Intelligence artificielle : un *game changer* pour la supervision financière ?

Présentation de Vincent Guérin, Directeur risques et conformité, Onepoint

Chez Onepoint nous nous inscrivons auprès de nos clients sur le conseil en technologie au service des métiers, dans une logique de « bout en bout », c'est-à-dire en étant à la fois du côté des parcours clients et du régalien – sur les textes, les finalités, le prudentiel – et à la fois sur les mises en oeuvre dans les systèmes d'information. Vous l'aurez compris, vous êtes ici chez Onepoint dans nos espaces de vie. Je vais donc croiser la technologie, les usages, le droit ; je vais tenter d'hybrider, de faire du « bout-en-bout ».

Avec ce positionnement de bout en bout, hybride de la technologie et des visions régaliennes, nous accompagnons déjà nos clients sur les usages de l'IA et la mise en oeuvre au service des métiers, grâce à des capacités que nous développons depuis plus de 8 ans grâce à une équipe de plus de 200 collègues dont des PhD qui travaillent sur des projets IA, et des partenariats académiques et en R&D sur les sciences de la donnée, le « machine learning », le traitement du langage naturel et, maintenant, les IA génératives.

Sur le plan, règlementaire, il y a aujourd'hui un vrai « game changer » sur l'IA au sein de l'Union, c'est l'AI Act. A un moment où les acteurs économiques aux USA et en Chine investissement massivement dans l'IA, que la priorité serait de construire ou de consolider des avantages compétitifs, que la priorité serait d'investir et d'innover, il est remarquable de constater qu'au sein de l'Union Européenne nous ayons ce texte sur l'IA élaboré autour d'une perspective dont l'ambition forte est de protéger les droits fondamentaux des citoyens de l'Union avec une approche fondée sur les risques.

Après l'intervention de Jacques sur l'IA pour la conformité, je vous propose de compléter la perspective en croisant ces usages avec les principes posés par l'AI Act.

- Que voyons-nous, dans notre position de consultant, sur les attentes de nos clients en matière d'IA pour la conformité, l'anti-blanchiment et, plus largement les activités de contrôle et le régalien ?
- Ces attentes et les cas d'usages, comment se conjuguent-ils avec les principes posés par l'AI Act ?
- Et quelles sont les conséquences que nous pourrions voir se dessiner pour les fonctions conformité ?

1 - LES ATTENTES DES FONCTIONS CONFORMITE EN MATIERE D'USAGES DE L'IA

Aujourd'hui, rappelons-le, les usages de l'IA dans les entreprises se déploient sur deux dimensions :

- les usages sur l'optimisation des processus existants, internes (non visibles des clients) ou externes (visibles des clients) ;
- les usages sur la création de nouveaux services, internes ou externes.

Dans les établissements de crédit et dans les entreprises d'investissement, ce sont les usages de l'IA sur la relation client qui sont les plus visibles. Ces usages de première ligne de défense peuvent, évidemment, concerner les fonctions conformité dès lors, par exemple, qu'ils touchent à la commercialisation des instruments financiers et

aux services d'investissement.

Ce que font les fonctions conformité pour elles-mêmes n'a pas nécessairement vocation à être visible de l'extérieur : ce sont les usages de la technologie et de l'IA qui visent d'une part à l'optimisation des coûts et, d'autre part, à l'amélioration de la qualité et de la sécurité des processus internes. L'optimisation plus la qualité, cela amène à plus d'efficacité. Les cas d'usage en IA pour la conformité, nous les voyons se dessiner et parfois commencer à être mis en oeuvre sur ces axes : qualité et efficacité, dans des logiques industrielles.

- D'abord, l'optimisation, à cause des coûts. Le grand chiffre qui circule, un chiffre très largement questionnable d'ailleurs, c'est que la lutte anti-blanchiment représenterait, première et deuxième ligne de défense confondues, environ 3% des charges d'exploitation des établissements. Au-delà de la proportion, ce qu'il faudrait surtout apprécier c'est l'entièreté des coûts, y compris l'amortissement des investissements IT et le « run », y compris en y englobant plus largement l'ensemble des domaines de conformité et sur les trois ligne de défense : la lutte anti-blanchiment, les sanctions et embargos, la lutte contre le terrorisme certes, mais aussi la protection des investisseurs, l'intégrité de marché et la protection de l'information privilégiée, la conformité fiscale (avec FATCA, DAC et notamment DAC), l'anti-corruption, EMIR, etc. Sur tous ces domaines, les fonctions conformité travaillent en réalité à protéger la société, à protéger ce qui est extérieur à l'entreprise. Car les risques de non-conformité pèsent d'abord et avant tout sur la société, bien avant de peser sur les établissements qui participeraient insuffisamment au respect de ces lois et des règlementations qui visent à protéger les investisseurs, les marchés, etc. En cela, les risque de non-conformité sont très différent des risques financiers ou opérationnels. La plupart des établissements gèrent sérieusement les risques de non-conformité. Mais cela coûte très cher. Et cela se fait évidemment dans une équation budgétaire. Donc il faut être efficace, pas uniquement pour les actionnaires, mais aussi pour le bien commun : chaque euro dépensé se doit d'être dépensé le plus efficacement possible. Tout ce qui permet d'être plus optimisé a un intérêt, y compris pour le bien commun. En LCB-FT, les archétypes des besoins et des cas d'usage qui visent à l'optimisation portent aujourd'hui sur (i) le devoir de connaissance, avec la capacité à intégrer plus automatiquement notamment avec de l'IA générative de la donnée non structurée sur des chaines KYC et sanctions / embargos ; et sur (ii) le devoir de vigilance, avec des outils de ML pour pré-analyser plus rapidement les alertes et optimiser la charge de traitement des faux positifs.

