt que sur la relation entre les acteurs eux-mêmes, comme c'est le cas pour l'externalisation, qui qualifie une relation entre une Institution Financière et un tiers prestataire. Dès lors, le rôle de l'acteur au sens du RIA ne constitue pas d'emblée une activité pertinente au sens de la réglementation sectorielle sur l'externalisation. Les statuts au sens du RIA et de la réglementation sectorielle ne nous semblent ni antinomiques ni incompatibles et doivent s'analyser séparément.

Ainsi, le fait de confier à un tiers une activité ou un service que l'Institution Financière aurait elle-même effectué (ou qu'il serait raisonnable de concevoir qu'elle l'aurait effectué) semble être le premier critère permettant d'apprécier une éventuelle relation d'externalisation, sans que le rôle défini par le RIA pour chaque partie prenante n'interfère.

En mettant en perspective les concepts du RIA avec l'externalisation, plusieurs scénarios peuvent être distingués pour évaluer une éventuelle relation d'externalisation. D'abord, si une Institution Financière fait appel à un tiers pour la conception de son Système d'IA, alors elle ne réaliserait pas d'opération d'externalisation proprement dite, car cette opération interviendrait hors du champ de ses services et activités découlant de son statut. En revanche, si une Institution Financière, fournisseur de Système d'IA, confie à un tiers déployeur l'usage de son système pour la fourniture d'un service ou d'une activité qu'elle aurait exercée, ou si une Institution Financière fait appel à un tiers, agissant comme fournisseur ou déployeur, pour la fourniture d'une activité ou d'un service que l'entité aurait elle-même exercée ou fournie, alors un schéma d'externalisation eu égard à l'activité confiée au tiers serait à considérer.

Le recours à toute prestation de services en matière d'IA méritera une attention particulière, notamment lorsque l'Institution Financière, qui agit en tant que déployeur, utilise un outil d'IA fourni par un tiers, pour la réalisation d'une activité réglementée. Cette hypothèse pourrait ne pas être considérée comme de l'externalisation car l'Institution Financière conserverait sa fonction en interne et ne ferait appel à un tiers qu'en vertu d'un contrat de prestation de services. Toutefois, cette approche doit être nuancée, par une analyse du Système d'IA, de son fonctionnement, de son développement, de son déploiement et de ses finalités. En effet, cette prestation de service pourrait être assimilée à de l'externalisation si elle s'avère « *critique* », i.e. dont l'anomalie ou la défaillance pourrait nuire sérieusement à l'activité, les prestations de service réglementé, la continuité ou encore la solidité de l'Institution Financière.

D'une manière générale, comme le souligne notamment l'ESMA[155], les Institutions Financières doivent scruter toute relation avec des prestataires tiers en matière d'IA pour identifier une éventuelle qualification d'externalisation, et a fortiori pour la fourniture d'une PSEE entraînant l'application d'obligations supplémentaires pouvant remettre en question le schéma envisagé par l'Institution Financière.

B. Les défis de l'articulation du RIA avec les autres réglementations européennes sur les données

Le RIA ne précise pas toujours clairement son articulation avec les autres réglementations européennes relatives aux données, qu'elles aient une portée générale comme le RGPD (pourtant très souvent cité par le RIA) ou NIS 2, ou sectorielle comme DORA (alors que le RIA inclut un certain nombre de dispositions spécifiques aux entités financières).

Pourtant, ces textes visent à responsabiliser les acteurs non seulement en leur imposant des obligations strictes, mais également en les contraignant à documenter et à démontrer leur conformité à ces obligations.

Cependant, tant DORA que le RGPD peuvent être des alliés pour renforcer la protection des données et, par conséquent, les actifs des Institutions Financières. Ces dernières doivent gérer leurs actifs constitués ou utilisant des données, évaluer les risques et garantir la transparence pour se conformer à DORA, au RGPD et au RIA, en particulier lorsqu'elles déploient des solutions d'IA à haut risque.

1. DORA

DORA, entré en application le 17 janvier 2025, vise à consolider et harmoniser les exigences en matière de risque lié aux TIC en matière de risque opérationnel qui avaient jusqu'à présent été répartis dans divers actes juridiques de l'UE.

L'objectif du RIA est également d'établir un cadre juridique uniforme concernant les Systèmes d'IA, afin de promouvoir l'adoption de l'IA tout en garantissant un niveau élevé de protection des droits fondamentaux et en soutenant l'innovation. Dans le secteur financier, les objectifs de ces règlements sont donc intrinsèquement liés, pour autant que la technologie de communication

[155] *ESMA, Public Statement On the use of Artificial Intelligence (AI) in the provision of retail investment services, ESMA35-335435667-5924, 30 mai 2024, «The deployment of AI tools in various steps of the provision of investment services can be based on the acquisition of solutions developed by third-party service providers. In such instances, firms are reminded of the applicable MiFID II requirements regarding outsourcing of critical and important operational functions aimed at ensuring an adequate level of due diligence in the selection process of such providers along the value chain and the implantation of adequate controls.»*

sous-jacente s'appuie sur l'IA ou que le Système d'IA en question constitue une TIC. En d'autres termes, certaines Institutions Financières pourraient fréquemment devoir appliquer en parallèle les deux règlements à un même produit ou à un même prestataire. À titre d'exemple, les Systèmes d'IA devraient être considérés comme des « *actifs de TIC* » au sens de DORA, déclenchant l'application des règles relatives à ces actifs. En particulier, cela devrait déclencher l'intégration de ces Systèmes d'IA au cadre de gestion des risques prévu à l'article 6 de DORA.

Or, ces règlements ne sont pas toujours parfaitement alignés, en raison de leur différence d'objet et de champ d'application. Par exemple, DORA impose la mise en place d'audits des prestataires tiers de services TIC et des TIC de l'Institution Financière elle-même, alors que le RIA impose, concernant les Systèmes d'IA à haut risque, qu'ils permettent « *un contrôle effectif par des personnes physiques pendant leur période d'utilisation* ». Deux niveaux de contrôle devraient donc pouvoir s'appliquer à certaines TIC qui s'appuieraient sur des Systèmes d'IA à haut risque, au risque de créer des redondances ou des manques dans les contrôles effectués. Les Institutions Financières devraient donc s'assurer que leurs politiques et procédures en matière de contrôle de ces systèmes sont parfaitement articulées pour répondre aux exigences réglementaires tout en limitant en pratique les doublons sur le champ des contrôles, leur fréquence, les actions de remédiation, etc.

DORA et le RIA imposent également tous les deux des obligations de documentation, sur des champs néanmoins différents. Les obligations de DORA se focalisent en effet logiquement sur les TIC, visant notamment les fonctions « *métiers* », les rôles et les responsabilités s'appuyant sur les TIC, les actifs informationnels et les actifs de TIC qui soutiennent ces fonctions, ainsi que leurs rôles et dépendances en ce qui concerne le risque lié aux TIC. Les obligations découlant du RIA concernent de leur côté en particulier la documentation technique relative aux Systèmes d'IA à haut risque – qui peuvent se recouper avec les obligations en matière de TIC. Les Institutions Financières devront donc prévoir des politiques et procédures permettant de respecter ces deux jeux d'obligations de documentation et d'identifier là encore les redondances.

L'innovation est au cœur des enjeux du RIA et de DORA, dont les dispositions visent à encadrer les risques et appliquer un cadre de conformité éthique et de sécurité opérationnelle. Les Systèmes d'IA mis en place par les Institutions Financières devront donc se conformer à ces exigences, l'enjeu pour les Institutions Financières étant de poursuivre leurs projets innovants tout en respectant ce cadre.

L'un des piliers de DORA et de la réglementation applicable aux Institutions Financières en général, consiste dans la maîtrise des risques découlant du recours à des prestataires externes. Le recours à ces derniers doit faire l'objet de manière générale à des processus décisionnels précis, à des contrôles réguliers, etc. Les prestataires tiers pourront désormais, le cas échéant en sus de la réglementation applicable en matière d'externalisation, être également soumis à deux autres couches d'obligations : celles mises à la charge des Institutions Financières par DORA et le RIA, lesquels imposent, chacun pour leur champ d'application, des obligations de documentation, de gestion des biais des Systèmes d'IA, de résilience opérationnelle et de cybersécurité, etc.

On notera qu'en marge de DORA et du RIA, d'autres textes concernent la cybersécurité des Systèmes d'IA. Si le RIA consacre son article 15 à la cybersécurité des IA à haut risque, il faut se tourner vers un autre règlement pour aborder globalement cette question. Il s'agit du Règlement « *Cyber Resilience Act* » n° 2024/2847 du 23 octobre 2024 concernant des exigences de cybersécurité horizontales pour les produits comportant des éléments numériques. Ce texte vise la certification européenne de cybersécurité des produits, matériels ou logiciels comportant des éléments numériques (notamment les objets connectés) mis à disposition sur le marché « *dont l'utilisation prévue ou raisonnablement prévisible comprend une connexion directe ou indirecte, logique ou physique, à un dispositif ou à un réseau* ». L'objectif est de protéger les consommateurs et les entreprises des risques lors de la conception, du développement, de la production et de la mise à disposition sur le marché.

Ce règlement est à lire conjointement avec le *Scheme* EUCC[156], premier schéma européen de certification de cybersécurité fondé sur des critères communs, notamment en matière d'évaluation et de certification des logiciels utilisés dans le marché intérieur. Basé sur le volontariat, l'EUCC permet aux fournisseurs de TIC de passer par un processus d'évaluation communément admis par l'UE pour certifier des produits TIC tels que notamment des logiciels[157].

Ce schéma complète la certification SOG-IS[158], dont l'objectif est de protéger les utilisateurs contre les risques de cybersécurité liés aux produits informatiques.

2. RGPD

DORA, entré en application le 17 janvier 2025, vise à consolider et harmoniser les exigences en matière de risque lié aux TIC en matière de risque opérationnel qui avaient jusqu'à présent été répartis dans divers actes juridiques de l'UE.

2.1 - Une articulation délicate avec le RIA

Le RIA prévoit explicitement son articulation avec le RGPD, quand bien même certains concepts n'ont pas toujours la même portée ou le même champ d'application.

