Décembre 2018

Intelligence artificielle : enjeux pour le secteur financier

Document de réflexion

AUTEURS
Olivier FLICHE, Su YANG - Pôle Fintech-Innovation, ACPR

ACPR
BANQUE DE FRANCE

SYNTHÈSE

Les travaux de l'ACPR sur la révolution numérique dans les secteurs de la banque et de l'assurance (mars 2018) ont mis en lumière le foisonnement des projets de mise en œuvre de techniques d'intelligence artificielle. Une *task force*, rassemblant professionnels du secteur financier (fédérations professionnelles, banques, assurances, Fintechs) et autorités publiques (AMF, CNIL, Tracfin, DGT) a donc été mise en place par l'ACPR début 2018 pour échanger sur les cas d'usages actuels et potentiels de l'intelligence artificielle dans le secteur, les opportunités et les risques associés, ainsi que les enjeux qu'ils représentent pour les autorités de contrôle. Le présent document de réflexion, partant de ces discussions ainsi que d'échanges à l'international ou avec d'autres acteurs français, a pour objectif de présenter un premier diagnostic de la situation et de soumettre à consultation les pistes de réflexion qui méritent d'être approfondies pour permettre le développement de ces nouvelles technologies dans un cadre sécurisé.

L'intelligence artificielle est une notion polysémique, qui tend à recouvrir des réalités différentes au fur et à mesure que les techniques algorithmiques évoluent : le rapport s'en est tenu à une définition relativement large de l'intelligence artificielle, incluant toutes les techniques d'apprentissage machine, ou « *machine learning* », mais excluant généralement les processus de robotisation automatisant certaines tâches cognitives répétitives.

Le premier constat établi par la *task force* est que, si les projets fondés sur l'intelligence artificielle sont à des niveaux d'avancement disparates et souvent encore peu développés dans les processus qu'une autorité de contrôle aurait tendance à juger les plus sensibles, toutes les conditions sont réunies pour un développement rapide et généralisé des techniques d'intelligence artificielle dans le secteur financier : prise de conscience croissante des possibilités d'exploitation de données, elles-mêmes de plus en plus nombreuses et diversifiées ; développement des offres technologiques disponibles (bibliothèques *open source*, nouveaux acteurs spécialisés, grands prestataires de services technologiques, notamment via le *cloud*…) ; multiplication des tests et des projets.

De fait, les usages – en production, en test ou envisagés – sont nombreux et couvrent la plus grande partie des activités des banques et des assurances : de la relation client (avec le déploiement déjà très avancé des *chatbots* mais également des possibilités dans le conseil ou l'explication individualisée) à la gestion de *back office* (la gestion des sinistres en assurance par exemple) en passant par la tarification personnalisée, sans oublier la gestion des risques et la conformité (détection des fraudes, lutte contre le blanchiment, cyber-sécurité, modélisation interne des risques pour le calcul des exigences de capital réglementaires).

Le développement de ces technologies ne va naturellement pas sans risques, ceux inhérents aux techniques utilisées et ceux liés à leur pouvoir « disruptif ». Se rattachent à la première catégorie les risques de biais des algorithmes, accrus par leur complexité et les effets induits par la combinaison des différentes méthodes statistiques et heuristiques sous-jacentes, ainsi que les cyber-risques. Relèvent de la seconde catégorie les risques liés à l'émergence possible d'un petit nombre d'acteurs incontournables pour l'usage de ces techniques et aux rapports de force – éventuellement aux effets systémiques - qu'un tel phénomène induirait.

Dans ce contexte, les superviseurs doivent faire face à des enjeux dont les énoncés et les termes temporels diffèrent fortement.

À court terme, il paraît important que le développement de l'intelligence artificielle dans les secteurs de la banque et de l'assurance s'accompagne d'une réflexion pratique sur les critères minimaux de gouvernance et de maîtrise de ces nouvelles technologies par les entreprises. Cette réflexion doit permettre de progresser notamment sur les techniques de preuve de la fiabilité des algorithmes utilisés (en vue de leur auditabilité tant interne qu'externe), sur leur « explicabilité » et sur les interactions entre humains (clients, conseillers, contrôleurs, etc.) et algorithmes intelligents. Elle doit aussi permettre de préciser également, de façon plus générale, ce que pourrait être une bonne « gouvernance des algorithmes » dans le secteur financier.

Parallèlement, les autorités de contrôle doivent rester attentives à l'impact à moyen et long terme des développements de l'intelligence artificielle sur la structure du marché afin d'anticiper les changements nécessaires dans l'exercice de leurs missions.

Enfin, le document de discussion aborde les besoins de montée en compétence et de coopération accrue des autorités de contrôle pour faire face à ces deux types d'enjeux.

Mots-clés : Intelligence Artificielle, Fintech, innovation, technologie, digitalisation

Codes JEL : G28, O38

SOMMAIRE

Introduction

L'usage de l'intelligence artificielle (IA) dans le secteur financier fait l'objet de jugements contrastés. D'une part, cet ensemble de nouvelles techniques apparaît très prometteur pour le futur des services financiers. D'autre part, ses applications concrètes se heurtent encore à de nombreux défis non résolus. Toutefois, les progrès réels et rapides en la matière pourraient bientôt trancher la question : le secteur semble bel et bien au seuil d'un ensemble d'innovations qui vont profondément le transformer.

L'importance de l'IA se révèle à mesure que les contours de la transformation numérique[1] se précisent. Les entreprises ont pris conscience de la valeur des données dont elles disposent. Il leur faut désormais des outils permettant de mieux les exploiter. L'émergence de l'intelligence artificielle est ainsi favorisée par un double mouvement : d'une part, celui de la numérisation de l'économie et de l'automatisation de processus existants ; d'autre part, une rupture dans l'offre de services qui se fonde sur l'exploitation de ce gisement de données qu'est le *Big data*.

Ce *document de réflexion* a été rédigé par le pôle Fintech-innovation de l'ACPR. Il s'inscrit dans la suite des réflexions menées par une *task force* composée d'acteurs de la place et d'autorités publiques et se fonde notamment sur la réponse des membres de la *task force* à trois questionnaires thématiques élaborés par le pôle. Il s'enrichit aussi des réflexions menées tant à l'échelle nationale par l'AMF, la Banque de France, la Commission Nationale de l'Informatique et des Libertés (CNIL), Tracfin et la Direction du Trésor, qu'à l'échelle européenne et internationale par le Financial Stability Board (FSB), l'Autorité Bancaire Européenne (ABE) ou encore l'Autorité Européenne des Assurances et des Pensions Professionnelles (l'AEAPP).

Le document caractérise en premier lieu l'état du développement de l'intelligence artificielle dans le secteur financier ainsi que les facteurs qui accélèrent ce développement. Il liste rapidement, dans un deuxième temps, les cas d'usages en production ou en projet dans les secteurs de la banque et de l'assurance afin d'identifier les risques et les opportunités de l'intelligence artificielle pour le marché. Ce double diagnostic permet, dans une troisième partie, d'identifier les enjeux pour les autorités de contrôle liés aux changements à l'œuvre à court, moyen ou long terme.

[1] La révolution numérique dans les banques et les assurances françaises, ACPR, mars 2018. Les études sectorielles (banque et assurance) sont disponibles sur le site de l'ACPR.

1. Le développement de l'intelligence artificielle dans le secteur financier

1.1. L'intelligence artificielle, une notion polysémique

1.1.1. Définir l'intelligence artificielle

La définition de l'intelligence artificielle (IA) a donné lieu à des formulations très différentes, allant de l'imitation des fonctions cognitives humaines à la faculté d'interagir avec l'environnement, en passant par la capacité d'une machine à atteindre des objectifs de manière autonome. L'IA a en effet pour objectif d'imiter les différentes fonctions cognitives comme la perception, la mémoire, le raisonnement, l'apprentissage ou reproduire des compétences telles que l'organisation, la description et le traitement de l'information. Toutefois, si l'on peut définir l'intelligence artificielle comme l'ensemble des technologies tendant à imiter le fonctionnement humain de manière autonome[2], il semble utile, pour l'objet de ce document, de restreindre le concept d'IA à des programmes qui disposent au minimum d'une capacité d'apprentissage autonome, autrement dit aux algorithmes de *machine learning*[3].