- Ensuite, la qualité. Alors que beaucoup de besoins portent en France sur le traitement des faux positifs, dans d'autres pays l'enjeux est également de pouvoir détecter différemment : faire ressortir moins d'alertes, mais des alertes qui sont plus ciblées et qui se rapportent dans une plus large proportion à de vrais dossiers à risque. Cette différence entre pays semble tenir, du-moins c'est une hypothèse, à des différences dans la pratique des parquets et des tribunaux vis-à-vis des déclarants de bonne foi. Dans certaines juridictions, ces déclarants ont un risque accru d'être sanctionnés par l'ordre judiciaire lorsqu'ils ne mettent pas fin aux relations d'affaires, alors même qu'ils n'ont eu qu'une suspicion et non une certitude de blanchiment : d'où l'intérêt pour contenir le risque d'incrimination par les tribunaux (au-delà donc des sanctions pouvant être infligées par les autorités de contrôle nationales) de pouvoir détecter plus profondément et avec plus de certitude les dossiers suspects. Pour renforcer le monitoring et les détections, les sciences de la donnée et le « machine learning » apportent des capacités que les approches fondées sur des modèles linéaires ou déterministes ne permettent pas d'atteindre. Détecter mieux, cela intéresse aussi les autorités de contrôle.

2 – LA CONJUGAISON DES ATTENTES ET DES CAS D'USAGES CONFORMITE AVEC L'AI ACT

Il convient de dire, à titre liminaire, que si l'élaboration de l'AI Act a nécessité de longues discussions, le texte dans sa version définitive vient à peine d'être voté ; que sa mise en application sera progressive ; et, surtout, qu'il s'agit d'un règlement « principle based ». Je ne vais pas résumer l'AI Act mais me concentrer sur l'Annexe 3 qui recense les cas d'usage de l'IA qualifiés de cas d'usage à « haut risque ». L'AI Act n'interdit pas ces systèmes dits à « haut risque », mais il encadre leur production du côté des « provider » et leurs usages du côté des « *deployer* ». Pour qu'un système soit à « haut risque », il faut en particulier qu'il puisse avoir une influence chez le « *deployer* » en matière de prise de décision vis-à-vis d'une personne physique et du respect de ses droits fondamentaux. Les systèmes à « haut risque » sont à distinguer des systèmes à risque inacceptable qui, eux, sont interdits (p. ex. scoring social).

En ce qui concerne les services financiers, dans cette liste des systèmes à « haut risque », nous trouvons les usages biométriques et ceux pouvant empêcher d'accéder à un service financier.

- D'abord sont à « haut risque » tous les systèmes d'identification biométrique à distance, à l'exception toutefois notable des systèmes dont le seul objectif serait de confirmer l'identité d'une personne en particulier au titre des obligations sur l'anti-blanchiment. Les systèmes d'entrée en relation et le KYC à distance enrichis par de l'IA devraient donc demeurer hors Annexe III, à moins que ces systèmes de « KYC biométrique » puissent venir heurter, dans un détournement de leur usage premier, un droit fondamental des citoyens : ce qui reviendrait alors à reclasser ces systèmes comme étant à « haut risque » voir, même, comme étant inacceptables.

- Ensuite, sont à haut risque les systèmes qui peuvent contrevenir au droit d'accéder à un service. L'AI Act exclut expressément de cette catégorie les systèmes d'IA supportant les dispositifs AML et KYC. Donc, il sera toujours possible de refuser l'entrée en relation avec un client ou mettre fin à une relation d'affaire sur un fondement AML et avec des scénarii de détection fondés sur de l'IA. En l'espèce, le point de complexité que j'identifie sera plutôt d'articuler cette exclusion des modèles à « haut risque » et les droits fondamentaux avec l'article 55 du nouveau règlement AMLR.

Vous l'aurez remarqué, à part l'AML, l'annexe III ne porte aucune exclusion explicite des usages à « haut risque » sur les autres domaines de conformité dont il pourrait résulter des conséquences sur l'accès ou le niveau d'accès à un service. Les contrôle et décisions anti-corruption sur la clientèle et même sur les salariés ? Les tests d'adéquation sur la clientèle ? Le monitoring des transactions au titre de MAD2/MAR et de STOR ? L'AI Act demeure silencieux sur ces points, quand bien même sur certains cas d'espèce il y a une complexité juridique en matière d'articulation avec les droits fondamentaux, par exemple entre les manipulations de marché et la liberté d'expression.

