

L'intelligence artificielle dans les services financiers : déployer en conformité

Arnaud Houplain - Directeur Conformité spécialiste en Sécurité Financière,
OnePoint

- Quelles opportunités de croissance ?

Les directions de la conformité doivent relever le défi représenté par l'inflation législative, cela sur fond de recherche d'une plus grande efficacité opérationnelle dans les établissements bancaires. Une meilleure gestion des données, notamment par le recours à l'intelligence artificielle, constitue une piste d'amélioration.

Dans le domaine de la connaissance du client (KYC) par exemple, les inefficacités opérationnelles sont nombreuses. Dans la phase d'entrée en relation, on a affaire à des itérations (allers-retours) coûteuses en temps, mais aussi à des données hétérogènes provenant de plusieurs outils (de collecte, de stockage, etc.). L'usage des algorithmes permet la réconciliation d'une multitude de données disparates (dont des données externes). Des outils spécifiques peuvent, eux, procéder à l'analyse réputationnelle et à la collecte d'informations négatives.

L'apport des outils se traduit non seulement par des gains de temps significatifs, mais aussi par une amélioration de la fiabilité des dispositifs. Cela permet aussi de procéder à un KYC quasi permanent, à base d'alertes sur la foi desquelles on procède à des revues approfondies, mais encore d'aller au-delà des obligations réglementaires avec l'enrichissement de la relation commerciale, notamment dans la banque privée. Enfin, l'intelligence artificielle générative (robots conversationnels de type Chat GPT) facilite le travail du spécialiste de la conformité, spécialement dans la rédaction de rapports.

Dans le domaine de la surveillance transactionnelle (lutte contre le blanchiment de capitaux et détection des abus de marché), les dispositifs à base d'intelligence artificielle sont surtout mis à contribution dans le traitement des alertes, à partir de l'analyse de l'historique. Les outils à base de *machine learning*, éventuellement couplés avec des logiciels de visualisation de la donnée, accélèrent quant à eux le processus d'investigation renforcée. Par ailleurs, certains acteurs européens explorent la piste du croisement de signaux faibles répétés pouvant conduire à une suspicion de client à risque.

L'intelligence artificielle peut donc être synonyme d'efficacité renforcée et de meilleure maîtrise des risques, mais elle introduit de la complexité, ce qui nécessite une organisation ad hoc. Cette technique, par ailleurs, est encadrée dans certaines juridictions : il faut notamment veiller à l'explicabilité des modèles. Enfin, les algorithmes, le *machine learning* ou les robots conversationnels ne peuvent en aucun cas se substituer purement et simplement à l'humain.

Vincent Lefevre - Directeur Services Financiers, Sopra Steria Next

Bruno Maillot - Head of Practice AI for Business, Sopra Steria Next

- Quelles réglementations pour quels déploiements ?

Le dispositif législatif européen ne cesse de se renforcer en matière de données, depuis le Règlement général sur la protection des données (RGPD) en 2018, jusqu'au règlement sur l'intelligence artificielle récemment.

S'agissant du secteur financier, la résilience numérique est depuis quelques années l'une des préoccupations majeures de la Banque centrale européenne. Le règlement européen sur la résilience opérationnelle numérique (DORA), qui entrera en application en janvier 2025, impose aux acteurs une surveillance de leurs systèmes et la réalisation de tests de résistance. Quant aux orientations de l'Autorité bancaire européenne sur l'octroi et le suivi des prêts, entrées en vigueur en 2024, elles tracent une voie étroite vers l'utilisation de l'intelligence artificielle.

Le règlement européen sur l'intelligence artificielle (AI Act en anglais), dont l'application progressive a débuté en août 2024 et qui vise à protéger les droits fondamentaux des résidents et à éviter la fragmentation du marché, s'adresse à tous les secteurs (sauf la défense) et réglemente les usages et non les techniques, à l'exception de l'intelligence artificielle générative. Son champ d'application, extraterritorial, s'étend à tous les acteurs de la chaîne de valeur.

Le règlement établit une gradation des risques, qui vont des usages inacceptables comme le profilage social ou au travail, aux risques limités (les obligations sont ici plutôt limitées à la transparence), en passant par les hauts risques (60 % du texte).

Les hauts risques concernent les domaines comme la santé ou l'éducation, pas le secteur financier en tant que tel, mais peuvent aussi être déterminés en fonction de la nature de l'usage, par exemple ce qui a trait au crédit (l'usage de l'intelligence artificielle n'est pas formellement interdit) ou encore à la tarification des

assurances. Implicitement et en l'état actuel des choses, on peut en déduire que les autres aspects de la finance ne sont pas concernés.

L'intelligence artificielle générative est réglementée (droits d'auteur, choix des données, etc.) et impose des obligations renforcées pour des grands modèles, au nombre de deux pour l'instant (Gemini de Google et dernière version de Chat GPT).