---

[156] *Règlement d'exécution 2024/482 du 31 janvier 2024 portant modalités d'application du règlement (UE) 2019/881 du Parlement européen et du Conseil en ce qui concerne l'adoption du schéma européen de certification de cybersécurité fondé sur des critères communs (EUCC - European Union Common Criteria Cybersecurity Certification Scheme).*

[157] *Ce règlement a été complété par un second règlement 2024/482 du 31 janvier 2024 portant modalités d'application du règlement (UE) 2019/881 du Parlement européen et du Conseil en ce qui concerne l'adoption du schéma européen de certification de cybersécurité fondé sur des critères communs (EUCC).*

[158] *L'accord du SOG-IS a été créé en réponse à la décision du conseil des communautés européennes du 31 mars 1992 en matière de sécurité des systèmes d'information (92/242/CEE) et de la recommandation du Conseil 1995/144/CE du 7 avril 1995, concernant des critères communs d'évaluation de la sécurité des technologies de l'information. https://www.sogis.eu/index_fr.html.*

Dans le domaine de l'IA, les données agissent comme le carburant qui alimente le moteur des algorithmes. Dès lors, la qualité et la quantité des données influencent directement la capacité de l'IA à apprendre et à prendre des décisions.

Lorsque ces données en question sont des données à caractère personnel, y compris pseudonymisées, le RGPD a vocation à s'appliquer et ce de manière automatique. Les données à caractère personnel sont centrales dans de très nombreux Systèmes d'IA mis en œuvre dans le secteur financier. À chaque étape du développement et du déploiement d'un Système d'IA, des données à caractère personnel peuvent en effet être incluses et traitées, notamment au sein des données d'entraînement, des données de validation, des données de test, des données d'entrée ou des données de sortie. Il est même possible qu'un Système d'IA puisse inférer des données personnelles à partir de données d'entrée qui ne contiennent aucune donnée à caractère personnel. Cela serait théoriquement le cas lorsqu'un Système d'IA peut déduire l'identité unique d'une personne à partir des données non personnelles qui lui sont fournies. En outre, la formation des grands modèles de langage (LLM) nécessite des informations liées aux individus pour affiner le modèle en exploitant des informations contextuelles.

Le traitement des données à caractère personnel dans les Systèmes d'IA nécessite donc une vigilance accrue et une conformité rigoureuse au RGPD, afin de protéger les droits des individus à chaque étape du développement et du déploiement de ces technologies. Il est crucial de considérer les implications en matière de confidentialité, même lorsque les données initiales ne sont explicitement pas personnelles.

Le RGPD s'applique donc simultanément au RIA. Les deux règlements sont complémentaires, le RIA ne se substituant pas au RGPD.

Le RGPD repose sur un principe de responsabilité et sur des règles technologiquement neutres, exigeant des opérateurs qu'ils s'assurent que le traitement des données à caractère personnel est licite et proportionné. En revanche, le RIA fonctionne selon une approche par les risques, similaire à l'approche des réglementations relatives aux produits défectueux, selon laquelle certains types de Systèmes d'IA sont simplement interdits ou présumés constituer un risque élevé et ne peuvent être déployés que dans certaines circonstances et sous certaines conditions.

Malgré ces différences fondamentales, les deux règlementations partagent un objectif commun : la protection des individus. Cette approche passe à travers la mise en cause de la responsabilité des acteurs impliqués. Le RGPD, centré sur le traitement et la protection des données à caractère personnel, garantit aux individus un contrôle sur leurs informations. Il introduit des droits tels que le droit d'accès, le droit de rectification, le droit à l'effacement, et le droit d'opposition à des traitements de données, notamment lorsque ces traitements sont automatisés. Dans le cadre du RGPD, les responsables du traitement et sous-traitants doivent mettre en place les mesures techniques et organisationnelles pour garantir la conformité de leurs traitements.

En parallèle, le RIA adopte une approche spécifique aux Systèmes d'IA, en imposant des exigences particulières pour éviter les violations de droits fondamentaux. Il s'agit, par exemple, d'imposer des critères de transparence et plus généralement de garantir que les systèmes à haut risque ne compromettent pas les droits à la dignité humaine, à la protection des données ou à la non-discrimination. Les acteurs de l'IA doivent également prouver leur conformité à des normes strictes incluant des obligations de documentation et d'évaluation d'impact. Par exemple, le RIA et le RGPD visent tous deux à protéger les droits des individus dans le cas de procédures automatisées en intégrant le concept d'intervention humaine. Le RGPD concède aux personnes concernées le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé (y compris le profilage) produisant des effets juridiques les concernant ou les affectant de manière significative (article 22 RGPD). Le RIA quant à lui enjoint les systèmes à haut risque à intégrer une garantie humaine chargée de minimiser les risques et assurer la fiabilité du SIA (article 14 RIA). À noter qu'une décision prise exclusivement par un Système d'IA pourrait ainsi entrer dans le champ d'application du RGPD conformément à l'article 22 évoqué précédemment. À titre d'illustration, la CJUE a considéré que l'évaluation du *credit scoring* est une décision automatisée, à condition que ce score ait exercé une influence déterminante dans la prise de décision[159]. Le RIA, lui, permet dans certains cas aux personnes concernées faisant l'objet d'une décision prise par un déployeur sur la base des sorties d'un Système d'IA (à haut risque mentionné à l'annexe III) d'obtenir des explications sur le rôle du SIA dans la procédure décisionnelle et sur les principaux éléments de la décision prise et ce conformément à l'article 86 du RIA.

Ensemble, ces deux textes visent à protéger les droits individuels contre les effets indésirables des technologies numériques tout en promouvant l'innovation, notamment en termes de circulation des données. Ces textes visent finalement à développer des innovations qui soient respectueuses des droits des individus.

Cela étant, le RIA et le RGPD peuvent entrainer des divergences dans la mise en œuvre du principe de *privacy by design*. Pour rappel, le principe en question consiste à intégrer la protection des données personnelles dès la conception des systèmes en veillant à ce que les mesures de sécurité soient prises en compte de manière proactive tout au long du cycle de vie des données. Selon le RGPD, les systèmes qui traitent des données à caractère personnel doivent être conçus dès le départ de manière à intégrer des mécanismes de protection des données. Cela peut inclure des principes de minimisation des données, de limitation des finalités, et de sécurisation des données par défaut.

Le principe de minimisation des données est la traduction directe du principe de *privacy by design* dans les SIA dont l'application peut parfois s'avérer délicate, notamment lorsqu'il s'agit de traiter

[159] *CJUE, C-634/21, OQ c/ SCHUFA Holding AG, 7 décembre2023.*

des grandes quantités de données pour entrainer des Systèmes d'IA ou de garantir la transparence et l'explicabilité des modèles complexes. Les algorithmes d'apprentissage automatique nécessitent de larges quantités de données pour entrainer leurs modèles. Or, pour améliorer la performance et réduire les biais, il est parfois nécessaire d'utiliser des ensembles de données redondants ou d'inclure des informations non essentielles. Il faudra alors garder à l'esprit le principe de minimisation lors de l'incorporation de ces larges bases de données et évaluer les besoins du SIA par rapport à la protection des données. Certaines pondérations s'avèreront par conséquent indispensables, notamment quant à la nécessité d'entrainer le modèle sur de grandes bases de données face à la réduction du nombre de données qui pourrait impacter la qualité du SIA. En d'autres termes, il ne faut traiter que le minimum de données strictement nécessaires à maintenir la qualité d'un SIA[160].

De plus, le RGPD instaure également des obligations de limitation de la durée de conservation des données. Les modèles d'IA nécessitent souvent des ensembles de données historiques pour être réentraînés et maintenus à jour, ce qui doit être articulé avec l'obligation du RGPD de limiter la durée de conservation des données. Afin de respecter cette obligation, la CNIL encourage les fournisseurs à fixer une limite de conservation des données proportionnelle à leurs usages. Bien qu'elles puissent être gardées pour la maintenance du produit ou à des fins d'amélioration du système, ces données devront toutefois faire l'objet de mesures de sécurité renforcées[161]. De même, l'obligation de traçabilité des décisions prises par des systèmes automatisés, qui impose souvent une rétention de données plus longue pour pouvoir vérifier et expliquer ultérieurement les décisions des algorithmes, se traduit par la nécessité de conserver des données sur une plus longue période.

Afin d'atténuer l'impact sur la vie privée tout en maintenant une conformité avec le principe de minimisation, une pratique courante consiste à pseudonymiser ou anonymiser les données utilisées pour l'entraînement des systèmes IA. Cependant, la pseudonymisation ne résout pas totalement le problème, dans la mesure où les données peuvent dans certaines situations être réidentifiées, elles sont toujours considérées comme étant personnelles et dès lors sont soumises à la protection du RGPD. Quant à l'anonymisation, cette pratique peut rendre les données moins fiables ou réduire la performance des algorithmes.

Une autre considération à prendre en compte concerne les finalités de traitement, principe clé du RGPD[162]. Selon ce dernier, les données devraient être collectées pour un but déterminé et légitime et ne pas être traitées ultérieurement de façon incompatible avec cet objectif initial. Toutefois, les

[160] *CNIL, IA : tenir compte de la protection des données dans la conception du système, Recommandation, 08 avril 2024.*

[161] *Ibid.*

[162] *Article 5 du RGPD.*

SIA ont un besoin constant de données pour s'améliorer au fil du temps grâce à l'apprentissage continu. Cela signifie que des données initialement collectées pour une finalité spécifique peuvent être réutilisées pour d'autres finalités afin d'améliorer le modèle. Pour encourager une saine réutilisation des données, en cohérence avec le RGPD, les acteurs financiers pourront se tourner vers le règlement européen du *Digital Governance Act* (**DGA**) adopté en 2022 qui promeut des règles d'échange et de réutilisation de données entre tous les acteurs du marché commun. De plus, l'Union européenne prévoit d'adopter un autre texte se concentrant précisément sur l'échange de données financières (*Financial Data Access Regulation* (**FiDA**))[163]. Par ailleurs, la CNIL mentionne que la réutilisation de bases de données pour entraîner les SIA est possible à condition que ces données n'aient pas été collectées de manière « *manifestement illicite* » et que la réutilisation soit compatible avec la collecte initiale[164].

