CENTRE DE DROIT
BANCAIRE ET FINANCIER

Groupe bancaire

Mise en œuvre d'une intelligence artificielle

Par Gaëlle de Cannière le 14 octobre 2024

ChatGPT et GenAI, ces nouveaux mots sont entrés dans notre quotidien depuis novembre 2022 et on ne les présente plus aujourd'hui. L'utilisation croissante de l'intelligence artificielle (IA) dans le secteur bancaire soulève des questions juridiques et règlementaires complexes. Comment naviguer dans le monde de l'IA lorsque l'on est actif dans le secteur financier en Suisse ?

Le point de départ est de connaître le cadre légal et règlementaire existant. À ce jour, peu de lois régissant spécifiquement l'IA sont en vigueur. Toutefois, plusieurs projets sont à des stades plus ou moins avancés du processus législatif. On peut notamment penser au règlement européen sur l'IA (cf. cdbf.ch/1359/), dont le texte est entré en vigueur le 1er août 2024 ou encore les travaux du Conseil de l'Europe pour aboutir à une Convention sur l'intelligence artificielle, ouverte à ratification. Il vaut la peine encore de mentionner les travaux des législateurs anglais et canadiens, pour édicter une loi sur l'IA.

En matière d'IA, la plupart des régulateurs financiers n'ont pas attendu 2022 pour faire part de leurs attentes. Par exemple, la CSSF (Luxembourg) a déjà mené une étude et formulé ses recommandations en décembre 2018 et relève notamment que le *top management* est le responsable ultime pour l'utilisation de l'IA et du *machine learning*. Il en va de même pour la BaFIN (Allemagne), qui publie en juin 2021 ses *guidelines* pour l'utilisation de l'IA. Plus récemment, c'est au tour de l'ESMA de donner des recommandations en lien avec l'utilisation de l'IA dans le respect de MiFID II. La FINMA quant à elle, a identifié quatre domaines clés en lien avec l'utilisation de l'IA, qui sont (1) la définition des rôles et responsabilités, (2) la précision et la fiabilité des résultats, (3) la transparence et l'explicabilité, et (4) la non-discrimination. Au niveau législatif, le DETEC devrait se positionner d'ici la fin de l'année sur l'opportunité de légiférer sur le sujet. Une veille règlementaire doit être mise en place pour identifier ces nouvelles exigences publiées presque quotidiennement.

Globalement, les régulateurs soulignent l'importance de (1) mettre en place une stratégie, (2) définir une gouvernance, (3) identifier les risques et les contrôles et (4) former les employés, qui sont quatre points clés à garder à l'esprit lorsqu'une IA est mise en œuvre dans une institution financière.

La stratégie

Le conseil d'administration a la compétence ultime pour approuver une stratégie. Ses membres

doivent donc être formés et sensibilisés afin d'être en mesure de définir une stratégie : autorise-t-on l'IA ? Le cas échéant, dans quel cadre et pour quelles finalités ? Quelles en sont les limites ? etc. Ces questions doivent être adressées et formalisées, puis approuvées par le conseil d'administration ou l'organe compétent local.

La gouvernance

Pour mettre en œuvre la stratégie, des rôles et des responsabilités doivent être attribués, en particulier pour le service informatique, le département de la sécurité informatique ou le département légal. Il ne faut pas oublier toutes les lignes de défense (L1, L2 et L3), qui a chacune son rôle à jouer. Quand la première ligne de défense doit mettre en œuvre le modèle d'IA conformément à la stratégie définie, la deuxième ligne de défense va devoir contrôler le respect des règles par la première ligne et finalement, la troisième ligne va devoir l'auditer. Il convient donc d'impliquer les différents acteurs compétents dès l'initiation d'un projet d'IA et d'obtenir les validations internes nécessaires (par exemple, celles du management, d'un comité de projet, des comités de métier, etc.). La pérennisation de ces rôles est clé pour assurer une gouvernance solide et elle peut notamment passer par la rédaction d'une politique interne en la matière.

Les risques et contrôles

L'utilisation de l'IA présente des risques spécifiques, tels que la protection des données personnelles, la propriété intellectuelle, la sécurité ou la gestion des tierces parties. Il est essentiel d'utiliser les processus existants pour identifier ces risques. Ainsi, chaque organisation pourra apprécier son appétit au risque et prendre les mesures de mitigation adaptées. En particulier, on peut penser aux risques liés au lieu de stockage ou de traitement des données personnelles, de la réutilisation des données pour nourrir l'IA ou encore des risques de fuite de données.

La formation

Les employés doivent être sensibilisés et formés. Une telle formation doit s'adapter en fonction du public cible, par exemple, de la sensibilisation générale à des formations spécifiques pour les experts. Le niveau de compétence pour la gestion d'une IA doit autant que possible être pérenne et acquis, à tout le moins partiellement, en interne.

La mise en œuvre d'une IA au sein d'un groupe bancaire soulève un certain nombre de défis, dont je ne citerai ici que trois d'entre eux. Premièrement, les experts, le management et les organes compétents doivent s'accorder sur une définition de l'IA. Quand bien même aujourd'hui une définition est donnée par l'OCDE et le règlement européen sur l'IA, les discussions autour de ce qui est vraiment « intelligent » ou non sont inévitables entre experts. Deuxièmement, la rapidité d'évolution et d'adoption de cette technologie par la société et par conséquent, des employés ou des clients doit être suivie. Il faut être réactif pour rester compétitif. Finalement, la transparence quant à la stratégie IA et l'optimisation des processus doit être pensée afin de sortir du mode « *task force* ». En d'autres termes, il faut penser à « industrialiser » la mise en œuvre d'une IA.