La supervision s'effectue à deux niveaux : européen avec le Bureau européen de l'intelligence artificielle (stratégie, bilans, évolution des règles, etc.) et national avec des autorités ad hoc.

Brice Henry - Avocat à la Cour, A&O Shearman

- Perspectives croisées avec les Etats-Unis et le Royaume-Uni

Comme souvent, l'Union européenne a fait œuvre de pionnier, tandis qu'aux Etats-Unis et au Royaume-Uni, où la réglementation est naissante, on a tendance à privilégier une approche itérative et plutôt pro-business.

Aux Etats-Unis, il n'y a pas de loi fédérale à ce stade et la probabilité qu'il y en ait dans les quatre années à venir est très faible ; quelques Etats ont légiféré, notamment sur le sujet de la protection des données, tandis que le Président Biden a publié un décret demandant aux agences fédérales - dont certaines ont publié des lignes directrices - de prendre la mesure du phénomène.

Au Royaume-Uni, le nouveau gouvernement prévoit des mesures d'encadrement des grands acteurs de l'intelligence artificielle, mais il est plus que probable que se perpétue l'approche itérative.

L'Europe a une longueur d'avance avec le règlement sur l'intelligence artificielle. S'agissant des services financiers, l'une des interrogations concerne l'articulation entre ce texte horizontal et les règles sectorielles. Quels que soient les rythmes adoptés dans ces pays, on trouve des points d'attention communs : robustesse des dispositifs, protection des données, transparence.

S'agissant de la distinction entre l'approche par les acteurs et celle par les produits, on a aux Etats-Unis les deux versants, avec notamment des lois fédérales sur la protection des données visant les acteurs et des lois locales qui régissent par exemple la prise de décision automatisée. De même, l'Union européenne superpose les deux approches (en ce qui concerne les produits, en fonction l'importance des risques).

Si l'on se penche sur l'extraterritorialité, on pense aux Etats-Unis, dont on peut penser que si des règles fédérales émergent un jour, elles en seront fortement teintées. L'Europe, pour une fois, a intégré cette notion, ce qui introduira sans doute de la complexité pour les acteurs agissant dans plusieurs juridictions (quelles règles s'appliqueront, sachant qu'en matière financières, dominant généralement les plus exigeantes ?).

En ce qui concerne les prestataires externes, il y a une volonté commune de les encadrer - notamment parce que les autorités de marché se soucient des effets d'une trop grande concentration -, mais les approchent différent. En Europe, plusieurs textes traitent de cette question, notamment le règlement sur la résilience opérationnelle numérique (DORA). Aux Etats-Unis, le décret Biden envisage la création d'un cadre de gestion des risques et la notion de prestataire critique. Quant au Royaume-Uni, il s'est doté d'un régime des prestataires de services aux établissements financiers et le Trésor a annoncé qu'il pourrait obliger un prestataire jugé critique à se soumettre à une supervision directe par ses services (ce qui n'a pas encore été le cas).

Concernant l'arsenal répressif, le ministère de la Justice aux Etats-Unis (DoJ) considère que l'intelligence artificielle peut être considérée comme une circonstance aggravante en cas d'infraction, tandis que dans l'Union européenne, les autorités nationales compétentes peuvent infliger des sanctions significatives.

En matière de responsabilité, des déclarations officielles aux Etats-Unis et au Royaume-Uni laissent penser que les dommages ou préjudices au titre de l'utilisation de l'intelligence artificielle pourraient être réparés, mais cela devant des juridictions classiques. La spécificité de l'Europe en la matière réside dans la responsabilité extracontractuelle des acteurs et dans la mise en place de mécanismes de mise en cause des acteurs et d'indemnisation.

Julien Uri - Chargé de mission pôle Fintech/innovation, ACPR

- Comment l'ACPR se prépare-t-elle à la supervision du règlement sur l'intelligence artificielle ?

L'Autorité de contrôle prudentiel et de résolution (ACPR) étudie les implications du règlement européen la concernant, mais sans posséder toutes les réponses à ses interrogations à ce stade.

Le Comité européen de l'intelligence artificielle, qui sera composé d'un représentant par Etat membre, sera chargé de la coordination des autorités de contrôle nationales (durant les négociations, il a été obtenu que les Etats organisent le contrôle à leur main). Un sous-groupe dédié aux questions financières a été créé.

L'essentiel de la supervision s'effectuera au niveau national. En France, potentiellement mais probablement par l'ACPR.