Face à cette nécessité d'articulation, la CNIL a émis des recommandations à destination des fournisseurs qu'ils agissent en qualité de responsable de traitement ou de sous-traitant[165]. Ces opérateurs d'IA doivent respecter un certain nombre d'étapes pour garantir une saine utilisation des données personnelles dans les Systèmes d'IA. Tout d'abord, ils devront définir la finalité du traitement lorsqu'ils constitueront une base de données personnelles. C'est-à-dire définir clairement l'objectif de leur système, en établissant un cahier des charges minimisant les impacts sur les personnes concernées. Cela inclut la définition des résultats attendus, des indicateurs de performance, et des contextes d'utilisation[166], afin d'éviter une collecte excessive de données. Aussi, il faudra choisir des techniques permettant de ne pas traiter plus de données que nécessaire en application du principe de minimisation des données. De plus, le traitement devra être licite : la base légale du traitement des données personnelles devra être clairement définie par le Système d'IA, en s'assurant à la fois de sa pertinence et de sa validité. Une étude d'impact sur la protection des données (AIPD) avant le déploiement d'un Système d'IA, en particulier pour les systèmes à haut risque, pourra être nécessaire pour minimiser les risques. Il pourrait également être nécessaire de faire valider les choix effectués par des études pilotes ou d'obtenir l'avis d'un comité éthique pluridisciplinaire et indépendant, pour assurer la pertinence technique et éthique des données et des méthodes utilisées. Les opérateurs devront informer de manière transparente les personnes

[163] *Proposal for a Regulation on a Framework for Financial Data Access, Commission européenne (2 décembre 2024). https://data.consilium.europa.eu/doc/document/ST-16312-2024-INIT/en/pdf.*

[164] *CNIL, IA et RGPD : la CNIL publie ses nouvelles recommandations pour accompagner une innovation responsable, Recommandation, 7 février 2025.*

[165] *Voir CNIL, Les fiches pratiques IA, Recommandations.*

[166] *Cependant, les réutilisations de données pour des finalités non prévues initialement sont et restent possibles, sous réserve de la réalisation de démarches supplémentaires, telles qu'un test de compatibilité. À cet égard, la CNIL précise que la réutilisation des données pour améliorer des modèles n'est pas, à première vue, une finalité « incompatible » avec la finalité initiale. Voir CNIL, Réutilisation de bases de données : les vérifications nécessaires pour respecter la loi, 23 janvier 2025.*

concernées sur l'utilisation de leurs données par le Système d'IA et sur leurs droits en vertu du RGPD. Finalement, en aval, les opérateurs devront garantir la sécurité du SIA, notamment en mettant en place des mécanismes de contrôle et d'audit réguliers pour s'assurer de la conformité continue du Système d'IA et des données traitées.

L'application et l'interprétation futures des principes du RIA et du RGPD, à la lumière du RIA, devrait conduire les régulateurs à continuer d'éclairer les professionnels concernés sur l'application des règles relatives au traitement des données personnelles.

2.2 - Les sources de conflit en matière d'articulation entre les principes clé du RGPD et les finalités de l'IA.

Comme mentionné ci-dessus (cf. paragraphe III(B)(2)(2.1.)), le respect des principes essentiels du RGPD à toutes les étapes du développement et du déploiement d'un Système d'IA peut s'avérer complexe. Ainsi, le RGPD impose que des principes tels que celui de minimisation, de limitation des finalités ou encore d'exactitude soient respectés par le fournisseur et le déployeur lors de la collecte des données pour l'entraînement du Système d'IA, de leur utilisation pour l'entraînement, de leur utilisation comme donnée de sortie ou lors de la réintégration des données dans le système afin d'améliorer celui-ci. À titre d'illustration, le principe d'exactitude devrait s'appliquer lors de la collecte des données ; à ce titre cela imposerait au responsable de traitement de vérifier que toutes les données personnelles destinées à entraîner son modèle sont exactes. Or, comme ces données sont généralement collectées par *scraping* de données librement accessibles en ligne, mener une opération de vérification de l'exactitude de ces dernières serait en pratique complexe malgré l'existence de premières solutions envisageables[167]. De même, ce principe d'exactitude s'applique aux données de sortie. Ainsi, à supposer que les données d'entraînement aient été exactes, le fournisseur devrait également s'assurer de l'exactitude des données générées par le Système d'IA. Cela nécessiterait une étape supplémentaire de vérification qui pourrait s'avérer complexe du fait de l'absence de données d'entrée certifiées permettant de valider l'exactitude des données de sortie. À ce titre, en avril 2024, l'organisme NOYB a déposé plainte contre OpenAI devant l'autorité de protection des données autrichienne arguant que ChatGPT fournissait des données de sortie inexactes en réponse à un *prompt*.

(i) Tension en matière de transparence.

L'exception à l'obligation d'information prévue par le RGPD dans l'article 14.5.b, qui prévoit que cette exception est applicable si la fourniture d'information se révèle impossible ou exigerait des

[167] *Ces solutions consistent par exemple à exclure par défaut certains sites des sources de collecte de données personnelles, ou à limiter la collecte exclusivement à des données librement accessibles.*

efforts disproportionnés, est délicate à mettre en œuvre, en fonction du contexte de collecte des données. Cette exception s'applique pour des traitements à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique, historique ou statistique mais aussi dans les cas où les organismes qui ne sont pas ou ne sont plus en lien avec les personnes concernées, n'ont pas à leur disposition les informations qui leur permettraient d'assurer une information individuelle. En pratique, les autorités de protection des données demandent aux responsables de traitement d'évaluer et documenter le caractère disproportionné qu'impliquerait une communication individuelle aux personnes concernées par rapport à l'atteinte réelle portée à leur vie privée en l'absence d'une telle information individuelle[168]. Ainsi, les autorités reconnaissent que l'information individuelle des personnes concernées peut dans certains cas nécessiter des efforts disproportionnés de la part du responsable du traitement. Ce dernier pourrait alors procéder à une information générale sur son site internet, en la complétant le cas échéant par des mesures appropriées supplémentaires[169].

(ii) Tension en matière d'exercice des droits des personnes concernées.

Au titre du RGPD, les personnes concernées ont différents droits qu'elles peuvent exercer auprès d'un responsable de traitement (e.g. droit d'accès, d'effacement, de rectification,…). Cependant, il peut s'avérer difficile pour un responsable de traitement qui traite des données personnelles pour des finalités liées à un Système d'IA de faire droit à certaines de ces demandes : une telle situation peut même nécessiter que le responsable du traitement mette à jour l'organisation de ses process opérationnels. Par exemple, si une personne identifie que des données de sortie contiennent des données personnelles qui lui sont associées, elle doit pouvoir en demander l'effacement ou la modification conformément aux droits garantis par le RGPD. Or, cela implique de devoir identifier dans les données utilisées pour entrainer le système celles qui se rapportent à la personne concernée, ce qui n'est pas toujours immédiatement possible pour le responsable du traitement. Dans de nombreux cas, cela pourrait même entraîner de sa part un traitement supplémentaire mis en œuvre à des fins d'identification de la personne concernée. Or, le RGPD prévoit justement que le responsable de traitement n'est pas tenu de traiter des informations supplémentaires ou de conserver des données personnelles à la seule fin de respecter le règlement ou de répondre aux demandes des personnes concernées. Toutefois, la situation peut être simplifiée lorsque la personne concernée fournit elle-même des informations permettant de l'identifier : en l'invitant à procéder de cette manière, le responsable du traitement peut donc concilier des impératifs en apparence contradictoires. Enfin il est également possible que les données en question aient été générées

[168] *Un grand nombre de facteurs peuvent être pris en compte (absence des informations permettant de contacter les personnes concernées, ancienneté des données utilisées par le responsable du traitement, nombre important de personnes concernées par l'information à fournir, dimension intrusive ou non du traitement envisagé, existence ou non de risques particuliers liés à la mise en œuvre du traitement pour les personnes concernées, type de personnes concernées par l'information individuelle, etc.).*

[169] *CNIL, IA : Informer les personnes concernées, Recommandation, 7 février 2025.*

par le SIA. En pratique, la réponse à ces demandes nécessiterait donc un travail de classification (possible par le biais de métadonnées) des données afin de pouvoir, en cas de demande d'une personne concernée, rattacher la personne aux données la concernant parmi celles traitées. À ce titre, lors de la réunion du Comité Européen de la Protection des Données du 5 novembre 2024 sur les modèles d'IA « *Stakeholder event on AI models* », plusieurs acteurs ont souligné le fait qu'une fois entraîné, un modèle d'IA ne constituait pas une base de données au sein de laquelle il est possible de chercher facilement des données associées à une personne en particulier. Considérant que cette recherche n'est pas impossible, la CNIL recommande en réponse à cette analyse d'établir une procédure interne consistant à interroger le modèle pour vérifier les données qu'il aurait pu mémoriser concernant la personne concernée[170]. Une fois parvenu à traiter la demande, le responsable de traitement devra s'assurer que cette décision est répercutée sur le Système d'IA (e.g. pour une demande de rectification, que son système génère des données de sortie conforme à la modification demandée et que les données obsolètes ne soient plus traitées, en ré-entraînant le modèle sans les données litigieuses par exemple).

À noter que le coût, l'impossibilité ou les difficultés pratiques pourront parfois justifier un refus d'exercice des droits ; lorsque le droit doit être garanti, la CNIL prendra en compte les solutions raisonnables à la disposition du créateur du modèle et les conditions de délai pourront être aménagées. La recherche scientifique évolue rapidement dans ce domaine et les acteurs doivent se tenir informés de l'évolution de l'état de l'art pour protéger au mieux les droits des personnes.

(iii) Tension en matière de base légale.

Le RGPD prévoit que tout traitement de données personnelles doit être fondé sur une base légale appropriée. Pour ce qui est du traitement de données personnelles dans le cadre du développement et déploiement de Systèmes d'IA, la CNIL a fait valoir que l'intérêt légitime sera vraisemblablement la base légale la plus utilisée par les professionnels. Elle accompagne les professionnels qui souhaitent fonder leurs traitements sur cette base juridique, notamment en mettant en avant des garanties qui, mises en œuvre en fonction des risques présentés par le traitement, permettraient d'assurer une balance équitable entre les différents intérêts en présence[171]. Cependant, le RGPD prévoit que lorsque le traitement est fondé sur l'intérêt légitime, la personne concernée peut exercer son droit d'opposition, contraignant ainsi le responsable de traitement à cesser le traitement des informations qui la concernent. Comme indiqué précédemment, la mise en œuvre de ce droit est particulièrement complexe dans le cas d'un Système d'IA mais il est possible, dans certains cas, de justifier un refus ou d'aménager les conditions pour y donner suite[172].

