Association des avocats en droit boursier

Paris, 9 septembre 2026

Intelligence artificielle : les nouvelles frontières du risque

Discours de Denis Beau

Premier sous-gouverneur de la Banque de France

et Président désigné de l'ACPR

Mesdames, Messieurs,

Je suis heureux d'être parmi vous aujourd'hui pour échanger sur un sujet qui, en quelques années, s'est imposé au cœur des débats : **l'intelligence artificielle (IA).**

Dans le secteur financier, les perspectives d'utilisation de l'IA sont considérables. Une enquête conduite par l'ACPR en 2025 montrait que la quasi-totalité des banques et assureurs dispose désormais de cas d'usage en production. Une étude récente de l'AMF soulignait également la diversité des applications pour les acteurs de marché, qu'il s'agisse de la lutte contre la fraude et les abus de marché, de la détection d'opportunités d'investissement, ou encore de l'avènement de conseillers « augmentés ». En outre, les impacts de cette diffusion de l'IA ne font que commencer. Par exemple, si, jusqu'à récemment, l'IA assistait l'humain, elle peut désormais prendre des initiatives et agir. Les entreprises développent aujourd'hui des **agents** capables d'interagir avec leur environnement et d'accomplir de manière autonome des tâches de plus en plus complexes.

Mais comme souvent avec les grandes ruptures technologiques, les opportunités et les risques progressent de concert. Dès lors, la question de mon point de vue de superviseur est de savoir comment accompagner l'innovation sans renoncer aux exigences de sécurité, de transparence et de résilience qui sont au fondement de notre politique en matière de régulation du système financier.

Sans viser l'exhaustivité, je voudrais évoquer ce matin trois dimensions des risques posés par l'IA dans le secteur financier, en les confrontant aux réponses déjà engagées par les autorités et aux défis qui restent encore à relever. J'aborderai d'abord les risques pour la clientèle, autour de l'enjeu de la maîtrise des décisions assistées par l'IA (I) ; puis les risques cyber, qui se sont imposés dans l'actualité récente (II) ; et enfin les conséquences économiques et financières du développement rapide de l'IA.

*

I/ Le premier ensemble de risques concerne les citoyens et les consommateurs.

Car derrière les performances parfois impressionnantes des systèmes d'IA, il ne faut pas perdre de vue leur impact très concret sur les individus. Une décision fondée sur l'IA peut être erronée ; elle peut aussi reproduire ou amplifier certains biais, ou encore devenir difficile à expliquer lorsque les mécanismes qui la sous-tendent sont complexes. Dans le secteur financier, ces risques sont loin d'être anecdotiques : ils peuvent affecter l'accès au crédit et à l'assurance, et compromettre la capacité d'un client à comprendre les raisons d'une décision qui le concerne.

Face à ces enjeux, l'Union européenne s'est dotée d'un cadre ambitieux, avec le règlement sur l'IA. Ce texte repose sur un principe simple : plus un système d'IA présente des risques élevés pour les personnes, plus les obligations qui lui sont applicables sont exigeantes. Dans le secteur financier, les systèmes utilisés pour l'octroi de crédit et pour l'évaluation des risques et la tarification en assurance font partie des systèmes « à haut risque ». À ce titre, ils devront répondre à des exigences renforcées de gouvernance, de qualité des données, d'équité, de transparence et de contrôle humain.

L'ACPR sera chargée de la surveillance de ces systèmes à compter de décembre 2027. Nous nous préparons activement à cette nouvelle mission, qui s'inscrit dans le prolongement naturel de nos responsabilités en matière de protection de la clientèle et de supervision prudentielle. Alors que le cadre européen continue de se préciser, nous contribuons également à rendre certaines exigences plus concrètes. C'est notamment l'objectif des **travaux méthodologiques conduits par l'ACPR** ; celle-ci vient en particulier de publier un **document de réflexion sur l'équité algorithmique dans le secteur financier**, qui fait l'objet d'une consultation publique jusqu'à la fin septembre.

II/ J'en viens maintenant aux enjeux de cybersécurité et de souveraineté.

De plus en plus d'organisations utilisent l'IA pour renforcer leurs dispositifs de cybersécurité, mais, dans le même temps, celle-ci contribue à amplifier la menace cyber, et ce à deux niveaux.