Quel sera le périmètre de la supervision ? Il inclura les systèmes à haut risque en lien direct avec la fourniture de services financiers. Pour les systèmes à risque limité, la question se pose de savoir si l'autorité de contrôle sera la Commission nationale de l'informatique et des libertés ou l'ACPR, ce qui serait logique. S'agissant des acteurs, la Banque centrale européenne ayant établi que le contrôle de l'intelligence artificielle ne relevait pas de son mandat, l'ACPR sera compétente pour toutes les banques, y compris celles de taille significative. Des acteurs non financiers, en tant que prestataires de services, pourraient être soumis au contrôle de l'ACPR : ce point est l'objet de discussions.

Pour définir les missions des autorités de surveillance du marché (il en existe dans de nombreux secteurs), il faut se référer à la fois au règlement sur l'intelligence artificielle et à un règlement spécifique (règlement de 2020 sur la surveillance du marché et la conformité des produits). Ces textes établissent un cadre pour la collecte des informations, l'évaluation de premier niveau de l'intelligence artificielle, le contrôle approfondi ou encore l'instruction du dossier de sanction. Les autorités de surveillance disposent pour ce faire de pouvoirs génériques : possibilité de mener des inspections sur place et d'accéder aux codes sources par exemple.

Le règlement sur l'intelligence artificielle devra s'articuler avec les règles sectorielles. Comment traiter, par exemple, les droits fondamentaux, qui relèvent des règles sectorielles ? Dans le cas, par exemple, d'un modèle d'attribution de crédit qui serait discriminatoire, il semble que l'on se dirige vers un contrôle par le superviseur financier. Cependant, de nombreux points demeurent à clarifier dans ce domaine et l'ACPR s'attend à trouver des éclaircissements dans un rapport à venir du Haut Comité juridique de la place financière de Paris.

Pour les acteurs comme l'ACPR, on n'aura pas affaire à une révolution de la supervision et de la maîtrise des risques, dont les dispositifs (gouvernance, contrôle interne, etc.) sont bien connus, sachant par ailleurs que certaines exigences, par exemple en matière de cybersécurité, sont déjà couvertes par des textes existants. La surveillance s'effectuera ex-post et selon une approche par les risques. Par ailleurs, les cas

d'usages à haut risque prévus par le règlement sont peu nombreux, même si l'ACPR ne s'empêchera pas d'exercer sa vigilance de façon plus extensive.

Les acteurs, cependant, auront intérêt à ne pas sous-estimer ce nouveau texte, et notamment les exigences en matière d'explicabilité des outils à base d'intelligence artificielle.

Philippe Béraud - National Security Officer & Lead IA-responsable, Microsoft

- **Créer et utiliser des systèmes d'intelligence artificielle générative de façon responsable**

L'intelligence artificielle générative a trouvé des applications dans le grand public il n'y a que deux ans, mais il est important de se soucier dès à présent des risques qu'elle embarque afin d'en assurer le meilleur contrôle. Comme le *pharmakon* de la Grèce antique, on a affaire à des systèmes qui, selon le dosage, peuvent être des remèdes ou des poisons.

Microsoft doit sa prise de conscience des risques attachés à l'intelligence artificielle générative à une expérience douloureuse remontant à 2016 : un agent conversationnel a dû être immédiatement retiré du marché, car il tenait notamment des propos racistes. A ce moment a débuté un chemin vers des systèmes responsables, chemin qui ne s'achève jamais.

L'entreprise a publié dès 2028 des principes, dont elle s'est ensuite attachée à donner une traduction opérationnelle. Pour ce faire, il faut une organisation ad hoc, avec notamment un suivi au plus haut niveau de l'encadrement, des objectifs déclinés en étapes opérationnelles, des formations obligatoires. Par ailleurs, ces principes, propres à l'entreprise, doivent être mis en regard des exigences réglementaires.

L'organisation applique le principe de responsabilité, en procédant pour tous ses produits à des analyses d'impact prenant en compte non seulement les futurs utilisateurs, mais toutes les parties prenantes possibles.

Microsoft tient à ce que cette démarche, les travaux qu'elle implique et ses recherches, soient largement connus. Elle s'est ainsi engagée à publier un rapport annuel dont la première version date de 2024. Il y est notamment question des risques (liés à l'infrastructure, liés aux modèles eux-mêmes).

L'entreprise participe aux travaux de normalisation au niveau mondial et est favorable à la réglementation de l'intelligence artificielle.

Sara Meftah - Project Manager et chercheure, Square Management

- **Bien comprendre pour bien déployer : l'explicabilité des modèles d'IA, une nécessaire analyse**

Les modèles les plus connus sont aussi efficaces qu'assimilables à des boîtes noires dont on ne comprend pas le fonctionnement. L'explicabilité consiste à fournir des informations claires sur le pourquoi et le comment des décisions basées sur l'intelligence artificielle.

L'explicabilité est présente implicitement dans le règlement européen sur l'intelligence artificielle, et explicitement à deux reprises, associée aux notions de transparence et de supervision humaine.