Aujourd'hui, les progrès techniques de l'IA concernent en effet principalement le domaine du ***machine learning***, c'est-à-dire l'ensemble des algorithmes qui permettent d'apprendre en identifiant des relations entre des données et de produire des modèles prédictifs de manière autonome. Le ***deep learning***, ou apprentissage profond, est un domaine particulier du *machine learning* dont les algorithmes sont particulièrement efficaces dans le traitement des données complexes et non structurées comme les images ou la voix.

Pour ne citer qu'un exemple, le **traitement automatique du langage naturel** (*natural language processing* – NLP), qui consiste à élaborer des algorithmes permettant de traiter des données linguistiques comme des phrases ou des textes, est un des domaines de recherche les plus dynamiques aujourd'hui. Il est utilisé par exemple pour une première lecture automatique des emails par des institutions bancaires.

D'autres processus de robotisation assimilés à l'IA sont appréhendés comme des opportunités d'amélioration de l'expérience client (proximité, fluidité, personnalisation, transparence accrues), d'augmentation de la productivité et du bien-être des employés. L'automatisation des tâches les plus répétitives permet de se consacrer à des tâches plus créatives ou à plus haute valeur ajoutée. Ils ne seront pas abordés en détail dans ce document.

1.1.2. Les facteurs de sa croissance

Les avancées majeures de l'intelligence artificielle, dans le secteur financier comme ailleurs, reposent sur trois facteurs principaux :

[2] Les outils qui automatisent des tâches manuelles ou cognitives répétitives comme le *Robotic Process Automation* (RPA) ou la saisie de texte ou la collecte de données via *Web Scrapping*, sont parfois considérés comme des applications rudimentaires de l'IA. Le terme d'IA renvoie toutefois aujourd'hui à des processus algorithmiques bien plus complexes.

[3] Pour un contexte plus général, cf. Annexe I.

- **La disponibilité des données et leur diversité**. L'un des facteurs d'émergence du *Big Data* est la disponibilité croissante des données, aussi bien structurées que non structurées : on assiste aujourd'hui à une croissance annuelle de 80% de la quantité de données non structurées (photos, vidéos, textes, signaux cardiaques…). Ainsi, 90% des données qui existent en 2016 ont été produites sur les deux années précédentes[4].

- **Des équipements informatiques de plus en plus performants**, tant au niveau du stockage, qu'à celui de la vitesse de calcul (suivant la loi de Moore[5]) et de l'infrastructure (*cloud computing*).

- **Les progrès en *machine learning*** (ou *apprentissage statistique*) et notamment en *deep learning*, ou plus généralement le développement d'outils permettant d'exploiter des données de plus en plus variées et volumineuses (*Big Data*).

Les acteurs financiers tirent ainsi parti des progrès réalisés en IA par d'autres secteurs, en premier lieu des grandes entreprises technologiques qui financent la majeure partie de la recherche et du développement en ce domaine. Des facteurs plus généraux favorisent en outre ces progrès :

- **Une attente des consommateurs**, habitués à des services digitalisés de plus en plus rapides et ergonomiques ;

- Une **confiance accrue** de ces derniers envers la technologie ;

- **La maturité des solutions technologiques et des méthodes associées**, notamment en matière de sécurité informatique et de méthode de travail agile.

De manière corollaire, la baisse des coûts de ces technologies favorise le développement des Fintechs, augmente les attentes des clients, incitant les banques et les assurances à investir à leur tour dans ces technologies.

1.2. Le développement de l'intelligence artificielle dans le secteur financier s'effectue dans un contexte de profonde mutation des infrastructures informatiques

1.2.1. L'enjeu des données a changé les priorités stratégiques des banques et des assurances

Après la crise de 2007-2011, les banques et les assurances ont fait porter leurs efforts sur le renforcement des départements de conformité et de gestion des risques, encouragées en cela par les évolutions réglementaires et le renforcement de la supervision financière. Cette tendance s'est stabilisée depuis plusieurs années pour laisser place à un autre enjeu : celui des données.

En effet, avec l'émergence des grands acteurs de l'internet, le rôle des données est devenu central dans de nombreux secteurs de l'économie. Il est en passe de le devenir aussi dans le secteur financier, avec l'apparition d'acteurs innovants qui bâtissent de nouveaux

[4] *Straight talk about big data*, Octobre 2016, *McKinsey*, Nicolaus Henke, Ari Libarikian et Bill Wiseman
[5] Loi de Moore (site Wikipédia)

modèles d'affaires sur la connaissance du client, la compréhension de son comportement et les évolutions de ses attentes.

L'essor de l'intelligence artificielle dans le secteur financier tient substantiellement à sa valeur ajoutée en termes d'exploitation des données ainsi qu'à la disponibilité croissante et à la qualité des données récoltées. Pour les acteurs financiers, l'exploitation de ces dernières représente une opportunité pour améliorer l'expérience client et la performance de la fonction de distribution, augmenter la productivité et la performance opérationnelle et améliorer la gestion des risques. Il y a ainsi un lien symbiotique entre l'intelligence artificielle et les données : à mesure que les données deviennent un enjeu crucial de compétitivité pour les acteurs financiers, la maîtrise de l'IA devient nécessaire.

1.2.2. Des projets à des degrés d'avancement inégaux

Le degré d'avancement des projets d'IA est marqué par une forte disparité. La mise en application de telles technologies semble plus avancée dans le secteur bancaire que dans le secteur assurantiel, tandis que l'algorithmique est développée dans les métiers de banque d'investissement et de gestion d'actif depuis les années 2000, précédant le développement des outils d'IA.

L'utilisation effective des algorithmes complexes, tels ceux exploitant le *deep learning*, ne se retrouve que dans certains domaines limités : traduction, *chatbots*… La majorité des applications de l'IA reposent donc sur des algorithmes d'apprentissage plus simples, conduisant une partie des acteurs à affirmer que l'IA est déjà employée dans la plupart des activités financières. En effet, elle est déjà largement déployée pour l'optimisation des processus opérationnels, que ce soit pour traiter les contenus écrits avec une plus grande efficience via l'utilisation des technologies de NLP, ou pour traiter des problèmes de fraude. Elle semble en revanche encore très peu employée dans des activités ayant un impact fort sur le client, comme le *credit scoring*, le conseil, les démarches de souscription client, les réponses automatiques… Autant d'activités qui ne devraient pas recourir à de l'IA avant 2020.

Enfin, l'hétérogénéité des usages de l'IA s'explique par les différences de stratégie à l'œuvre dans les établissements. La plupart des banques et des assurances utilisent à la fois des librairies *Open Source*[6] qu'elles exploitent en interne et des solutions fournies par des partenaires technologiques. Toutefois, les plus petites structures financières ont tendance à développer leurs propres outils (certains n'utilisent aucun prestataire technologique, même si rares sont les cas où tout est fait à partir d'une véritable feuille blanche : l'utilisation des librairies *Open Source* semble être un dénominateur commun).

Plus généralement, le développement d'outils d'IA s'effectue selon trois modalités, souvent complémentaires :

- **Via un développement en interne**, généralement via des librairies *Open Source* comme *ScikitLearn, Keras*, *Faiss* ou *Tensorflow*. Ces algorithmes permettent souvent d'améliorer progressivement l'interprétabilité et l' « explicabilité » du *machine learning*.

[6] Le vocable « *open source* », ou « code source ouvert », s'applique aux logiciels (et parfois plus généralement aux œuvres de l'esprit) dont la licence respecte des critères précisément établis par l'Open Source Initiative, c'est-à-dire les possibilités de libre redistribution, d'accès au code source et de création de travaux dérivés. Mis à la disposition du grand public, ce code source est généralement le résultat d'une collaboration entre programmeurs. Wikipédia

- **Via un grand prestataire technologique** proposant des solutions incorporant de l'IA, à l'instar de Microsoft et son *Pack Office* ou de Salesforce.com. Presque tous les acteurs financiers ont recours à ce type de services, en particulier pour le *Cloud* (voir *infra*).