---

[170] *CNIL, IA : Respecter et faciliter l'exercice des droits des personnes concernées, 07 février 2025.*

[171] *IA : Mobiliser la base légale de l'intérêt légitime pour développer un système d'IA, CNIL, 10 juin 2024.*

[172] *CNIL, IA : Respecter et faciliter l'exercice des droits des personnes concernées, 07 février 2025.*

(iv) Tension en matière de mise en application des deux règlements.

Enfin, les autorités en charge de l'application du RIA pourraient être différentes de celles en charge de l'application du RGPD (lorsque le RIA ne prescrit pas la compétence des autorités de protection des données). À ce titre, la coopération entre les autorités concernées sera nécessaire pour éviter les divergences dans l'interprétation des principes applicables.

3. RIA, DORA et NIS 2

Bien qu'ayant des objectifs distincts, le RIA et la Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union (*Network and Information Security*) (**NIS 2**) peuvent interagir de manière résiduelle. En effet, la règlementation DORA agit comme *lex specialis* par rapport à NIS 2[173]. Il est précisé dans les deux textes que les États doivent en premier lieu appliquer DORA aux Institutions Financières, le tout en cohérence avec le cadre plus large de cybersécurité européen[174]. Si l'articulation de ces deux textes avec le RIA dépend de la transposition de NIS 2 en droit interne, plusieurs observations peuvent toutefois être soulevées.

En ce qui concerne la cybersécurité des Systèmes d'IA, le RIA impose des exigences strictes de robustesse et de sécurité pour les Systèmes d'IA à haut risque, tandis que NIS 2 renforce les obligations des organisations en matière de cybersécurité, incluant la protection des systèmes critiques utilisant l'IA. Par exemple, un Système d'IA utilisé pour la détection de fraudes dans les transactions bancaires devra simultanément répondre aux normes de sécurité du RIA et aux exigences de cybersécurité fixées par NIS 2, dans l'hypothèse où elles excèdent le cadre de DORA. On notera que le *Cyber Resilience Act*[175] (**CRA**) est également à prendre en considération en tant que texte complémentaire à NIS 2 couvrant les « *produits comportant des éléments numériques* », c'est-à-dire :

- « *un produit logiciel ou matériel et ses solutions de traitement de données à distance, y compris les composants logiciels ou matériels mis sur le marché séparément* »[176] ; et dont

[173] *On note que le projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité adopté par le Sénat le 13 mars 2025 cantonne la prédominance de la lex specialis DORA à la gestion des risques, la notification d'incidents et la supervision (article 62A).*

[174] *Considérant 28 de NIS 2 et considérant 16 de DORA.*

[175] *Règlement 2024/2847 du 23 octobre 2024 concernant des exigences de cybersécurité horizontales pour les produits comportant des éléments numériques.*

[176] *Article 3(1) du CRA.*

- « *la finalité prévue ou l'utilisation raisonnablement prévisible comprend une connexion de données logique ou physique directe ou indirecte à un appareil ou à un réseau* »[177].

Ce périmètre couvre les objets « *intelligents* »[178] au-delà du périmètre des IA à haut risque.

En matière de gestion des incidents, NIS 2 impose une notification rapide des incidents de cybersécurité qui ont un impact significatif. Si un Système d'IA est impliqué dans un incident, comme une attaque exploitant une vulnérabilité de ce système, cela peut nécessiter une double analyse pour s'assurer de la conformité aux deux cadres réglementaires (sans oublier la notification imposée par le RGPD[179]).

Les deux textes prévoient également des audits et des mécanismes de conformité réguliers. Les entités utilisant des Systèmes d'IA dans des secteurs critiques doivent ainsi coordonner leurs efforts afin de respecter les exigences des deux régimes.

C. L'appréhension des normes environnementales dans le cadre d'usage de l'IA/par le RIA

1. La durabilité, enjeu stratégique pour le secteur bancaire et financier

Le cadre de la durabilité est devenu depuis plusieurs années un enjeu stratégique visant à œuvrer en faveur du développement durable par le biais d'une transition vers des économies à bas carbone, respectueuses de l'environnement, utilisant efficacement les ressources et privilégiant l'équité et la justice sociale[180].

Dans le secteur bancaire et financier, les enjeux de durabilité environnementale, sociale et de gouvernance ne sont plus seulement une tendance mais un cadre général qui intègre une réflexion stratégique sur le financement de la transition économique. En témoignent les travaux européens

[177] *Article 2(1) du CRA*

[178] *Annexes III et IV du CRA.*

[179] *Cf. également les dispositions du règlement DORA sous réserve que les dispositions de ce dernier, en tant que lex specialis, l'emportent sur celles de NIS 2.*

[180] *L'expression « développement durable », apparaît pour la première fois en 1980 dans la* ***Stratégie mondiale de la conservation****, une publication de l'Union internationale pour la conservation de la nature (UICN). Cette notion est reprise, en 1987, dans le rapport de la* ***Commission mondiale sur l'environnement et le développement, Notre avenir à tous*** *(aussi appelé rapport Brundtland). C'est de ce rapport qu'est extraite la définition reconnue aujourd'hui : « Un développement qui répond aux besoins du présent sans compromettre la capacité des générations futures de répondre aux leurs. »*

mis en œuvre à la suite de la publication en mars 2018[181] du plan d'action pour financer une croissance durable, renouvelé en 2021 sous forme de stratégie en vue de financer les objectifs du Pacte vert pour l'Europe, à savoir, « *une société qui soit neutre pour le climat en 2050, efficace dans l'utilisation des ressources environnementales et qui accompagne les régions et les personnes particulièrement affectées par cette transition* »[182].

Le plan d'action européen sur la finance durable a conduit à des changements significatifs, le secteur bancaire et financier ayant été identifié comme étant clé pour faciliter une partie du financement de la transition économique. Avec l'adoption d'exigences légales et réglementaires strictes[183] et la sensibilisation accrue des parties prenantes, les Institutions Financières ont ainsi progressivement adopté les critères de durabilité environnementale en les intégrant dans les différents aspects de l'activité bancaire et financière : stratégies et décisions d'investissement, financements de projets et d'actifs, cadre de gestion des risques, publications en matière de durabilité etc.

Dans le cadre de la mise en œuvre des nouvelles obligations liées à la durabilité environnementale, les Institutions Financières ont identifié qu'un large éventail de questions devaient être traitées parallèlement à d'autres risques plus traditionnels.

Ces questions et enjeux concernent notamment l'évaluation et la comparaison des performances de durabilité environnementale de différents investissements alors que les données ESG fiables et standardisées sont rares ou non existantes. L'adaptation à un cadre légal et règlementaire qui, en matière de durabilité environnementale, évolue rapidement et varie considérablement d'une juridiction à l'autre peut également s'avérer complexe. Un autre défi de taille est l'intégration des critères de durabilité environnementale dans les modèles financiers et les processus décisionnels existants tout en tenant compte de manière adéquate des risques et des opportunités ESG.

Ces nouvelles problématiques nécessitent des modifications et des ajustements techniques qui peuvent s'avérer complexes et consommateurs de ressources importantes.

---

[181] *Communication de la Commission au Parlement européen, au Conseil européen, au Conseil, à la Banque centrale européenne, au Comité économique et social européen et au Comité des régions, Action Plan: Financing Sustainable Growth, le 8.3.2018 COM (2018) 97 final.*

[182] *Communication de la Commission au Parlement européen, au Conseil européen, au Conseil, à la Banque centrale européenne, au Comité économique et social européen et au Comité des régions, Stratégie pour le financement de la transition vers une économie durable, le 6.7.2021 COM (2021) 390 final.*

[183] *Voir notamment, le règlement (UE) 2019/2088 du Parlement européen et du Conseil du 27 novembre 2019 sur la publication d'informations en matière de durabilité dans le secteur des services financiers, le règlement (UE) 2020/852 du Parlement européen et du Conseil du 18 juin 2020 sur l'établissement d'un cadre visant à favoriser les investissements durables et modifiant le règlement (UE) 2019/2088, les informations à publier au titre de l'article 449 du règlement n° 575/2013 relatif aux exigences prudentielles applicables au établissements de crédit.*

La capacité de l'IA à analyser de vastes ensembles de données de manière efficace et précise peut représenter un atout clé dans la gestion de la durabilité environnementale. Par exemple, l'IA pourrait traiter et interpréter des données environnementales à grande échelle, ce qui permettrait aux institutions financières d'évaluer les risques financiers liés au climat avec plus de précision et de prudence.

Dans cette perspective, l'IA pourrait s'imposer comme un outil essentiel pour naviguer dans l'interaction complexe des activités financières et des objectifs de durabilité environnementale.

Cependant si l'essor soudain de l'IA promet de transformer avec succès l'intégration de la durabilité dans le secteur financier, il présente également de nouvelles complexités pour les acteurs impliqués dans la finance durable.

L'un des impacts directement lié à l'objectif de développement durable défini en 1987 dans le rapport « *Brundtland* » comme étant « *un développement qui répond aux besoins du présent sans compromettre la capacité des générations futures de répondre à leurs propres besoins* » concerne les dégâts sur l'environnement que provoquerait l'utilisation sans discernement de l'IA dans le secteur financier.

Certes, la transposition de la directive CSRD en droit français et le devoir de vigilance imposent de veiller au respect de l'environnement à un grand nombre d'entités du secteur financier et de divulguer leurs impacts environnementaux. Mais ces textes n'imposent pas d'exigences environnementales particulières, afférentes à la création et à l'utilisation de l'IA.

Faut-il en déduire que d'autres textes régissent l'impact de l'IA et du numérique sur l'environnement ?