D'une part, l'IA **renforce les capacités offensives des attaquants –** les systèmes les plus avancés peuvent déjà identifier des vulnérabilités dans le code informatique, faciliter la conception de logiciels malveillants et industrialiser les techniques d'ingénierie sociale. D'autre part, **les systèmes d'IA utilisés par les organisations deviennent eux-mêmes des cibles** – cibles finales, mais aussi cibles « intermédiaires » car, à mesure qu'ils s'intègrent aux processus critiques des institutions financières et se connectent à leurs données et leurs outils, ils ouvrent l'accès à de nombreuses ressources sensibles.

Face à ces risques, **nous ne partons heureusement pas d'une page blanche**. Le règlement DORA pose déjà un cadre robuste de gestion du risque informatique, fondé sur des principes suffisamment souples pour intégrer les risques liés aux nouveaux usages de l'IA. Le règlement européen sur l'IA complète ce dispositif, avec des exigences spécifiques de cybersécurité pour les systèmes d'IA à haut risque et pour les modèles à usage général les plus puissants.

Mais ce cadre n'est probablement pas suffisant pour faire face aux risques des modèles les plus avancés dont les concepteurs eux-mêmes ont du mal à maîtriser la dangerosité. Les modèles les plus avancés laissent en particulier entrevoir des capacités cyber d'un niveau

inédit. Ainsi, au cours de l'incident avec Hugging Face de cet été, des agents d'Open AI ont réussi à contourner leur isolement et à se coordonner, jusqu'à ce que près de 700 d'entre eux participent à une attaque de bout en bout – une illustration spectaculaire de la capacité de l'IA à maîtriser l'ensemble de la chaîne offensive. **Il est donc urgent de renforcer le cadre existant pour mieux maîtriser les dangers liés à l'IA de pointe**.

Dans ce contexte, l'ACPR plaide au niveau international pour la mise en place de garde-fous spécifiques : un déploiement progressif et contrôlé des modèles les plus puissants, un accès dans un premier temps réservé à des « partenaires de confiance » (par exemple au niveau du G7), ou encore le développement de capacités indépendantes d'évaluation, notamment en Europe – cette orientation est portée par la Commission européenne dans le Plan d'action en matière d'IA et de cybersécurité qu'elle a récemment présenté.

III/ Je terminerai en évoquant les conséquences économiques et financières de l'adoption rapide de l'IA.

Aux États-Unis, le développement de l'IA et des centres de données produit un effet macroéconomique tangible sur l'investissement et l'activité, et génère des pressions inflationnistes. En Europe, ces effets restent sans doute plus modestes, et sont aussi plus difficiles à isoler d'autres ajustements structurels en cours comme le changement climatique ou le vieillissement de la population. Ils ne justifient donc pas, à court terme, d'inflexion de la politique monétaire. À plus long terme, nous manquons encore de recul pour mesurer pleinement l'ampleur des transformations induites par l'IA, et notamment ses effets sur la productivité et l'emploi.

A ces incertitudes économiques s'ajoutent des enjeux de stabilité financière. L'IA pourrait d'abord entraîner des recompositions profondes entre entreprises et entre secteurs, avec des conséquences sur les défaillances d'entreprises de certains secteurs. D'autre part, et à plus court terme, l'ampleur des capitaux investis dans l'IA et les attentes qu'elle suscite alimentent le débat sur l'existence d'une possible « bulle », avec le risque qu'une révision brutale de ces anticipations entraîne une **correction désordonnée des marchés**.

L'enjeu pour l'Europe est donc double : accélérer, en maitrisant ces risques. Avec le plan de la Commission « *AI Continent* et le *Cloud and AI Development Act »*, elle entend précisément stimuler l'adoption de l'IA et mobiliser des investissements importants dans les infrastructures et les capacités de calcul. Cette ambition est essentielle pour notre compétitivité ; elle doit s'accompagner d'une surveillance attentive des risques de déséquilibres économiques et financiers susceptibles d'émerger à mesure que cette transformation s'accélère.

En définitive, l’IA porte la promesse d’une transformation profonde de nos sociétés, de nos entreprises et de notre économie. **Mais à la mesure de cette promesse doit répondre une ambition tout aussi forte dans la maîtrise des risques qu’elle fait émerger**. Car les bénéfices que nous tirerons de cette révolution technologique dépendront de notre capacité collective à en comprendre les effets, à en anticiper les conséquences et à en encadrer les usages. C'est à cette condition que nous pourrons construire une IA sûre, responsable et digne de confiance.