- **Via les offres de services de nouveaux acteurs** incluant de l'IA. Encore une fois, nombreuses sont les banques et assurances concernées. À noter que cela comprend autant des Fintech fournissant des services intégrant l'IA (comme *Shift Technology*) que des prestataires technologiques généralistes (comme *Datarobot*).

1.2.3. La généralisation du recours au *Cloud*

La nécessité d'exploiter une quantité en croissance exponentielle de données fait émerger de nouveaux enjeux techniques. Le stockage interne, solution privilégiée il y a peu, rencontre d'importantes limites : le coût de maintien des serveurs, la variabilité du besoin de stockage, l'exposition croissante aux attaques… Recourir à des prestataires technologiques qui ont fait du *Cloud* et du *Big data* leur cœur de métier devient dès lors non seulement avantageux mais parfois aussi nécessaire, selon les acteurs financiers, pour optimiser le potentiel des données et, *in fine*, des outils d'intelligence artificielle.

La très grande majorité des établissements financiers ont recours aux services de *cloud computing* - et à ses prolongements incluant l'IA - sur une partie de leurs activités. Les principaux avantages qu'ils identifient sont les suivants :

- *La flexibilité*. L'entreprise peut moduler la capacité de stockage qu'elle loue selon ses besoins.

- *L'interopérabilité*. Les services étant proposées sur un serveur distant, l'accès à ces ressources peut s'opérer à partir de n'importe quel appareil permettant l'échange des données (smartphones, ordinateur etc...).

- *La mutualisation*. Le *Cloud* permet de répondre, en les mutualisant, aux variations de la demande des clients en calcul et bande passante. Il assure ainsi une optimisation des coûts d'utilisation.

- *La sûreté et la disponibilité*. Les fournisseurs de *Cloud* font souvent plusieurs copies des données et les stockent dans des lieux différents[7]. Ainsi, l'accès aux données est quasi permanent et la perte des données peu probable.

- *L'accès à des technologies de pointe*. Les fournisseurs de *Cloud* possèdent des technologies que les acteurs financiers ne peuvent pas acheter, notamment certains algorithmes d'IA embarqués directement sur les solutions de *cloud computing*…

Les acteurs financiers bénéficient ainsi de l'expertise des fournisseurs de *Cloud* tant sur le plan opérationnel que sur celui de la sécurité. Le *Cloud* accentue néanmoins certains cyber-risques dans la mesure où une grande partie des entreprises y recourt et que les données transitent à la fois par l'entreprise, le réseau et le fournisseur de services *Cloud* : autant de failles potentielles à surveiller[8].

[7] On notera que la pratique des centres de secours est également courante dans les systèmes informatiques « internes » des banquiers et des assureurs, dans le cadre de leur plan de continuité d'activité.

[8] Sur le volet du risque informatique, l'ACPR a également publié un papier de discussion en mars 2018 qui comporte des éléments relatifs à l'utilisation du *Cloud*.

Le leader du marché est sans conteste *Amazon Web Services* avec 40% des parts de marché dans le monde. Microsoft (avec *Microsoft Azure*), IBM (avec *Blue Cloud* ou *Bluemix*) ou encore Google (*Google Cloud Platform*) sont les principaux *challengers* et détiennent 23% du marché[9]. L'hégémonie américaine est à peine entamée par les acteurs asiatiques : à l'échelle du globe, seul *Alibaba Cloud* concurrence réellement les acteurs américains. La plupart de ces prestataires technologiques proposent, en plus des services de stockage, des services de surveillance des opérations, d'analyses des données, de gestion de domaine voire des applications/médias services… Autant de services susceptibles d'intégrer de l'intelligence artificielle et d'accentuer de ce fait l'enjeu de dépendance stratégique et technologique aux fournisseurs de *cloud*.

[9] *Microsoft, Google and IBM Public Cloud Surge is at Expense of Smaller Providers*, Février 2017, Synergy Group

2. L'intelligence artificielle dans le secteur financier, opportunités et risques

2.1. Usages et opportunités

2.1.1. Un enjeu de compétitivité et d'amélioration de l'offre

Sur le plan de la compétitivité, la maîtrise de l'intelligence artificielle apparaît comme une priorité stratégique[10] : elle permet d'accélérer les processus de décision, de rester au plus près de la frontière technologique et de ne pas laisser un oligopole technologique se constituer au profit de quelques acteurs (GAFAM, BATX…). D'après le rapport Villani[11], les acteurs financiers français ne sont pas aujourd'hui en retard en matière d'IA ; il semble toutefois primordial de rester parmi les pays en pointe sur ce sujet au vu des transformations à venir.

Pour les acteurs du secteur financier, les intérêts opérationnels de l'intelligence artificielle sont multiples :

- *D'un point de vue marketing*. L'analyse des données permet de **mieux comprendre les besoins** des clients et de comprendre les aspects des produits financiers à améliorer. Les produits financiers s'en trouvent plus adaptés.

- *D'un point de vue commercial*. Les technologies d'IA peuvent fournir d'excellents outils (assistant bancaire, simulation complexe, robot-advisor) pour faciliter **la compréhension**, par le client ou le conseiller, **des offres de produits et de services** financiers quelquefois perçus comme trop riches ou trop complexes.

- *D'un point de vue réglementaire*. L'IA est susceptible d'améliorer la qualité des processus de **détection du blanchiment**, enjeu crucial pour la sécurité et la stabilité du système financier.

- *D'un point de vue de gestion des risques*. L'IA permet une **meilleure gestion des risques** en fournissant une riche boîte à outils permettant de mieux maîtriser les risques en contribuant à l'aide à la prise de décision.

- *D'un point de vue financier*. Enfin, l'IA rend possible des **économies d'échelle** notables par l'automatisation de certaines tâches répétitives et la possibilité d'améliorer l'organisation des processus…

2.1.2. La relation client et l'amélioration du service rendu

L'intelligence artificielle peut aussi transformer les modalités de la relation client, en particulier dans un contexte de prise d'autonomie croissante des clients. Les applications de *Chatbot*, de *Voicebot* et d'analyseurs de mails sont les processus utilisant de l'intelligence artificielle les plus couramment relevés. Ces outils sont destinés aux clients mais aussi aux collaborateurs. Ils peuvent servir à qualifier le sentiment du client, mesurer le caractère urgent de la demande et dans certains cas analyser son contenu. Plus généralement, l'IA est utilisée pour traiter des questions répétitives ou réaliser un premier tri afin de faciliter le travail de

[10] Selon l'étude de l'ACPR sur la digitalisation du secteur financier en France, jusqu'à 30% des projets dans les établissements financiers sont conçus principalement autour de l'utilisation de l'IA. Plus de la moitié des projets en développement utilisent l'IA.

[11] VILLANI Cédric, *Donner un sens à l'intelligence artificielle*

l'analyste ou du conseiller. Ce genre d'applications pourrait évoluer pour aboutir à des outils de compréhension du client tout au long de sa relation avec l'établissement.

Les services de paiement

Dans le domaine du paiement, l'application principale semble être **l'analyse des données en temps réel** afin de détecter des transactions frauduleuses. Les projets actuels relevés sont entre le stade de développement et le stade d'industrialisation. D'autres acteurs du secteur ont évoqué des applications plus avancées en matière d'**évaluation du taux d'attrition** du nombre de clients lors de leur parcours d'achat.

En assurance

Dans la **prévention du risque** : l'installation d'objets connectés, par exemple dans les voitures ou les habitations, permet de contacter les clients en cas de risque et de prévenir des dommages. L'utilisation de l'IA permet de détecter à l'avance ou tout du moins suffisamment tôt ces risques en utilisant des paramètres liés à l'environnement de ces objets connectés.

L'optimisation de la recherche des personnes bénéficiaires en vue de répondre aux obligations relatives aux contrats en déshérence. Chez certains assureurs, ces applications seraient déjà en phase d'industrialisation.

