CENTRE DE DROIT
BANCAIRE ET FINANCIER

**Intelligence artificielle**

# Les attentes de la FINMA en matière de gouvernance et gestion des risques

Par Yannick Caballero Cuevas le 19 décembre 2024

Les banques et établissements financiers intègrent de plus en plus l'intelligence artificielle (IA) dans leurs services et processus internes (cf. not. Jotterand, cdbf.ch/1377). Cette utilisation peut notamment présenter des risques opérationnels, juridiques et réputationnels (cf. not. Levis, cdbf.ch/1380). Il en résulte également une dépendance croissante envers des fournisseurs tiers, en particulier, pour les modèles d'IA et les services *cloud*. À cela s'ajoute la difficulté d'attribuer des responsabilités claires en cas d'erreurs du système ou du modèle d'IA. L'utilisation de l'IA par les banques et établissements financiers pose un défi majeur en matière de surveillance. À cet effet, la FINMA a publié la communication sur la surveillance 08/2024 relative à la gouvernance et la gestion des risques en lien avec l'utilisation de l'IA, et où elle y décrit les enseignements tirés de sa surveillance.

Tout assujetti doit mener une réflexion sur les répercussions de l'utilisation de l'IA pour son profil de risque au regard du cadre règlementaire en vigueur, et adapter sa gouvernance, sa gestion des risques ainsi que son système de contrôle (cf. not. de Cannière, cdbf.ch/1376). Outre les questions de protection des données, la FINMA attire l'attention des assujettis sur la robustesse et l'exactitude des modèles d'IA, ainsi que sur la nécessité de garantir que les résultats sont corrects, explicables et exempts de biais. Elle axe ainsi sa surveillance sur sept thématiques : (i) la gouvernance, (ii) l'inventaire et la classification des risques, (iii) la qualité des données, (iv) les tests et la surveillance constante, (v) la documentation, (vi) l'explicabilité, et (vii) la vérification indépendante. Certaines thématiques se retrouvent d'ailleurs dans le règlement européen sur l'IA (RIA), en particulier les art. 9 à 15 RIA relatifs aux exigences des systèmes d'IA à haut risque.

Pour la FINMA, la gouvernance en matière d'IA est essentielle. Elle doit être établie à l'aune des risques qui ont été identifiés par les assujettis. Ces derniers doivent, d'une part, définir clairement les compétences et responsabilités en lien au développement, à la mise en œuvre, à la surveillance et à l'utilisation de l'IA, et, d'autre part, établir des prescriptions pour les tests des modèles, les contrôles auxiliaires du système, ainsi que pour les normes de documentation et les formations. Lorsque les assujettis acquièrent des solutions d'IA tierces, les assujettis doivent également déterminer quelles données et méthodes sont utilisées et l'existence d'une diligence raisonnable de la part du fournisseur tiers notamment. En cas d'externalisation, des tests et des contrôles doivent être mis en place. De plus, des clauses contractuelles doivent régir les compétences et questions de responsabilité. En outre, les assujettis s'assurent que les tiers disposent des compétences et de l'expérience nécessaires. Selon nous, la

gouvernance se pense de manière globale, puisqu'elle comprend la gestion des risques, les compétences internes et externes, l'attribution des responsabilités, ainsi que le cadre juridique et contractuel.

Afin d'inventorier et classifier les risques, les assujettis doivent déterminer si l'application envisagée entre dans leur définition de l'IA. Cette dernière doit être suffisamment large sans quoi l'inventaire des risques ne pourra pas être exhaustif. Définir ce qu'est un système ou un modèle d'IA constitue déjà un défi pour les assujettis, en l'absence de législation spécifique sur l'IA en droit suisse. À notre sens, le RIA peut servir de source d'inspiration (cf. Caballero Cuevas, cdbf.ch/1382). Ensuite, les assujettis sont amenés à classifier les risques selon leur importance, leur spécificité et la probabilité de la réalisation des risques identifiés. Ici, nous rappelons que le RIA adopte également cette approche fondée sur les risques (cf. Caballero Cuevas, cdbf.ch/1390). Les assujettis doivent par ailleurs définir des critères systématiques leur permettant d'identifier les applications d'IA importantes qui nécessitent une attention particulière.