Si j'élargis le propos au-delà des activités de la conformité, l'AI Act traite aussi du cas des risques prudentiels. Sont exclus des systèmes d'IA à « haut risque » les systèmes utilisés à fins de gestion des risques prudentiels pour calculer les charges en capital, par exemple sur les modèles IRB. En revanche, sont désignés comme systèmes à « haut risque » les « AI systems intended to be used to evaluate the creditworthiness of natural persons or establish their credit score » … même si en pratique, les politique de distribution crédit et les score d'octroi se doivent d'être articulés avec les modèle prudentiels. Dans le domaine de l'assurance vie et santé,

sont aussi à « haut risque » les systèmes d'IA conçus pour la tarification en lien avec l'évaluation des risques vie et santé des personnes physiques.

3 – AVEC L'IA ET L'AI ACT, QUELLES SONT LES CONSEQUENCES QUE NOUS POURRIONS VOIR SE DESSINER POUR LES FONCTIONS CONFORMITES ?

- Les fonctions conformité seront, comme d'autres fonctions, utilisatrices et souvent propriétaires de système d'IA. Il va falloir balayer les modèles, identifier si les modèles entrent ou non dans le champ d'application de l'AI Act, sachant que le champ définitoire de l'IA - calqué sur celui de l'OCDE - est très large. En effet, il y a deux types de techniques dans le viseur du texte : selon son art. 3(1), d'une part le Machine Learning et, d'autre part, les approches dites « logic and knowledge based » dès lors que le système « a un certain degré d'autonomie » et peut s'adapter après le déploiement. Quand le texte a commencé à être élaboré, l'IA générative n'était pas encore sur le marché, elle a été intégrée tardivement dans le règlement via une annexe sur les « General-Purpose AI Model ».

- Il faudra se demander si l'établissement est « provider » ou « deployer » du système d'IA, … ou les deux. Car quand un établissement développera pour ses usages propres des systèmes d'IA, l'établissement sera à la fois « provider » et « deployer ». Sur ce point, l'industrie financière a peut-être, pour une fois, un avantage compétitif car, côté « provider », ce qui est demandé sur le contrôle des modèles est assez proche de ce qui est déjà réalisé aujourd'hui sur les modèles interne et le prudentiel. L'industrie financière a les équipes et le savoir-faire, avec les équipes d'auditeur modèle et des fonctions risque compétentes et staffées. Les éditeurs n'ont pas nécessairement ces compétences et les industriels non plus. Ces exigences pourraient également ouvrir un nouveau domaine d'affaires pour les cabinets de conseil et les cabinets d'audit. Ces exigences vont renchérir les coûts.

- En interne, il va y avoir une question de gouvernance. Est-ce que la conformité à l'AI Act entrera dans le domaine de compétence des directions de la conformité ? Est-ce que les directions de la conformité devront avoir une charge de contrôle de 2d niveau sur l'AI Act ? Le règlement parle de « fonction de gestion des risques ». S'il s'agit bien en l'espèce d'un risque de non-conformité, les fonctions conformité n'ont pas nécessairement les compétences pour faire du contrôle de second niveau sur des sujets IT et modèle. Par analogie, l'exemple du positionnement des DPO sur le RGPD pourrait apporter des éléments de réponse.

Conclusion :

Je conclurais par deux commentaires sur l'AI Act.

- Le premier commentaire, directement inspiré de réflexions de collègues juristes, c'est que ce règlement est construit selon une approche « produit » fortement inspirée du droit de la consommation. Pour simplifier à l'extrême, le « provider » de système d'IA fournit une notice d'utilisation et de conformité au « deployer », qui doit bien lire la notice et se conforme aux usages prévus. C'est en particulier dans cette approche produit que le texte est nouveau pour les acteurs du secteur financier, jusqu'ici plutôt exposés à des réglementations orientés « services ».

- Le deuxième commentaire, c'est que ce règlement conjugue le respect des droits fondamentaux et la

gestion des risques. Ces droits fondamentaux figurent en haut de la hiérarchie des normes juridiques dans les traités de l'Union et dans les 54 articles Charte des droits fondamentaux de l'Union Européenne. La prise en compte des libertés fondamentales va probablement conduire à devoir développer de nouvelles compétences en interne sur une branche du droit qui n'est pas du tout le droit bancaire et financier. Même si l' « AI Office » élaborera des questionnaires pour aider à évaluer les atteintes possibles aux droits fondamentaux, ces examens de conformité seront nouveaux pour l'industrie financière. Et donc peut-être le règlement va-t-il ouvrir de nouveaux contentieux là où, aujourd'hui, il n'y en a pas encore : l'histoire le dira.