L'automatisation d'une partie de la gestion de sinistres : c'est notamment le cas d'applications concernant l'analyse automatique des photos ou la recherche documentaire complète. En Chine, il est aujourd'hui possible d'envoyer des photos d'accidents simplement via l'application d'Alibaba et de recevoir un remboursement très rapidement grâce aux technologies de *deep learning* en reconnaissance d'images. Il est généralement admis dans le monde de l'assurance que ce genre de processus, comme tout ce qui a trait à l'estimation des dommages et traditionnellement effectuée par l'expert, se fera en partie via des outils d'intelligence artificielle d'ici 3 à 5 ans.

2.1.3. La tarification, la personnalisation des produits et la maîtrise des risques de souscription

L'octroi de crédit

L'utilisation de l'intelligence artificielle dans les activités de crédit semble devoir concerner principalement l'optimisation des **systèmes de *scoring***, à commencer par le crédit à la consommation où les clients sont plus sensibles à la fluidité et la vitesse d'exécution. En tirant profit des informations sur le client, le *scoring* permet de compléter l'approche traditionnelle, qui utilise des données financières limitées, par une approche exploitant le *Big data* faisant appel à des données non financières. L'exemple canonique est le score de crédit (ou *credit score*) qui détermine le montant et les conditions pour un emprunteur ; un problème de régression particulièrement adapté au *machine learning*. L'intérêt de cette approche réside bien dans l'utilisation de données externes (données de grands facturiers ou données en lien avec les comportements de leurs clients par exemple) aux données bancaires, traditionnellement utilisées pour le calcul du score de crédit. Cet apport permet à la fois de rendre plus précis le score mais également de le calculer lorsque l'historique bancaire de l'individu est faible ou inexistant, en utilisant des données non bancaires. Certains établissements affirment déjà utiliser des outils d'IA pour faire du *scoring*, tandis que d'autres indiquent avoir achevé la phase de développement mais travaillent à une plus grande lisibilité

et une meilleure « explicabilité » de la méthode pour s'assurer de sa conformité réglementaire.

La souscription en assurance

Si les données ont toujours été essentielles aux activités assurantielles, l'intelligence artificielle renforce encore leur valeur aux yeux des actuaires. Plusieurs solutions d'IA sont en effet susceptibles d'affiner les offres d'assurance**,** notamment en matière de **segmentation client**. L'IA serait ainsi employée pour mieux évaluer les risques des profils des clients et optimiser les systèmes de tarification. Certains indiquent avoir acheté des modules externes, d'autres s'appuient sur du développement interne.

Il existe par ailleurs des applications encore en phase de gestation :

- La qualification automatique de la conformité des clauses bénéficiaires en assurance vie, qui est utilisée grâce aux outils de reconnaissance d'entités nommées (*Named Entities Recognition*[12].)
- **Des scores liés à des moments de vie** : application envisagée par certains groupes qui cherchent à faire évoluer un score personnalisé de l'assuré tout au long de la durée de son contrat.
- Des services comme les **produits d'assurance paramétrique**, c'est le cas par exemple de la tarification en fonction de la conduite automobile et des conditions météorologiques, qui constituent les paramètres de ces contrats.

La prévention de la fraude et la lutte contre le blanchiment et le financement du terrorisme (LCB-FT)

Pour les secteurs de la banque et de l'assurance, **l'identification de fraudes documentaires et la lutte contre le blanchiment et le financement du terrorisme** sont des domaines d'usages récurrents de l'intelligence artificielle. Les techniques d'IA sont notamment employées pour la reconnaissance, l'analyse et la validation des documents fournis. Les algorithmes développés dans ce domaine sont généralement mures et déjà intégrés dans nombre de processus de contrôle.

Dans le domaine des paiements, la **détection des transactions frauduleuses** est également un champ d'application notable de l'analyse de données en temps réel permise par l'IA. La maîtrise de ces techniques pourrait déboucher, dans un deuxième temps, sur d'autres usages, aux objectifs plus commerciaux, liés à la meilleure compréhension des habitudes de consommation des clients. Toutefois, la valorisation des données de paiement, si elle n'échappe pas aux réflexions des acteurs établis, est encore balbutiante[13].

En assurance

[12] Page Wikipédia

[13] Certains entretiens, menés en dehors de la *task force*, ont montré toutefois que de nombreux projets de Fintechs gravitent autour de la valorisation des données relatives aux transactions.

- **La lutte contre la fraude à la souscription** : l'objectif est de résilier durant la période de garantie provisoire les contrats frauduleux, à l'aide d'algorithmes du type *Gradient Boosting*[14] et de données croisées (à la fois contractuelles et obtenues sur le Web).

- La **détection de la fraude dans la gestion de sinistres** : la plupart des organismes d'assurance semble recourir à des prestataires technologiques pour développer des solutions de lutte contre la fraude documentaire et les réseaux d'escroc. Ces applications semblent plutôt mures.

2.1.4. La gestion du cyber risque

Les acteurs financiers, notamment bancaires, utilisent de plus en plus l'intelligence artificielle pour se prémunir contre les cyberattaques. Les données de sécurité sont très difficilement compréhensibles pour un humain : il s'agit essentiellement de logs de connexions et d'activités générées automatiquement par l'infrastructure informatique. Les données sont donc semi-structurées (sous format texte) mais peuvent être traitées avec efficacité par des algorithmes intelligents. Ces outils-là présentent l'avantage de s'adapter en temps réel sans demander une mise à jour par le fabricant de logiciel. Les utilisations de l'IA contre les cyber-menaces peuvent être classées en trois catégories :

L'IA peut être utilisée de façon préventive avant la manifestation de l'attaque :

- Via la détection des vulnérabilités au moyen d'outils autonomes de scan.

- Via la correction de ces vulnérabilités, soit par un correctif temporaire soit par l'application d'une solution durable.

- Via l'accompagnement des développeurs dans l'écriture du code en les aidant, par l'analyse des motifs connus des attaques passées, à écrire un code sécurisé.

L'IA peut être employée pour détecter des cyber-attaques :

- Les algorithmes de détection d'anomalies sont souvent utilisés pour détecter les attaques sur internet (notamment sur les sites internet des acteurs financiers), des failles de sécurité ou de bugs ou encore des virus avant qu'ils ne se propagent au sein des réseaux informatiques internes aux entreprises.

- En particulier utilisée pour identifier les attaques visant les transactions de paiement, l'IA permet de compléter les techniques traditionnelles de détection par des outils plus adaptés aux attaques informatiques, notamment dans l'analyse des comportements.

L'IA peut également contribuer à la gestion et l'analyse des incidents :

- Certains outils d'IA sont expérimentés pour mieux identifier l'origine des cyber-attaques, ce qui permettrait notamment d'établir les profils des cybercriminels.

- Enfin, l'IA permet d'affiner les bases de données qui recensent les incidents connus et ainsi de contribuer au *rating* de la sécurité des entreprises[15].

[14] Page Wikipédia

[15] On peut ajouter que, d'une certaine manière, l'IA permet de combler les inégalités en matière de cyber-sécurité. En effet, beaucoup de PME font état de nombreuses difficultés pour atteindre le niveau de sécurité souhaité ; l'écart avec les grands acteurs du secteur, qui bénéficient souvent de l'expertise des grands acteurs technologiques, est substantiel. Les outils d'IA permettent de limiter les effectifs et les fonds affectés à la

2.1.5. Intelligence artificielle et conformité

L'intelligence artificielle pourrait améliorer la performance de la gestion des risques et de la conformité[16] en automatisant certains processus. Pour ce faire, la plupart des organismes financiers préfèrent innover en interne plutôt que faire appel à des solutions externalisées, notamment pour des questions de gouvernance, de données, de propriété intellectuelle et de responsabilité juridique.

Parmi les applications citées, on retrouve principalement les processus de *Know Your Customer* (KYC). Toutefois, l'analyse finale est toujours effectuée par un expert. Toujours en matière de lutte contre le blanchiment et le financement du terrorisme, des tests sont en cours pour assister les services conformité dans les déclarations de soupçons, notamment en détectant des signaux faibles dans les transactions enregistrées.