Au-delà de l'aspect réglementaire, l'explicabilité permet d'améliorer les performances des modèles, d'atténuer certains risques (notamment le risque de réputation) et de détecter des biais.

Il s'agit cependant d'une notion difficile à encadrer : sa définition n'est pas consensuelle et peut par exemple varier selon les disciplines de recherche qui s'emparent de cette notion. Il y a aussi des divergences de vue concernant le niveau d'explicabilité requis.

L'explicabilité comporte deux volets : i) le fait d'apporter des informations sur la façon dont le modèle a été développé et sur les données utilisées ii) des éclaircissements sur les algorithmes, soit la réponse à la question « comment sont générées les prédictions ? », cela au niveau global, mais aussi pour chaque prédiction (pourquoi a-t-on refusé un crédit à telle personne ?).

Le champ de recherche sur l'explicabilité est confronté à un challenge technique, avec des modèles de plus en plus complexes et aux paramétrages de plus en plus fins.

Enfin, l'un des défis les plus importants en matière d'explicabilité consiste à répondre à cette double question : qu'est-ce qu'une bonne explication ? comment l'évaluer ? Square Management a publié un article (l'outil d'évaluation qui y est présenté est en libre-service) à l'occasion d'une conférence internationale. L'outil décrit se fonde sur trois critères : la fidélité de l'explication, sa stabilité (ou robustesse), son niveau de complexité.

Jacques Sudre - Directeur adjoint conformité groupe, La Banque postale

- Déploiement de l'intelligence artificielle au sein d'une unité de conformité

L'intelligence artificielle et la conformité font bon ménage, cela à un moment où ses effectifs, qui représentent en moyenne 2,5 % du total, ont probablement fait le plein. L'intelligence artificielle est capable de couvrir les principaux grands domaines de la conformité : la veille réglementaire, l'établissement de cartes des risques de non-conformité, le développement de procédures, la formation et la sensibilisation, le contrôle, le conseil et le reporting. Idem s'agissant des fonctions : sécurité financière, protection de la clientèle, lutte contre la corruption, fraude, protection des données, etc. Par ailleurs, dans une direction de la conformité, 60 % environ des salariés sont affectés à la détection des alertes (abus de marché, blanchiment de capitaux, fraude, etc.)

Toutes les composantes de l'intelligence artificielle trouvent des applications en conformité : par exemple le *deep learning* dans la gestion des risques, le *machine learning* dans la gestion des alertes, l'intelligence artificielle générative dans la production écrite.

Une petite musique commence cependant à se faire entendre selon laquelle l'intelligence artificielle ne tiendraient pas toutes ses promesses, voire serait un miroir aux alouettes, même si de nombreux cas d'application ont été testés avec succès. Ainsi se pose la question de savoir s'il faut persévérer, ou au contraire jeter l'éponge.

Il est probablement raisonnable de persévérer, mais dans ce cas, il faut avoir conscience des difficultés inhérentes à une utilisation extensive de l'intelligence artificielle : i) si les tests sont prometteurs, le passage à l'échelle est compliqué, notamment en raison de la masse de données de bonne qualité nécessaires et de la puissance de calcul que cela requiert ii) l'usage de l'intelligence artificielle, qui demande de la souplesse, s'insère dans des architectures informatiques rigides : l'organisation idéale reste à trouver iii) il existe un choc des cultures entre les spécialistes de la conformité, souvent des juristes à l'aise avec l'écrit et les revues de littérature, et les *data scientists*, qui manipulent des nombres et qu'il faut acclimater aux finesses des métiers de la banque iv) les directions se sont habituées à des équipes de conformité ayant atteint un bon niveau de maturité : le recours à l'intelligence artificielle est ainsi vue comme une prise de risque, même si cette technique porte des promesses d'économies de coûts.

L'usage de l'intelligence artificielle peut modifier les rapports avec les autorités de contrôle, qui, par ailleurs, auront des approches différentes selon les juridictions. En matière d'explicabilité, il faut que s'ouvre un débat avec elles. Les décisions prises par des machines seront aussi probablement un objet d'inquiétude pour les superviseurs (même si dans le domaine de l'oncologie par exemple, une étude a mis en évidence que l'intervention du médecin dégradait les résultats de la machine).

Si l'on part de l'hypothèse que l'intelligence artificielle s'imposera dans la conformité (c'est la conviction de Jacques Sudre), il faudrait que les responsables de la conformité envisagent dès maintenant ce que pourrait être leur unité à moyen terme, avec notamment ces questions : où utiliser l'intelligence artificielle en priorité ? quels risques sont prioritaires ?

En tout état de cause, l'intelligence artificielle constitue la première révolution dans le domaine de la conformité.