2. La place de l'environnement dans le RIA

Le RIA contient un certain nombre de dispositions qui visent explicitement l'environnement et qui tendent à améliorer la transparence sur les incidences de l'IA en ce domaine (cf : considérant n° 27 : « *les systèmes d'IA sont développés et utilisés d'une manière durable et respectueuse de l'environnement* » ; considérant n° 48 : « *Le droit fondamental à un niveau élevé de protection de l'environnement, consacré dans la Charte et mis en œuvre dans les politiques de l'Union, devrait également être pris en considération lors de l'évaluation de la gravité du préjudice qu'un système d'IA peut causer* » ; considérant n° 165 : « *Les fournisseurs et, le cas échéant, les déployeurs de tous les systèmes d'IA, à haut risque ou non, et modèles d'IA devraient aussi être encouragés à appliquer sur une base volontaire des exigences supplémentaires liées, par exemple, aux éléments des lignes directrices de l'Union en matière d'éthique pour une IA digne de confiance, à la durabilité environnementale (…)* » ; article 95, 2, b : « *Le Bureau de l'IA et les États membres facilitent l'élaboration de codes de conduite concernant l'application volontaire, y compris par les déployeurs, d'exigences spécifiques à tous les systèmes d'IA, sur la base d'objectifs clairs et d'indicateurs de performance clés permettant de mesurer la réalisation de ces objectifs, y compris des éléments tels que, entre autres, (…) l'évaluation et la réduction au minimum de l'incidence des systèmes*

d'IA sur la durabilité environnementale, y compris en ce qui concerne la programmation économe en énergie et les techniques pour la conception, l'entraînement et l'utilisation efficaces de l'IA ».).

S'agissant des impacts environnementaux de l'IA, la réglementation européenne ne définit pas de normes de durabilité des Systèmes d'IA en tant que telles, renvoyant la responsabilité d'une telle définition aux États membres[184]. Le RIA doit donc être mis en miroir du droit interne français, pour envisager notamment les éventuelles conséquences juridiques de la transparence des incidences environnementales des Systèmes d'IA.

3. L'empreinte environnementale du numérique en droit français

Pris par des injonctions contraires, à savoir la promotion d'une économie favorable au numérique tout en assumant une politique de lutte contre le changement climatique et les émissions de carbone, le législateur français a trouvé un point d'équilibre avec la loi n° 2021-1485 du 15 novembre 2021 visant à réduire l'empreinte environnementale du numérique en France (dite loi REEN). Cette loi a pour objectif de rendre visibles les coûts écologiques cachés du numérique, en incitant les entreprises à adopter des pratiques numériques plus responsables, en mettant l'accent sur la sensibilisation, l'écoconception, la gestion durable des équipements et l'efficacité énergétique des infrastructures. Or, à l'occasion des débats parlementaires, une disposition visant à inscrire l'impact environnemental du numérique dans la déclaration de performance extra financière des entreprises a été proposée avant d'être supprimée à l'issue du processus parlementaire. Il est remarquable que le législateur ait ainsi envisagé une transparence de l'empreinte environnementale liée au numérique dans le cadre des informations publiées en application du droit des sociétés. Si la proposition n'a pas été retenue à ce stade, elle révèle une tendance très nette à faire de l'empreinte environnementale un nouvel « *indicateur* » ou à tout le moins un élément de la reddition de comptes des entreprises[185]. Dès lors, il faut être vigilant sur la réception de cette transparence environnementale auprès des investisseurs et envisager les éventuelles incidences juridiques de ces informations au regard de l'exigence d'information « *exacte, précise et sincère* » (article 223-1, RG AMF). Outre la nécessité d'une transparence environnementale, l'impact que peut avoir l'usage du numérique et des Systèmes d'IA pourrait faire l'objet d'une analyse coût-avantage de la part des Institutions Financières. Celles-ci pourraient ainsi mettre en balance, d'une part les bénéfices apportées par l'utilisation de l'IA et, d'autre part le coût environnemental que cette technologie pourrait engendrer, notamment lorsqu'elle est utilisée pour accomplir certaines tâches à la place de technologies préexistantes[185bis].

---

[184] *Rapport au Sénat n° 379, 2024-2025, L'IA et l'avenir du service public, p. 37.*

[185] *Marina Tellier, De la RSE à la RNE : la petite lettre qui change tout, Mélanges AEDBF, volume 8, Revue Banque, 2022, (hal-03480269).*

[185bis] *ESMA, Institut Louis Bachelier, The Alan Turing Institute, Leveraging Large Language Models in Finance: Pathways to Responsible Adoption, Working papers, 2025, p. 24.*

D. L'articulation des dispositifs de protection de la propriété intellectuelle avec le RIA

1. La Directive sur le droit d'auteur et les droits voisins dans le marché numérique et le RIA

En Europe, la Directive sur le droit d'auteur et les droits voisins dans le marché numérique (la **Directive (UE) 2019/790 du 17 Avril 2019**) avait introduit une exception pour les fouilles de texte et de données (*text and data mining* - TDM) qui permettait l'utilisation de contenus protégés à des fins de recherche et d'innovation.

En vertu de ces règles, les titulaires de droits peuvent choisir de réserver leurs droits sur leurs œuvres et autres objets protégés afin d'empêcher l'exploration de textes et de données, à moins que cela ne soit fait à des fins de recherche scientifique. Lorsque la réserve de droits a été expressément effectuée de manière appropriée, les fournisseurs de modèles d'IA à usage général doivent obtenir une autorisation des titulaires de droits s'ils souhaitent effectuer des fouilles de textes et de données sur ces œuvres (considérant n° 105 du RIA).

Les références à la propriété intellectuelle sont peu nombreuses dans le RIA, néanmoins l'article 53 du RIA intègre des obligations à ce sujet : « *1. Les fournisseurs de modèles d'IA à usage général : […] c) mettent en place une politique visant à se conformer au droit de l'Union en matière de droit d'auteur et droits voisins, et notamment à identifier et à respecter, y compris au moyen de technologies de pointe, une réservation de droits exprimée conformément à l'article 4, paragraphe 3, de la directive (UE) 2019/790* »

Néanmoins, la mise en pratique de ces dispositions soulève encore de nombreuses questions, non seulement pour les fournisseurs mais aussi pour les déployeurs ou utilisateurs d'IA.

2. Les utilisateurs d'IA et les droits de propriété intellectuelle

Les données utilisées pour rédiger des prompts ou pour alimenter les Systèmes d'IA peuvent contenir des informations protégées par des droits de propriété intellectuelle mais aussi des informations sensibles protégées par les lois relatives aux secrets commerciaux ou aux secrets bancaires. Les utilisateurs d'IA peuvent ne pas être conscients que les données qu'ils exploitent pourraient enfreindre de la propriété intellectuelle ou des secrets commerciaux ou encore violer des obligations de confidentialité.

Il est essentiel que les utilisateurs soient formés et informés sur les implications juridiques de l'utilisation des données de ce type, ainsi que sur les risques associés à l'exploitation d'informations potentiellement protégées par des droits spécifiques tels que les secrets commerciaux.

Un guide de bonne pratique dédiée aux utilisateurs peut réduire ce type de risques liés à leur input, en leur demandant notamment de :

- ne pas utiliser lors de l'usage de l'outil d'IA des données protégées par la propriété intellectuelle ou bien des données confidentielles/secrets commerciaux/professionnels de la société de l'utilisateur ;

- vérifier que le résultat des prompts faites sur l'outil n'enfreint pas l'obligation de protection de certaines données à travers des recherches sur Google ou d'autres moteurs de recherche ;

- étudier les conditions et termes d'usage de l'outil IA en ce qui concerne l'usage fait des données fournies.

3. Les fournisseurs et leur modèle d'entraînement IA et les déployeurs confrontés aux droits de propriété intellectuelle

Les données utilisées pour entraîner des modèles d'IA peuvent inclure des œuvres protégées par des droits de propriété intellectuelle, telles que des textes, des images ou des enregistrements sonores.

Le RIA définit des exigences sur les activités des fournisseurs et des déployeurs même si les références à la propriété intellectuelle dans le RIA sont limitées.

L'article 53 du RIA dispose que les fournisseurs de modèles d'IA à usage général doivent mettre en place des mesures pour garantir le respect du droit d'auteur, conformément à la Directive (UE) 2019/790 du 17 Avril 2019. Parmi ces mesures, les fournisseurs sont tenus de créer et de rendre accessible au public « *un résumé suffisamment détaillé* » des données utilisées pour entraîner le modèle d'IA.

Cette exigence de transparence sur les sources devrait permettre aux titulaires de droits d'auteur et de droits voisins de s'assurer que les conditions d'accès et d'utilisation de leurs œuvres ont été respectées et, le cas échéant, de faire valoir leur droit d'opposition à toute exploitation de leurs données, c'est-à-dire leur « *opt-out* ». Cette obligation prendra effet douze mois après l'entrée en vigueur du règlement, soit le 2 août 2025. Le Bureau de l'IA, établi par une décision de la Commission européenne le 24 janvier 2024, sera chargé de concevoir un modèle de résumé clair et efficace des données d'entraînement utilisées par les IA. L'obligation de respecter le droit d'auteur et de fournir ce résumé s'appliquera aux fournisseurs d'IA proposant des modèles au sein de l'UE, peu importe le lieu où ces modèles ont été entraînés.

Dans la troisième version de projet de code de pratiques pour les modèles d'IA généraliste (GPAI) publié par le Bureau de l'IA le 11 mars 2025, il est mentionné que les fournisseurs qui signeront ce code reconnaissent que toute utilisation d'un contenu protégé par le droit d'auteur nécessite l'autorisation du ou des titulaires de droits concernés, à moins que des exceptions et limitations au droit d'auteur ne s'appliquent (cf. considérant n° 105 du RIA).

La section sur le droit d'auteur du code de bonnes pratiques établit des engagements que les fournisseurs de modèles d'IA à usage général doivent respecter pour se conformer à la législation de l'UE. Ce projet vise à simplifier et clarifier les obligations par rapport aux versions précédentes, tout en maintenant les éléments essentiels.

Le troisième projet de code de bonnes pratiques pour l'IA à usage général inclut une section sur le droit d'auteur, définissant des engagements pour les fournisseurs de modèles d'IA. Cette section vise à assurer la conformité avec la législation de l'Union sur le droit d'auteur, conformément à l'article 53(1) c) du RIA.