Dans le cadre de ses missions de contrôle, l'ACPR a pu observer que des méthodes d'apprentissage automatique sont employées dans les **modèles internes** pour pallier l'incapacité des méthodes actuarielles classiques à traiter de grandes quantités de données en grande dimension. Une attention particulière est portée sur le **cadre de validation** permettant de s'assurer de la qualité des résultats obtenus, tout en prévoyant des mécanismes ***d'add-on*** permettant de tenir compte de l'éventuelle erreur introduire si celle-ci se révélait significative.

Par ailleurs, des arbres décisionnels sont utilisées pour modéliser les **futures décisions de gestion**, prises en compte dans le calcul du ***best estimate vie***, prenant en compte de nombreux facteurs exogènes (environnement économique) ou endogènes (comptable : par exemple, richesses disponibles). L'attention se porte dans ce cas sur le ***backtesting*** *in sample* (au regard des décisions passées) des IA ainsi utilisées et sur le caractère vraisemblable et prudent du comportement induit dans des scénarios extrêmes (*backtesting out of sample*). Au regard du risque de sur-paramétrisation, l'autorité recommande de privilégier des algorithmes simples et robustes afin que ces derniers puissent être compris par l'AMSB[17] qui est responsable de les valider.

2.1.6. Services d'investissement, gestion d'actifs et activités liées aux marchés financiers

Un rapport du conseil de stabilité financière a montré les perspectives ouvertes par l'IA pour les marchés financiers, en améliorant l'analyse et la gestion des risques et en réduisant plus rapidement les écarts de prix[18]. Pour s'en tenir aux travaux de la *task force*, les principales applications de l'IA relevées sont les suivantes :

- **La détection d'anomalies dans les opérations de marché,** à la fois contre les fraudeurs extérieurs, les délits d'initiés et les erreurs du type « *fat fingers* ».

---

cyber-sécurité dans la mesure où les solutions fournies par le *cloud* intègrent très souvent des systèmes de sécurité performants, basés sur cette technologie.

[16] L'application des nouvelles technologies (dont l'IA) à ce domaine de la gestion des risques et de la conformité est communément désignée sous le vocable "Regtech".

[17] *administrative management or supervisory body*, introduite dans l'article 40 de la Solvabilité II, cette notion désigne l'organe d'administration de gestion ou de contrôle responsable ultime de l'implémentation de Solvabilité II au sein de l'organisme ou du groupe.

[18] *Artificial intelligence and machine learning in financial services*, FSB, novembre 2017

- **La surveillance des risques de marché :** des algorithmes de *machine learning* sont testés pour anticiper la réalisation des risques de marché (intrinsèques ou liés aux actions à venir de l'établissement), certaines de ces méthodes sont sur le point d'être mises en production.

- **La recommandation de stratégies d'investissement pour les clients :** cette application semble être déjà mise en production chez certains établissements. Les algorithmes proposent des solutions les moins coûteuses pour l'acheteur/vendeur et qui ont le moins d'impact sur le marché. Cela conduit à des stratégies autour d'un séquençage aléatoire des ordres d'achat/vente, une approche moderne de *Time Weighted Average Price*.

- **L'évaluation des profils de risque** pour la gestion des portefeuilles qui permet de mieux appréhender l'appétence des clients vis-à-vis de différents produits d'investissement et d'épargne. De même, certains assureurs ont mis en place des outils permettant de détecter l'appétence éventuelle de leurs assurés à certains produits d'assurances ou à certains supports d'investissement : certains de ces outils sont récemment entrés en production.

- **La gestion de portefeuille pour compte de tiers (gestion d'actifs, gestion sous mandat)** où l'IA ne semble pas en production selon les réponses ; des algorithmes d'IA sont toutefois testés par certains établissements pour faciliter cette tâche.

2.2. Risques

2.2.1. Le traitement des données : les risques liés à l'intelligence artificielle

La performance de l'intelligence artificielle est largement dépendante de la qualité des données et de l'absence de biais dans leur traitement. L'existence de biais dans les résultats des algorithmes d'intelligence artificielle peut être dommageable à la fois aux entreprises qui les utilisent et à leurs clients, en tant que consommateur ou citoyen, en raison des risques de discrimination ou de conseils inadéquats qu'ils recèlent.

La qualité des données est naturellement un prérequis à l'efficacité des algorithmes intelligents. Elle implique de vérifier la qualité des sources utilisées, la pertinence des données au regard des objectifs recherchés ainsi que leur complétude : il faut s'assurer en particulier que les données sont bien représentatives de la population ciblée afin qu'elles n'engendrent pas des phénomènes d'exclusion.

Les biais, quant à eux, peuvent exister à la fois dans les données collectées et dans les modalités de leur traitement.

- Ils peuvent être directement présents dans les variables utilisées, par exemple, avec des variables considérées comme discriminatoires telles que le genre ;

- Ils peuvent être implicites : ces biais sont plus difficiles à repérer car la discrimination résulte de l'interaction de plusieurs variables qui n'apparaissent en soi discriminatoires. Ils demandent une analyse des résultats par un expert métier et, pour ce qui est du risque de discrimination, une comparaison avec un résultat qui serait obtenu à partir de variables discriminatoires.

Les biais peuvent être renforcés par l'algorithme et aboutir à des traitements inéquitables. Par exemple, une information comme le département peut discriminer les habitants d'un département pauvre pour l'obtention d'un prêt, ce qui peut renforcer les inégalités existantes. De même, les modèles basés sur un historique de comportement sont moins performants pour les clients jeunes qui ont un historique réduit, auquel cas il faut trouver d'autres variables explicatives. Certains effets pourraient constituer un enjeu d'inclusion financière significatif.

Dans le fonctionnement même des algorithmes, d'autres effets indésirables peuvent voir le jour. C'est le cas de l'effet « *bulle de filtre* », c'est-à-dire le fait de proposer constamment les mêmes produits à des profils similaires, empêchant une entreprise de proposer des offres inhabituelles à un individu. C'est ce qui arrive souvent dans les algorithmes de suggestion de contenu, lorsque les profils type dominent l'offre en ne laissant pas de place aux nouveaux produits. On parle de *bulle de filtre* lorsque les suggestions envoyées à un utilisateur sont le résultat d'un processus de personnalisation dont il ne peut comprendre les ressorts.

L'identification et la suppression des biais reposent *in fine* sur la rigueur des *data scientists* qui ne sont pas toujours formés pour prendre en compte ces risques de biais. C'est la raison pour laquelle certains établissements financiers mettent en place des formations spécifiques de sensibilisation de leurs *data scientists* à ces aspects.

2.2.2. L'intelligence artificielle accroît les enjeux de cyber-sécurité

En matière de cyber-sécurité, le développement de l'intelligence artificielle n'ouvre pas de nouvelles failles, mais pourrait en accentuer des failles préexistantes. Le diagnostic peut être résumé comme suit.

L'IA augmente les points d'attaques possibles :

- L'utilisation de l'intelligence artificielle permet d'automatiser des tâches répétitives et augmente le volume d'interconnections informatiques. Cette automatisation décuple donc le nombre de failles potentielles exploitables par des cybercriminels.

- Le recours de plus en plus systématique au *Cloud* pour les besoins d'IA multiplie les points d'entrée possibles pour un cybercriminel, bien que les prestataires technologiques assurent un niveau de sécurité très élevé. Par exemple, le déploiement de solutions SaaS (*Software as a Service*) implique des interactions régulières entre l'acteur financier et le fournisseur de services, qui peuvent ainsi faire naître de nouvelles failles exploitables par les cybercriminels.

De nouvelles attaques sont conçues pour altérer le fonctionnement des algorithmes d'intelligence artificielle :

- L'une des attaques les plus fréquentes fait appel aux techniques de « *flooding* », qui cherchent à biaiser les résultats de l'algorithme d'IA par l'introduction de données falsifiées dans les modèles.