La qualité des résultats des applications d'IA dépend, dans une large mesure, de la qualité des données. Selon les données utilisées lors des différentes phases, les résultats peuvent être erronés, incohérents, incomplets, non représentatifs, obsolètes ou biaisés. Les assujettis doivent dès lors définir dans leurs directives internes et instructions des prescriptions visant à garantir l'exhaustivité, la correction et l'intégrité des données et à assurer que celles-ci sont disponibles et accessibles. Cette attente nous semble toutefois élevée lorsque les assujettis utilisent des systèmes ou modèles d'IA de fournisseurs tiers. D'ailleurs, la FINMA reconnaît que les assujettis n'ont souvent aucune influence sur les données sous-jacentes, voire ne les connaissent pas. Afin de se conformer, les assujettis devraient, à notre sens, prévoir des clauses contractuelles afin de leur permettre de signaler au fournisseur les cas dans lesquels la qualité des données est compromise, et assurer une correction des données sous-jacente. À notre avis, cette difficulté n'excipe pas les assujettis de leur responsabilité de veiller à la qualité des données d'entrée, d'où l'importance de prévoir des directives internes sur la gouvernance des données et leur utilisation dans des systèmes d'IA.

Pour garantir le bon fonctionnement du système ou modèle d'IA, des tests réguliers ainsi qu'une surveillance constante sont essentiels. La FINMA évalue si les assujettis prévoient des contrôles réguliers sur l'exactitude, la robustesse et la stabilité du système ou du modèle d'IA. Ces tests aident à vérifier que l'application n'ait pas de biais. La FINMA s'attend à l'utilisation d'indicateurs de performance pour évaluer dans quelle mesure le système atteint les objectifs fixés. Les assujettis veillent également à ce que des changements dans les données d'entrée n'affectent pas le modèle d'IA sous-jacent à l'application d'IA. De plus, les assujettis doivent analyser les cas où des résultats ont été ignorés ou modifiés par les utilisateurs, puisque ces situations peuvent être des indices d'une faiblesse du système ou du modèle d'IA. Dès lors, ils doivent mettre en place une surveillance des applications d'IA tout au long de leur utilisation.

La FINMA met un accent sur l'importance de la documentation. Les assujettis doivent disposer d'une documentation détaillée et orientée vers le destinataire (par ex. conseiller, secrétariat, *compliance*, etc.). Pour les applications importantes, cette documentation doit notamment aborder le but de l'application, la sélection et la préparation des données, le choix du modèle, les mesures de performance, les hypothèses, les limitations, les tests et les contrôles ainsi que les solutions de repli.

L’explicabilité des résultats et leur compréhension par les collaborateurs des banques et établissements financiers sont cruciales pour évaluer de manière critique les systèmes et modèles d’IA. Ceci est d’autant plus vrai lorsque des résultats doivent être motivés envers des investisseurs, la clientèle, des collaborateurs (cf. Hirsch, cdbf.ch/1384), la surveillance ou la société d’audit. Or, la FINMA a constaté que les résultats n’étaient souvent pas compris ou expliqués et qu’ils ne pouvaient pas être évalués de manière critique, ce qui pose un problème pour garantir la robustesse et l’exactitude du système ou modèle d’IA.

En résumé, la communication sur la surveillance 08/2024 nous informe sur les attentes de la FINMA en matière d’IA. Cependant, de nombreuses questions demeurent, notamment sur la mise en œuvre concrète par les assujettis de ces attentes. La FINMA prévoit par ailleurs de les développer et de les communiquer de manière transparente. Cela dit, les assujettis souhaitant utiliser l’IA doivent faire preuve de proactivité dans l’analyse du cadre réglementaire, l’identification et la gestion des risques, ainsi que dans la formation de leurs collaborateurs. À ce sujet, les assujettis doivent s’intéresser aux initiatives qui sont prises à l’international. On pense, par exemple, à la déclaration de l’ESMA sur l’utilisation de l’IA dans les services d’investissement.

*Les thématiques abordées dans ce commentaire seront discutées lors du webinaire sur l’intelligence artificielle prévu le 21 janvier 2025, et approfondies plus largement dans le cadre du CAS Digital Finance Law.*

---