Les principaux points sont les suivants :

(a) politique de conformité : les signataires doivent élaborer, mettre à jour et mettre en œuvre une politique en matière de droit d'auteur, qui inclut des engagements spécifiques pour respecter le droit d'auteur et les droits voisins ;

(b) mesures spécifiques : les signataires doivent également élaborer une politique en matière de droit d'auteur, documentée et supervisée au sein de l'organisation. Ils s'assureront que seuls les contenus légalement accessibles sont reproduits ou extraits lors de l'exploration Web. Ils devront identifier et respecter les réserves de droits lors de l'exploration, obtenir des informations adéquates sur le contenu protégé non exploré, atténuer les risques que les modèles d'IA génèrent des résultats portant atteinte aux droits d'auteur, et désigner un point de contact pour la communication avec les titulaires de droits et établir un mécanisme de dépôt de plaintes ;

(c) proportionnalité : les engagements doivent être adaptés à la taille et aux capacités des signataires, en tenant compte des petites et moyennes entreprises ;

(d) respect du droit d'auteur : la section ne diminue pas l'application des lois existantes sur le droit d'auteur et les accords commerciaux entre signataires et titulaires de droits.

Ce code vise à établir un cadre clair pour que les fournisseurs de modèles d'IA respectent les droits d'auteur, tout en intégrant des mécanismes de communication et de responsabilité.

4. Les créations générées par l'IA

L'émergence de l'IA soulève aussi des questions importantes concernant les œuvres qu'elle génère. La titularité des droits d'auteur sur ces créations est un sujet de débat juridique significatif.

4.1 - Titularité des droits d'auteur

La question de savoir qui devient titulaire des droits sur les créations générées par l'IA est complexe. Dans de nombreux cas, les conditions générales d'utilisation (CGU) des outils d'IA stipulent que les droits peuvent être cédés aux utilisateurs. Cependant, il est crucial de s'interroger sur la clarté de ces cessions et sur les droits qui sont réellement transférés.

Il convient de distinguer deux scénarios : celui des **créations générées de manière autonome**. Lorsque l'IA produit un contenu sans intervention humaine, la titularité des droits peut être floue et dépendra des stipulations contractuelles. Dans ces cas, il y aura un risque à utiliser ce type d'œuvres puisqu'elles pourront être copiées si elles ne bénéficient pas de la protection des droits de propriétés intellectuelle (sous réserve des cas de parasitisme etc.). Et un second scénario de **créations assistées par l'IA** : lorsque l'utilisateur modifie le contenu généré par l'IA, cela pourrait renforcer la revendication de droits d'auteur par l'utilisateur, surtout s'il apporte une contribution créative significative.

4.2 - Risques associés à l'exploitation du contenu généré par l'IA

L'exploitation du contenu généré par l'IA comporte également des risques juridiques, notamment en matière de contrefaçon. Si l'IA génère un contenu qui est similaire ou identique à une œuvre protégée, deux cas de figure peuvent se présenter. D'une part, le fournisseur devra une indemnisation : certains fournisseurs d'outils d'IA proposent dans leurs conditions générales une indemnisation en cas de contrefaçon, à condition que l'utilisateur n'ait pas commis de faute et avec certaines limites de montant ou des limites concernant certaines garanties pour l'image des biens ou des personnes représentées. Cela protège dans une certaine mesure les utilisateurs, mais ils doivent tout de même faire preuve de diligence dans l'utilisation des outils. D'autre part, la responsabilité de l'utilisateur pourra être mise en œuvre dans d'autres cas où le fournisseur décline toute responsabilité, et l'utilisateur doit assumer la totale responsabilité de l'exploitation du contenu généré. Cela pose des défis pour les utilisateurs qui peuvent ne pas être pleinement conscients des implications juridiques de leurs choix.

IV. Enjeux de responsabilité pour les Institutions Financières

A. Une responsabilité pleine et entière des Institutions Financières vis-à-vis de leurs clients/investisseurs et des autorités de supervision

Le RIA ainsi que les dispositions européennes sectorielles, comme MiCA ou DORA, sont des règles *ex ante* définissant des obligations pour les opérateurs.[186] Ces règles constituent l'essentiel du cadre juridique applicable mais ne contiennent pas, ou par exception, de règles relatives à la responsabilité des opérateurs soumis à leurs dispositions. Elles prévoient habituellement des sanctions en cas de violations des obligations qu'elles imposent, dont l'objet n'est toutefois pas de réparer les dommages subis par les victimes éventuelles et causés par l'activité des opérateurs. En ce qui concerne le traitement *ex post* des dommages causés par l'utilisation de technologies informatiques et notamment par l'IA, le cadre juridique, européen comme national, est encore relativement incertain, notamment suite au retrait de la proposition de directive du 28 septembre 2022 relative à l'adaptation des règles en matière de responsabilité civile extracontractuelle au domaine de l'IA. Ce retrait est à ce stade regrettable si l'on considère le risque de dommage, de nature variable, causé par l'usage fréquent et en augmentation de Systèmes d'IA. Le risque de dommage, nouveau, est lié aux caractéristiques des technologies employées, à savoir leur complexité, opacité, autonomie, imprévisibilité, ouverture vers l'extérieur, dépendance aux données et leur vulnérabilité.

Les risques générés par les Systèmes d'IA et par d'autres technologies informatiques sont particulièrement importants dans des secteurs comme celui des services financiers où le dysfonctionnement de Systèmes d'IA est susceptible d'avoir des impacts importants tant au niveau de la protection des individus (e.g. un *robo-adviser* à l'origine d'erreurs pouvant causer un lourd préjudice économique à un investisseur particulier), qu'à celui de la stabilité des marchés.

Les principales hypothèses liées à l'usage des technologies en question qui pourraient être à l'origine de dommages et donc de responsabilité sont : le *credit scoring*, l'utilisation de *robot advisors*, le *trading* à haute fréquence, l'organisation interne des établissements et la gestion de la conformité et du risque. Quant aux caractéristiques des technologies d'IA à l'origine d'un risque accru de responsabilité, il s'agit principalement :

- de l'entrainement des modèles/algorithmes sur la base de données insuffisamment pertinentes, non représentatives, insuffisantes et reproduisant des biais existant dans la société ;

[186] *Ces règles sectorielles peuvent renvoyer aux règles de responsabilité civile, le plus souvent nationales, en cas de dommages causés par les manquements aux obligations qu'elles contiennent, mais sans plus de détails quant au contenu des règles, le fondement de la responsabilité et son régime.*

- de l'interconnexion avec d'autres systèmes ou sources de données (notamment dans le *credit scoring* ou le *trading* à haute fréquence) pouvant désavantager des emprunteurs ou bien nuire au bon fonctionnement de l'algorithme de *trading* ;

- de l'utilisation de données externes rendant imprévisible l'évolution des systèmes auto-apprenants ; de la vulnérabilité aux cyberattaques et aux fuites de données, personnelles et confidentielles. Les risques de responsabilité engendrés existent pour les développeurs et fournisseurs des technologies en question mais aussi pour ceux qui les utilisent.

En effet, plus les établissements financiers utilisent des systèmes et applications d'IA, plus le lien entre les règles juridiques applicables aux marchés financiers, d'une part, et les règles de responsabilité, d'autre part, est susceptible de se resserrer.[187] L'articulation entre ces deux corps de règles doit dès lors faire l'objet d'une analyse précise et progressive compte tenu du contexte législatif évolutif en la matière. Par la même occasion, il devient plus complexe d'évaluer la responsabilité et la conformité à la législation applicable sans une gouvernance très structurée.[188] Les règles de responsabilité (actuelles ou à venir, applicables spécifiquement à l'IA), particulièrement celles européennes, auront donc un impact plus important sur les établissements financiers à la mesure du recours par ces derniers à l'IA et à d'autres technologies informatiques dans la conception et la prestation des services réglementés concernés. Les règles de responsabilité vont en quelque sorte rendre plus effectives les obligations découlant des règles ex ante applicables aux Institutions Financières (RIA et réglementation sectorielle).

Les responsabilités que les Institutions financières sont susceptibles d'endosser du fait de l'utilisation de Systèmes d'IA peuvent donc être multiples. Lesdites responsabilités peuvent varier en fonction de la contribution plus ou moins importante de l'Institution Financière à l'élaboration du Système d'IA qui sera en cause dans la violation de normes impératives et/ou dans la production de préjudices. En effet, le domaine de la responsabilité découle est d'autant plus large que la catégorie des opérateurs est vaste.[189] Au gré des circonstances, il s'agira de rechercher le fait générateur de responsabilité le plus pertinent (conception ou utilisation et modification du système) et de désigner le responsable le plus approprié.

---

[187] *Les corps de règles sectorielles et le RIA, d'une part et les règles de responsabilité, d'autre part, sont destinés à s'intégrer davantage (eg. obligation de surveillance des établissements financiers valant obligations du déployeur au titre de l'article 26 RIA).*

[188] *ESMA, Artificial Intelligence in EU securities markets, (2023) https://www.esma.europa.eu/sites/default/files/library/ESMA50-164-6247-AI_in_securities_markets.pdf.*

[189] *Voir article 3(8) RIA : « opérateur », un fournisseur, fabricant de produits, déployeur, mandataire, importateur ou distributeur.*

Quant aux rapports avec les clients/investisseurs, il conviendra d'envisager des manquements contractuels classiques mettant en cause un Système d'IA (e.g. mauvais conseils…), pour lesquels l'emploi de Systèmes d'IA ne devrait pas changer radicalement la façon dont est envisagée la responsabilité par rapport à la situation actuelle, si ce n'est que les hypothèses de manque d'une supervision humaine suffisante pourraient être plus nombreuses. Les dommages qui sont susceptibles d'être causés en l'occurrence et la responsabilité (contractuelle comme extracontractuelle en découlant) sont somme toute classiques. En ce qui concerne les clients professionnels, des clauses contractuelles limitatives ou exonératoires classiques, légèrement adaptées à l'usage de Systèmes d'IA devraient permettre de maintenir l'exposition de responsabilité à des niveaux comparables à ceux actuels. Une telle démarche sera plus complexe face à des clients particuliers, considérés dès lors comme des consommateurs, pouvant se prévaloir notamment du droit relatif aux clauses abusives (e.g. clauses limitatives ou exonératoires de responsabilité considérées comme abusives), de l'arsenal relatif au formalisme contractuel et au devoir d'information, des règles de bonne conduite applicables, voire du droit relatif aux pratiques commerciales déloyales. Un point de vigilance particulier doit dès lors être fait dans l'usage de Systèmes d'IA vis-à-vis de clients ayant la qualité de consommateurs.