- D'autres attaques ciblées peuvent apparaître, comme les attaques *adversarials*, qui par une petite altération d'une image induisent un algorithme de reconnaissance de forme en erreur[19].

L'IA pourrait surtout augmenter la dangerosité des cybercriminels :

- L'utilisation de l'IA pourrait rendre plus accessible et moins chère la cybercriminalité : l'utilisation de l'IA pour automatiser les tâches nécessaires à une cyberattaque modifiera le compromis existant entre l'ampleur et l'efficacité des attaques.

- L'usage du *machine learning* pourrait permettre de « craquer » des mots de passe à partir des archives de mots de passe précédents.

- Enfin, les cyber-attaques pourraient être personnalisées, ce qui les rendraient plus efficaces (*phishing* personnalisé, utilisation de *chatbots* ou de technologies d'imitation de voix pour extraire des informations confidentielles).

2.2.3. Le risque de dépendance des acteurs et le changement des rapports de force dans le marché

La maîtrise des techniques de l'intelligence artificielle par des grandes sociétés informatiques majoritairement non-européennes (fournisseurs de solutions informatiques ou de services, comme les « *cloud services* », sociétés de conseil…) pourrait entraîner une concentration excessive du marché entre les mains de quelques acteurs, avec les inconvénients potentiels suivants :

- Des prix artificiellement élevés ;

- Un accès limité à certains services qui utiliseraient de l'IA ;

- Des relations commerciales déséquilibrées ;

[19] *Shotgun shell: Google's AI thinks this turtle is a rifle*, The Guardian

- Des questions de souveraineté liées au contrôle des plateformes, des technologies et des données (exemple : « *cloud service providers* », fournisseurs de solutions d'IA…) ;

- Une maîtrise moyenne par les utilisateurs finaux et une opacité accrue des algorithmes (« boite noire ») ;

- Des difficultés d'accès et d'audit nécessaires dans le contrôle des activités financières.

Le risque le plus important est sans doute que la sophistication croissante des algorithmes d'IA ne rende impossible leur reproduction, voire leur simple explication, par d'autres acteurs. Aussi, un retard dans ce domaine pourrait inciter les établissements financiers français à adopter des solutions étrangères et à alimenter un cercle vicieux laissant le monopole du développement de l'IA à des firmes non-européennes.

2.2.4. Des enjeux de stabilité financière et de souveraineté

Sur la stabilité financière

La question de la stabilité financière a été posée dès le début du XXIème siècle avec l'arrivée des algorithmes de *trading* haute fréquence. Elle connaît un renouveau avec l'arrivée des algorithmes de type *machine learning* puisqu'il est difficile de prévoir le comportement futur de ces algorithmes. En particulier, trois facteurs de risque pourraient être accentués par l'utilisation de l'IA :

- **Le trading directionnel technologique**, à l'origine de « comportements moutonniers ». En codant les algorithmes avec des variables similaires, les programmes de trading à haute fréquence tendent à converger vers la même stratégie. Le risque qui en découle est d'accentuer ainsi la pro-cyclicité et la volatilité du marché via des achats et ventes simultanés de grandes quantités.

- **La vulnérabilité du marché face aux attaques**, en partie due aux comportements moutonniers. Il est en effet plus aisé pour un cybercriminel d'influencer des agents qui agissent de la même manière plutôt que des agents autonomes, ayant des comportements bien distincts.

- **L'entraînement sur des données historiques** : beaucoup d'algorithmes ont été entraînés dans des situations normales, et non en temps de crise. Il y a donc un risque que le *machine learning* accentue les crises du marché financier en l'absence d'entraînement en période de crise.

Ces risques ne sont pas les seuls. Une mauvaise utilisation de l'IA peut également conduire à des risques systémiques dans d'autres activités financières. Par exemple, elle peut conduire à des risques de crédit accrus si l'algorithme les évalue mal, et ainsi fragiliser le marché obligataire ou des acteurs bancaires.

Sur la souveraineté

Les inégalités en matière d'expertise technologique ont déjà été évoquées : elles pourraient engendrer de fortes asymétries entre pays. Le risque de fuite de données vers des prestataires américains en est un exemple. Le gouvernement américain a promulgué le 23 mars 2018 le *Cloud Act*, qui lui octroie la possibilité d'accéder aux données hébergées sur les serveurs des fournisseurs américains de *Cloud*. Cette législation semble entrer en directe confrontation avec les principes du RGPD, notamment l'article 48 sur les « Transferts ou divulgations non autorisés par le droit de l'Union » qui dispose que « *Toute décision d'une juridiction ou d'une autorité administrative d'un pays tiers exigeant d'un responsable du*

traitement ou d'un sous-traitant qu'il transfère ou divulgue des données à caractère personnel ne peut être reconnue ou rendue exécutoire de quelque manière que ce soit qu'à la condition qu'elle soit fondée sur un accord international […] »[20].

[20] Texte du RGPD disponible sur le site de la CNIL .

3. Le développement de l'intelligence artificielle : quels enjeux pour les superviseurs ?

3.1. La gouvernance et « l'explicabilité » des algorithmes

L'intelligence artificielle a pour objet d'automatiser un certain nombre d'actions ou de décisions prises jusqu'à présent par des humains ou d'individualiser des décisions auparavant standardisées. En modifiant les conditions d'élaboration des décisions, les développements de l'intelligence artificielle sont également susceptibles de remettre en cause les méthodes traditionnelles d'encadrement a priori, de traçabilité et de contrôle interne et externe de ces décisions.

Selon les cas d'usage de l'intelligence artificielle, les enjeux réglementaires diffèrent sensiblement.

Ainsi, l'utilisation d'un « *chatbot* » pour prendre en charge les réclamations des clients doit, de façon assez simple et dans un but de protection de la clientèle, se conformer aux règles générales de gestion des réclamations qui sont largement similaires dans les différents secteurs financiers[21].

Dans un tout autre domaine, l'utilisation de l'intelligence artificielle pour l'allocation d'actifs ou la modélisation interne des exigences de capital peut réinterroger les règles de gouvernance et de gestion des risques « prudentiels » de l'entreprise concernée : dans le deuxième cas, en particulier, un changement dynamique de certains paramètres du modèle par un algorithme auto-apprenant, comme par exemple les paramètres de probabilité de défaut pour les modèles de risque de crédit, serait susceptible de remettre en cause les politiques de changement de modèles et les règles de validation de ces modèles par les superviseurs.

Enfin, les exemples, déjà mentionnés dans le rapport, des possibilités ouvertes par l'intelligence artificielle en matière de sélection et de tarification des risques – tant en banque qu'en assurance – sont tout particulièrement intéressants car ils doivent prendre en compte les principes de plusieurs réglementations :

- La nécessité de maîtriser les risques acceptés par l'entreprise ;
- Le devoir de loyauté vis-à-vis des clients – voire, selon les réglementations, l'obligation de prendre en compte leurs intérêts ;
- Les obligations générales liées au traitement automatisé des données personnelles et de transparence sur les décisions prises par ces traitements ;
- Éventuellement, l'intégration des objectifs de lutte contre le blanchiment et le financement du terrorisme.

Dans ce contexte, trois enjeux principaux peuvent être identifiés.

[21] L'ACPR a publié en 2016 des recommandations en la matière sous la forme d'une annexe sur les interfaces numériques à la Recommandation sur le devoir de conseil en assurance vie qui date de 2013.

3.1.1. Définir une gouvernance appropriée des algorithmes

Les principes de gouvernance et de contrôle interne posés par les différentes réglementations sectorielles ont naturellement vocation à s'appliquer et, de façon générale, les objectifs qu'ils poursuivent (maîtrise des risques, protection des clients, LCB-FT) n'ont pas de raison d'être remis en cause.

Toutefois, leur prise en compte effective lors de la conception des algorithmes intelligents doit appeler une attention particulière de la part des organismes contrôlés et des superviseurs.

En matière de protection des données personnelles, le RGPD a explicité le principe du « *privacy by design* » - qui met bien en lumière la nécessité d'intégrer, dès les premières étapes de la conception de l'outil de traitement des données, les finalités de la réglementation[22].

Dans le secteur financier, il est clair que le principe du « *privacy by design* » ne suffit pas à traiter tous les enjeux réglementaires. En revanche, cette même idée peut sans doute être utilement transposée pour s'appliquer aux finalités des autres réglementations applicables, le point d'attention étant de recenser précisément et de prendre en compte chacun des objectifs fixés par la politique interne en conformité avec ces réglementations (prudentiel, protection de la clientèle, LCB-FT).

Par ailleurs, dans certains cas, l'utilisation de l'intelligence artificielle peut remettre en cause, en pratique, des conventions communément admises : on a évoqué le cas des politiques de changements de modèle ; on peut aussi mentionner, en matière de protection de la clientèle, la ligne de partage théorique entre « gouvernance des produits » et devoir de conseil ou d'explication personnalisée.

Ces considérations rejoignent le besoin, exprimé par certains acteurs, lors des travaux de la *task force* d'un code de bonne conduite voire d'éthique adapté au secteur de la banque et de l'assurance et exposant des exemples pratiques. L'objection principale, soulevée par d'autres participants, est que l'édiction d'un tel code serait prématurée, en raison de la faible maturité collective en matière d'utilisation de l'intelligence artificielle.

De fait, il peut y avoir un risque à édicter trop tôt des normes qui fassent obstacle au développement de certains usages de l'intelligence artificielle dans le secteur financier. Inversement, il apparaît toutefois important que le développement des usages de l'intelligence artificielle s'accompagne d'une réflexion pratique sur les formes adaptées de leur gouvernance, au regard d'objectifs réglementaires « technologiquement neutres ».

3.1.2. S'assurer de la fiabilité des algorithmes et de l'atteinte de leurs objectifs

Une fois assurées la compatibilité et la conformité des objectifs des algorithmes d'intelligence artificielle aux principes de gouvernance posés par les réglementations, la deuxième question qui se pose, tant aux entreprises qu'à leur superviseur, est celle de leur fiabilité.

[22] La perspective de l'entrée en vigueur en mai 2018 du RGPD a donné lieu à d'importants travaux de la part des acteurs financiers, dont certains travaux de place. On citera par exemple la norme de pratique NPA 5 publiée en novembre 2017 par l'Institut des actuaires.

Cette fiabilité passe en premier lieu par la qualité des données. Cette exigence, déjà prévue dans nombre de réglementations sectorielles[23], revêt une signification particulière dans le cas de l'intelligence artificielle, dont l'usage repose sur l'exploitation d'une volumétrie importante de données issues de sources très diverses. Quelques précautions semblent d'usage courant en la matière : minimisation du recours à des données personnelles externes publiques (quasiment pas de recours, actuellement, aux données des réseaux sociaux chez les acteurs interrogés), utilisation de données externes de sources jugées fiables (par exemple INSEE), vérification régulière de la qualité des données sur des échantillons, mise à jour régulière des données personnelles auprès des clients eux-mêmes.

La fiabilité des algorithmes passe ensuite par la vérification que l'usage des données est approprié au regard des objectifs fixés et qu'il n'induit pas de biais involontaires. Plusieurs méthodes sont envisagées par les acteurs financiers à cet égard :

- Recours à des experts pour valider la pertinence des variables utilisées, éliminer celles qui sont inutiles[24] ou sources de biais potentiels ;
- Emploi d'un processus parallèle plus sûr et plus traditionnel sur une partie des données tests ;
- Utilisation d'un jeu de données étalon sur les algorithmes pour contrôler régulièrement à la fois la pertinence et l'aspect non-discriminatoire des algorithmes ;
- Développement d'outils qui évalueraient la dérive conceptuelle pour maîtriser ce risque spécifique de l'apprentissage automatique.

Enfin, il convient de réfléchir aux conditions de contrôle de ces algorithmes – par le contrôle interne ou par le superviseur. Deux aspects complémentaires de la question peuvent être distingués.

L' « explicabilité » de l'algorithme

Celle-ci est nécessaire afin de raccorder les sous-jacents techniques et statistiques aux objectifs fixés ex-ante dans le cadre de la politique interne en matière d'algorithmes d'IA.

On notera, en outre, le cas particulier de certaines règles de protection de la clientèle, où l'obligation d'explicabilité dérive également des règles encadrant le service rendu. Il en est ainsi du conseil ou de la recommandation personnalisée en assurance ou de l'évaluation de la solvabilité de l'emprunteur en matière de crédit : le professionnel est tenu de démontrer la pertinence de la diligence effectuée ou du service rendu au regard de l'information fournie par le client sur ses besoins et sa situation financière. Selon les cas, tout ou partie de cette démonstration doit être exposée au client afin de l'éclairer sur la proposition qui lui est faite : c'est la reformulation des exigences et besoins du client et la motivation du conseil fourni.

Le professionnel doit donc se mettre en mesure d'expliquer :

- De façon générale, quels sont les mécanismes et les critères suivis par l'algorithme au cours de son processus d'analyse ;

[23] On peut citer par exemple, dans la règlementation prudentielle bancaire, les exigences de complétude et de qualité des données sur les risques et de la notification des risques de la norme BCBS 239.

[24] En matière de données personnelles, deux facteurs peuvent limiter l'utilisation d'un trop grand nombre de données : les obligations issues du RGPD mais également la nécessité de ne pas freiner excessivement le parcours client.

- Pour une action donnée (une décision prise, un conseil fourni) les critères objectifs et les éléments discriminants qui ont poussé l'algorithme, dans le cas étudié, à effectuer une action ou proposer une solution plutôt qu'une autre.

Les tests des résultats obtenus

En complément des travaux d'explication des algorithmes, un certain nombre de tests (sur de jeux de données indépendants de ceux utilisés pour l'apprentissage des algorithmes) pourraient être envisagés pour évaluer la qualité des résultats. La méthodologie de tels tests restent toutefois à définir : en particulier pour les algorithmes apprenants (et selon les enjeux réglementaires), la question se pose de l'historisation des versions – afin d'être en capacité de juger de la performance réelle d'un algorithme à une date donnée.

Algorithmes et intervention humaine

Par précaution, certain acteurs envisagent le maintien d'une intervention humaine pour vérifier la cohérence des résultats de l'algorithme, en particulier dans les domaines, sensibles règlementairement et commercialement, des informations et conseils délivrés aux clients ou de la LCB-FT. Cette précaution pratique, très compréhensible à un moment où les techniques de l'intelligence artificielle en sont à leurs débuts, ne doit toutefois pas amener à sous-estimer l'importance des travaux à mener pour améliorer l' « explicabilité » des algorithmes et les méthodologies de tests de leurs résultats. Il convient en particulier de rappeler les considérations suivantes :

- Un intervenant humain engage davantage sa responsabilité à contredire le résultat d'un algorithme qu'à le valider[25] ;

- S'il est susceptible de repérer les erreurs manifestes d'appréciation de l'algorithme (ce qui peut aider à l'apprentissage), il est moins armé pour repérer d'autres formes de biais, moins visibles mais dont le caractère systématique peut poser problème ;

- Sa propre perception de la situation peut l'amener à trouver des justifications au résultat de l'algorithme totalement déconnectés des sous-jacents réels de la décision proposée : ce qui pose des problèmes évidents de transparence vis-à-vis de clients, en matière de conseil ou d'information, mais également un problème plus général de gouvernance en retardant la détection des faiblesses structurelles éventuelles des algorithmes utilisés.

3.1.3. Le cas particulier d'usage des algorithmes dans le contrôle interne et la conformité

L'intelligence artificielle a un fort potentiel de développement dans les domaines du contrôle interne et de la conformité. Dans ce domaine, les usages et la réglementation sont appelés à évoluer de concert.