À l'inverse, des dommages en partie d'une nouvelle nature doivent aussi être considérés. En effet, les Systèmes d'IA, du fait notamment de données en entrée insuffisantes ou de qualité approximative, mais aussi de biais susceptibles de s'immiscer dans les mécanismes d'apprentissage machine, génèrent des dommages qui relèvent largement du domaine des dommages extrapatrimoniaux (e.g. atteinte à la dignité, discrimination…), dont l'ampleur peut être particulièrement significative. Ces dommages d'une nouvelle nature devront être examinés plus précisément car ils sont inhérents à l'usage de Systèmes d'IA.

Par ailleurs, la Directive (UE) 2020/1828 du 25 novembre 2020 relative aux actions représentatives peut constituer également un point d'attention. En effet, le RIA fait partie des textes entrant dans le domaine de cette directive, ouvrant ainsi la voie à des actions représentatives en raison d'infractions commises par des professionnels aux dispositions du droit de l'UE. Ladite directive n'a vraisemblablement pas fait l'objet de transposition en droit français pour l'heure mais peut entrainer un changement significatif dans l'exposition de responsabilité, particulièrement si l'on tient compte du développement du *third party funding*.

B. Un dispositif en gestation pour la responsabilité extracontractuelle

Les règles de responsabilité civile du fait de l'IA au niveau européen sont pour l'instant assez limitées, tout du moins jusqu'à l'entrée en application à venir de la nouvelle directive « *produits défectueux* ». Cette directive du 23 octobre 2024 doit être transposée dans les droits des États membres dans un délai de deux ans après sa publication. Ainsi, pour l'instant, les dommages découlant de l'usage de Systèmes d'IA seront réparés sur le fondement des règles nationales de

responsabilité extracontractuelle et/ou contractuelle (voire sur le fondement de règles nationales spécifiques aux dommages causés par l'IA). Il est à noter que le législateur européen a introduit des règles de responsabilité propres aux marchés financiers, comme celle des agences de notations de crédit (e.g. CRAR), des entreprises d'investissement, ou bien, plus récemment celle des émetteurs d'actifs numériques (MiCA), qui seront appliquées en parallèle des règles de responsabilité partiellement propres à l'IA.

La responsabilité du fait des produits défectueux s'applique aux produits et non pas aux services, cette dernière responsabilité étant généralement fondée sur la faute. Le régime de responsabilité des produits défectueux est dit sans faute car le fondement de cette responsabilité est la défectuosité du produit. Si cette défectuosité est à l'origine d'un dommage, alors le producteur/fabricant sera responsable. La nouvelle directive a un champ d'application plus vaste que sa précédente version. Elle s'applique en effet au-delà de la catégorie des producteurs au sens strict (tous les « *opérateurs économiques* » mentionnés à l'article 8). À cet égard, il convient de noter qu'un opérateur économique peut être soumis à la responsabilité du fait des produits défectueux et donc assimilé à un fabricant lorsqu'il « *modifie de manière substantielle un produit en dehors du contrôle du fabricant et le met ensuite à disposition sur le marché ou en service* ». Il conviendra à l'avenir de déterminer si des déployeurs de Systèmes d'IA ou des utilisateurs de technologies informatiques seront assimilée à des fabricants et soumis à ce régime de responsabilité, parce qu'ils auront modifié, au travers de l'entrainement local par exemple des systèmes, de manière substantielle ce type de produits.

Ceci d'autant plus que, quant à son champ d'application matériel, la nouvelle directive relative à la responsabilité du fait des produits défectueux englobe formellement les softwares dans la catégorie des produits. Ainsi, si un établissement financier développe en local un programme/algorithme, par exemple de *credit scoring*, que ce programme intègre ou pas de l'IA d'ailleurs, il pourrait en théorie être considéré comme un producteur au sens de la nouvelle directive produits défectueux. La mise à disposition des clients de ces produits pourrait alors être assimilé à une mise en circulation ou une mise sur le marché du produit, élément déclencheur du risque de responsabilité.

Notons que la directive « *produits défectueux* » ne couvre que le dommage matériel, mais pas le dommage moral (pour ce dommage, il faudra s'en remettre au droit national, ce qui sera le cas par exemple et selon toute vraisemblance pour les cas de discrimination, de perte de chance, de préjudice d'anxiété, etc.), ni la perte purement financière (*pure economic loss*).

La proposition de directive du 28 septembre 2022 relative à l'adaptation des règles en matière de responsabilité civile extracontractuelle au domaine de l'IA, retirée du programme législatif de la Commission européenne en février 2025, visait à établir un régime essentiellement basé sur la faute, pouvant découler notamment du non-respect de dispositions *ex ante*, telles que le RIA. Son apport principal devait se situer dans le domaine de l'accès aux informations détenues par le défendeur (*disclosure*), d'une part, et dans l'établissement de présomptions (faute et causalité entre la faute et l'output d'une IA causant un dommage) profitant au demandeur, d'autre part. Les

dispositions de la proposition de directive se concentraient essentiellement sur les Systèmes d'IA à haut risque. Malgré ses imperfections, cette proposition de directive avait le mérite d'introduire une articulation entre le corpus de règles *ex ante* (RIA) et celui des règles *ex post* (directive sur la responsabilité extracontractuelle pour les dommages causés par l'IA).

À ce stade, l'articulation se fera selon toute vraisemblance avec les règles nationales de responsabilité, d'une part, et avec les règles de la directive relative à la responsabilité du fait des produits défectueux, d'autre part. Dans l'attente d'un régime propre de responsabilité civile pour les dommages causés par l'IA, rien ne semble s'opposer à ce que les manquements aux différentes obligations découlant du RIA et des règles sectorielles permettent de caractériser la faute déclenchant une responsabilité. Même si pour l'instant les règles d'accès aux documents et de présomptions que contenait la proposition de directive sur la responsabilité extracontractuelle pour les dommages causés par l'IA ne sont plus d'actualité, il semble important de mettre l'accent sur la formation des personnels déployant des Systèmes d'IA, de même que sur le contrôle et la documentation de l'usage de ces systèmes.

C. Une responsabilité contractuelle des fournisseurs d'IA à négocier

Il faut envisager les différentes positions occupées par les Institutions Financières. En tant que clients, les Institutions Financières faisant appel à des prestataires de services de Systèmes d'IA devront veiller à ce que les éventuelles clauses limitatives ou exonératoires proposées par lesdits prestataires ne soient pas excessivement larges car les risques de responsabilité pour le déployeur de Systèmes d'IA sont assez importants. Les Institutions Financières pourront souhaiter à l'inverse stipuler des clauses en vertu desquelles les dommages subis du fait de l'usage des Systèmes d'IA fournis, comme le dommage de réputation, feront l'objet d'une réparation par le cocontractant.

En tant que déployeurs de Systèmes d'IA, les Institutions Financières veilleront à stipuler des clauses limitatives ou exonératoires de leur responsabilité pour les dommages causés par l'usage de Systèmes d'IA, ce qui ne sera envisageable que dans les relations avec des clients professionnels.

Si les Institutions Financières sont assimilées à des fournisseurs ou des producteurs de Systèmes d'IA, le régime de responsabilité encouru étant notamment celui fondée sur la responsabilité du fait des produits défectueux, la voie de clauses limitatives ou exonératoire de responsabilité ne pourra être invoquée dans la mesure où ce régime de responsabilité est extracontractuel.

CONCLUSION

L'usage de l'IA par les Institutions Financière est soumis non seulement à des réglementations sectorielles très établies mais aussi à une réglementation spécifique foisonnante sujette à interprétation[189bis].

L'exercice d'articulation des corpus réglementaires relève parfois de l'équilibrisme avec une prise de risque à la clé.

Trois niveaux d'incertitudes ont été particulièrement relevés :

- l'autorité de surveillance des Institutions Financières pour l'application du RIA n'a pas encore été formellement désignée en France – une fois sa désignation intervenue, il faudra déterminer comment vont s'articuler demain le contrôle de la mise en œuvre du RIA et les régimes disciplinaires qui s'appliquent d'ores et déjà aux Institutions Financières.

Un défi supplémentaire apparait également au niveau de la coordination européenne. Si les autres États Membres venaient à suivre l'exemple français et divisaient les prérogatives liées à l'application du RIA entre plusieurs autorités, l'harmonisation des pratiques pourrait s'en trouver affectée et des divergences d'interprétation pourraient apparaître. À cela s'ajoute un risque de décrochage - volontaire ou non - de certains États Membres créant ainsi des disparités d'application du RIA pouvant inciter certains acteurs à s'installer dans un pays plutôt qu'un autre. Pour pallier ces divergences, il pourrait être opportun de mettre en avant une autorité par État Membre qui serait chargée de faire le lien avec les autorités européennes. Ainsi, les autorités, nationales comme européennes, devront coopérer afin de se livrer ensemble à un travail de pédagogie cohérent, à l'initiative notamment du Bureau de l'IA et de la Commission européenne ;

- l'intégration des nouvelles obligations du RIA dans le domaine normatif des Institutions Financières, les mécanismes d'équivalence ou de complémentarité des règles du RIA avec les réglementations sectorielles demeurant largement sujets à interprétation ; et

- l'articulation du RIA avec les autres réglementations transversales régissant d'ores et déjà les Institutions Financières, notamment le RGPD et DORA, ajoute un niveau de complexité supplémentaire.

Si les usages de l'IA présentent indéniablement des moyens de développement et d'efficience pour les Institutions Financières, le surpoids normatif à la clé va peser dans la décision d'y recourir. Le

[189bis] *Tel que souligné dans le rapport publié par l'ESMA, l'Institut Louis Bachelier et le Alan Turing Institute, la grande majorité des juridictions consultées par l'OCDE ont indiqué avoir adopté une politique en matière d'IA couvrant, au moins en partie, le secteur bancaire et financier (ESMA, Institut Louis Bachelier, The Alan Turing Institute, Leveraging Large Language Models in Finance: Pathways to Responsible Adoption, Working papers, 2025, p. 28).*

RIA fondé sur la protection des droits fondamentaux ouvre également un territoire peu commun pour les Institutions Financières avec des enjeux de responsabilité qui leur sont propres.

L'impact de l'application du RIA sur la compétitivité des Institutions Financières européennes est également une préoccupation rendant impérative la capacité de l'Union Européenne à le faire appliquer extra-territorialement. Notons que dans son rapport « *The Future of European Competitiveness* » (9 septembre 2024), Mario Draghi précisait que les charges règlementaires pesant sur les chercheurs et développeurs d'IA en Europe constituent un réel frein au développement des projets d'IA par les acteurs de l'industrie européenne et pourrait à terme les inciter à développer leurs SIA en dehors de l'UE.

Cette pyramide d'enchevêtrements de textes encadrant l'usage de l'IA a naturellement conduit le groupe de travail à ne pas proposer d'autres textes[190] voire des modifications de textes existants mais plutôt à mener ces travaux d'analyse d'articulation.

Il a été salué toutes les initiatives notamment celles portées par la Commission européenne[191] pour clarifier les articulations entre les réglementations s'appliquant au recours à l'IA par les Institutions Financières.

Dans la lignée du plan d'action européen en matière d'IA[192], le groupe de travail appelle de ses vœux les autorités de supervisions et les législateurs à répondre au mieux aux demandes de simplification et de clarification des Institutions Financières en vue de favoriser une véritable cohérence des réglementations sectorielles, transversales avec celles régissant l'IA spécifiquement.

---

[190] *Cette position est alignée avec celle du projet de rapport de l'ECON en date en 14 mai 2025 : "[The European Parliament] warns against the adoption of new sectoral legislation to regulate AI in financial services, as there are already established sectoral rules that cover AI deployment; believes that this would create additional layers of complexity and uncertainty and ultimately deprive the sector of the benefits of AI use; strongly advises the Commission and the Member States to coordinate to avoid gold-plating relevant legislation and to prevent the creation of new barriers in cross-border markets; […]*
The alternative is to take a restrictive approach to AI deployment in finance, with new legislation out of fear of the unknown effects, or because status quo is comfortable. Such a policy would deprive the financial services sector of the opportunity to use AI. […]. Such a route should be off the table considering the global race for AI, the stark geopolitical realities underpinning it, and the fact that the EU is already lagging behind." (Parlement Européen, ECON, Draft report on impact of artificial intelligence on the financial sector (2025/202565INI)), 14 mai 2025.

[191] *Commission européenne, Consultation document – Target consultation on artificial intelligence in the financial sector, 18 juin 2024.*

[192] *Commission européenne, Communication from the commission to the European parliament, the council, the European economic and social committee and the committee of the regions – AI Continent Action Plan, 9 avril 2025, p. 3 : « Fifth, the EU's large single market is a significant asset, with one set of clear rules, including the AI Act, preventing market fragmentation and enhancing trust and security in the use of AI technologies. Nevertheless, there is a need to facilitate compliance with the AI Act, particularly for smaller innovators. » ; p. 22 : « The Commission will continue to work with the AI Board of Member States, which assists in providing guidance on the application of the AI Act, including within the context of sectoral legislation. » and p. 23 : « […] we should first gain experience in applying these new horizontal rules and evaluate their effect before any possible new legislation on AI can be considered. ».*

ANNEXE 1

Composition du groupe de travail

COMPOSITION DU GROUPE DE TRAVAIL

sur les impacts juridiques et règlementaires de l'intelligence artificielle en matière bancaire, financière et des assurances

PRÉSIDENT

- **Brice HENRY,** Avocat Associé, Allen Overy Shearman Sterling LLP

VICE-PRÉSIDENTE

- **Laurie-Anne ANCENYS,** Avocate Associée, Allen Overy Shearman Sterling LLP

RAPPORTEURS

- **Maxence KIEKEN,** Avocat, Allen Overy Shearman Sterling LLP
- **Constantin BEYTOUT,** Avocat, Allen Overy Shearman Sterling LLP
- **Pascal MOLINELLI,** Avocat Counsel, Allen Overy Shearman Sterling LLP
- **Morgane-Aude ROUSSEL,** Avocate, Allen Overy Shearman Sterling LLP

REPRÉSENTANTS DU HCJP

- **Jean-Guillaume DE TOCQUEVILLE,** Secrétaire Général, Haut Comité Juridique de la Place financière de Paris
- **Gérard GARDELLA,** Ancien Secrétaire Général, Haut Comité Juridique de la Place financière de Paris

REPRÉSENTANTS DE L'AMF

- **Maxence DELORME,** Directeur des affaires juridiques
- **Clément SAUDO,** Directeur, Division Marchés financiers et services sur crypto-actifs, Direction des affaires juridiques
- **Olivier BROCHAND,** Senior Policy Officer, Division Innovation et Finance Digitale, Direction de la régulation et des affaires internationales
- **Juliette LE DROGOU,** Policy Officer, Division Innovation et Finance Digitale, Direction de la régulation et des affaires internationales

- **Charles MOUSSY,** Directeur, Division Innovation et Finance Digitale, Direction de la régulation et des affaires internationales
- **Marc WOLFENSTEIN,** Juriste, Division Marchés financiers et services sur crypto-actifs, Direction des affaires juridiques

REPRÉSENTANTS DE L'ACPR

- **Barbara SOUVERAIN-DEZ,** Directrice juridique
- **Beatrice PASSERA,** Cheffe de la Cellule de Conseil en Droit européen, Direction des Affaires juridiques
- **Reda ROSTANE,** Expert juridique affaires européennes, Direction des Affaires juridiques

REPRÉSENTANTS DE LA DIRECTION GÉNÉRALE DU TRÉSOR

- **Paul ABADIE,** Adjoint au Chef de Pôle Affaires internationales et enjeux technologiques du secteur financier
- **Axelle BLANCHARD,** Adjointe aux affaires européennes à la cheffe du pôle des affaires internationales, européennes et technologiques
- **Arthur FRAPPEREAU,** Adjoint au Chef de Pôle Affaires internationales et enjeux technologiques du secteur financier
- **Florent JOILAN,** Adjoint au chef de bureau lutte contre la criminalité financière
- **Romain LOISEAU,** Adjoint à la cheffe de bureau entreprises et intermédiaires d'assurance
- **Victor MAUJEAN,** Adjoint au chef du bureau FINENT3, chargé du droit des sociétés et gouvernance des entreprises
- **Victor MILLARD,** Adjoint à la cheffe du bureau des entreprises et intermédiaires d'assurance
- **Alexis MINE,** Adjoint aux affaires internationales à la cheffe du pôle des affaires internationales, européennes et technologiques

REPRÉSENTANTS DE LA BANQUE DE FRANCE

- **Christophe ARNAUD,** Directeur des services juridiques
- **Céline GARIN-PIAT-DESVIAL,** Responsable innovation et digitalisation, Direction des services juridiques

REPRÉSENTANTS DU MINISTÈRE DE LA JUSTICE

- **Julien GOLDSZLAGIER,** Chef du Bureau du Droit des sociétés et de l'audit, Direction des affaires civiles et du Sceau du Ministère de la Justice
- **Martin GUESDON,** Sous-directeur du droit économique, Direction des affaires civiles et du sceau

PARTICIPANTS AUX GROUPES DE TRAVAIL

- **Ahmed BALADI,** Avocat Associé, Gibson Dunn
- **François BARRIERE,** Professeur de Droit, Université Lumière Lyon 2, French Counsel, Skadden Arps Slate Meagher & Flom LLP
- **Célestine BARTHOUT,** Avocate, Norton Rose Fulbright
- **Sébastien BONFILS,** Directeur Juridique, Crédit Mutuel Arkéa
- **Michel CANNARSA,** Professeur des Universités Catholiques, Doyen de la Faculté de Droit de l'Université catholique de Lyon
- **Thomas CAVIGLIOLI,** Directeur Juridique Corporate, BPI France
- **Agnès CHATELLIER,** Responsable Juridique – Regulatory Digital, BNP Paribas
- **Asmaa CHEIKH,** Responsable de la coordination du pôle de Règlementation bancaire et financière, Direction des affaires juridiques, Groupe Société Générale
- **Thiebald CREMERS,** Directeur Juridique, AMAFI
- **Katia CZARNOTTA,** Juriste, Natixis
- **Thomas DAUTIEU,** Directeur de l'accompagnement juridique, CNIL
- **Marie-Mathilde DELDICQUE,** Juriste référent coordinateur IP & Communication, Ambassadeur IA, BPCE
- **Louis DE MENEVAL,** Legal Head of Digital, Commercial contracts & Litigation, AXA IM
- **Pierre-Yves DEVRIERE,** Head of Digital Transformation / Managing Director, Ardian
- **Muriel FAURE,** Présidente de la commission innovations technologiques de l'AFG
- **Philippe GOUTAY,** Avocat Associé, Jones Day
- **Clara HAINSDORF,** Avocate Associée, White and Case LLP
- **Emmanuel JOUFFIN,** Responsable Référentiel SSI et Veille Réglementaire, La Banque Postale

- **Lara KIRDAR,** Legal Counsel in Digital & AI, Qonto
- **Nathalie LANERET,** VP Government Affairs and Public Policy, Criteo
- **Yves Marie LECOCQ,** Juriste Digital & Data, BNP Paribas
- **Loïc LEGOUET,** Directeur juridique, Amundi
- **Caroline LOUVEAUX,** Chief Privacy and Data Responsibility Officer, Mastercard
- **Matthieu LUCCHESI,** Avocat Counsel, Gide Loyrette Nouel AARPI
- **Catherine MARTIN,** Responsable Juridique Digital, AXA France
- **Matthieu MAZARE,** Juriste, CNIL
- **Julien NIVOT,** Chargé de mission au sein du département Marché et Innovation Numérique, ESMA
- **Luke O'LEARY,** Head of Legal & Compliance, Capi Money
- **Jerôme PEDRIZZETTI,** Juriste, Crédit Agricole S.A
- **Sébastien PRAICHEUX,** Avocat Associé, Norton Rose Fulbright
- **Albane RICHARD,** Juriste, BNP Paribas
- **Dibril SAKO,** Direction Juridique, AXA Group
- **Marina TELLER,** Professeure de Droit, Université Nice Côte d'Azur