De fait, les textes actuels[26], s'ils n'excluent pas l'utilisation de l'intelligence artificielle dans le dispositif de contrôle interne, ont été écrits dans l'idée que les contrôles étaient effectués par des humains :

[25] La responsabilité de l'humain qui se trompe « comme l'algorithme » peut sembler atténuée tandis que celle de l'humain qui se trompe contre l'avis de l'algorithme, risque de paraître aggravée, notamment aux yeux de ceux qui le contrôleront.

[26] Arrêté du 3 novembre 2014 relatif au contrôle interne

- Contrôle interne permanent exercé par des personnes exerçant des activités opérationnelles d'une part et par des personnes dédiées à la seule fonction de contrôles des opérations d'autre part ;

- Contrôle interne périodique réalisé par des personnes dédiées, de manière indépendante à l'égard des personnes, entités et services qu'elles contrôlent.

Il paraît toutefois difficile, dans une perspective de généralisation de l'intelligence artificielle, d'exclure par principe du champ de sa mise en œuvre les activités de contrôle interne, dont certaines peuvent être effectuées plus efficacement et à plus grande échelle par des algorithmes. Par ailleurs, la substitution croissante de processus automatisés, « intelligents » ou non, à des décisions humaines appelle en tout état de cause une révision de la cartographie des risques et des contrôles.

Aussi, l'introduction de l'intelligence artificielle, dans les processus opérationnels ou dans les contrôles eux-mêmes, appelle-t-elle une réflexion spécifique sur les modalités du contrôle réservé aux humains. À cet égard, si certaines formes de contrôle opérationnel sont amenées à disparaître, il convient aussi d'identifier les nouvelles formes de contrôle susceptibles d'exister, par exemple, dans les modèles d' « apprentissage supervisé ». Enfin, les interactions entre hommes et algorithmes, évoquées ci-dessus, doivent être prises en compte dans la conception des différents niveaux de contrôle permanent.

3.2. Les enjeux liés aux restructurations possibles du marché

Comme il a été rappelé dans la première partie, le développement de l'intelligence artificielle s'effectue dans un contexte de profonde mutation des infrastructures informatiques ; et elle contribue à cette mutation.

L'analyse du superviseur serait donc incomplète s'il ne prenait pas en compte les modifications que cette mutation est susceptible d'entraîner à la fois sur la nature ou la taille des organismes financiers, leurs interactions avec les fournisseurs technologiques et le déplacement éventuels des risques entre les différents acteurs.

3.2.1. Phénomènes de concentration ou de fragmentation envisageables

La quantité et la qualité des données étant un facteur déterminant dans le développement de l'intelligence artificielle, les acteurs qui détiennent déjà des données utiles en quantité bénéficient d'un avantage certain. Comme l'ont souligné les premières parties de ce rapport, cet avantage est particulièrement marqué pour les acteurs du *cloud* qui fournissent des services d'intelligence artificielle, puisqu'ils sont susceptibles de drainer davantage de données pour améliorer encore la performance de leurs algorithmes. La position oligopolistique de ces grands acteurs, déjà nettement affirmée, pourrait être renforcée par le développement de l'intelligence artificielle. De fait, de nombreux organismes interrogés envisagent de recourir à l'intelligence artificielle « comme service ».

Par conséquent, les problématiques déjà identifiées par les autorités de contrôle en matière de *cloud computing*[27] pourrait se retrouver *mutatis mutandis* dans les processus

[27] Recommendations on outsourcing to *cloud* service providers. On notera que l'EBA suggère que l'audit collectif d'un acteur majeur du *cloud computing* est une possibilité, premier signe d'une adaptation des superviseurs aux phénomènes de nouvelles mutualisations rendues nécessaires par les mutations technologiques.

dépendant des services d'IA rendus pas quelques grands prestataires technologiques. En particulier, l'inversion du rapport de force traditionnel entre organisme financier et sous-traitant et, peut-être plus encore, le décalage de compétences technologiques qui risque de croître entre ces deux parties, interroge sur l'effectivité à terme des règles encadrant aujourd'hui l'externalisation de « services essentiels[28] ».

À l'inverse de ce phénomène de concentration technologique, et concomitamment[29], peut également se produire un phénomène de ré-intermédiation, avec la multiplication d'acteurs de niche – spécialisés dans une clientèle ou dans un service. Ce phénomène, déjà visible dans le secteur des paiements en raison d'autres mutations technologiques, peut se voir renforcé, au moins dans un premier temps, par la rapidité des acteurs de la Fintech à identifier et à mettre en œuvre des services nouveaux ou plus efficaces rendus possibles par l'intelligence artificielle.

Une telle réorganisation du marché, si elle se produisait, ne serait pas sans poser des questions plus fondamentales aux superviseurs :

- En termes de contrôle individuel des organismes : l'hétérogénéité de la population à contrôler, tant en termes de taille que d'activité, appellerait à réviser les méthodes de contrôle et à prendre davantage en compte les risques de dépendance entre les acteurs. Elle questionnerait également l'approche actuelle de la réglementation qui tend à lier proportionnalité des règles applicables et statut d'exercice – la multiplication des statuts pour rendre compte de la diversification des modèles d'affaires ayant comme risques la perte de lisibilité de la réglementation et l'arbitrage réglementaire.

- En termes d'évaluation des risques pesant sur la stabilité financière : le déplacement de certains risques chez quelques prestataires technologiques, la création de nouveaux réseaux, plus complexes, d'acteurs interdépendants pourraient également amener à réétudier les méthodes actuelles d'appréhension des risques systémiques par les autorités de contrôle[30].

3.2.2. Recherche de mutualisation et responsabilité des organismes

Un autre phénomène lié au développement des nouvelles technologies, aux coûts de développement de nouvelles compétences et à la corrélation positive entre performance des algorithmes et disponibilité des données que l'IA induit est la recherche par les acteurs de marché de nouvelles mutualisations possibles.

---

[28] La liste de services essentiels dans lesquels l'IA pourrait trouver à s'appliquer est longue. Sur la base des réponses reçues, on peut citer notamment :

- Le calcul des échelles de tolérance de risque et d'aversion de perte ;
- L'identification de modèles d'épargne individuels ;
- L'allocation d'actifs ;
- L'optimisation de la tarification ;
- La gestion active ;
- L'analyse financière ;
- La gestion des sinistres en assurance ;
- La lutte contre la fraude ;
- La lutte contre le blanchiment et le financement du terrorisme.
- …

[29] Ce scénario de concentration et d'émergence simultanée d'acteurs de niche a été décrit, dans une approche plus globale, dans un rapport du *World Economic Forum* d'août 2018 : *The new physics of financial services* (page 39)

[30] Big Data meets artificial intelligence, *BaFin*, Juillet 2018

Un exemple de mutualisation possible, donné par des participants à la *task force*, porte sur la LCB-FT. De fait, le développement inégal des techniques d'intelligence artificielle dans ce domaine pourrait avoir pour conséquence non pas de diminuer les risques de blanchiment mais de les déplacer en les réorientant vers les acteurs les moins performants. Ainsi certains acteurs suggèrent une mutualisation des réflexions en matière d'algorithmes destinés à prévenir le risque de blanchiment ou de financement du terrorisme, avec une gouvernance adaptée à cette mutualisation pour :

- leur mise à jour et leur contrôle (incidents, données, faux positifs) ;
- la prévention de la divulgation des règles de fonctionnement afin d'en préserver toute l'efficacité.

Un tel exemple montre les bénéfices qui peuvent être retirés de certaines mutualisations. En termes de pratiques de contrôle, il appelle probablement de la part des autorités de supervision une articulation plus fine entre, d'une part, la normalisation et la mutualisation des processus dans un but d'intérêt général et, d'autre part, des règles qui responsabilisent chaque acteur individuellement en le rendant seul maître de ses choix en matière de gestion des risques.

3.3. Les défis à relever par les autorités de contrôle

Comme le suggère l'exposé précédent, les autorités de supervision doivent envisager les mesures à prendre pour :

- À court terme, accompagner le marché afin de s'assurer de son appropriation des techniques de l'intelligence artificielle dans des conditions qui garantissent le respect des objectifs réglementaires et permettent le contrôle par le superviseur ;
- Anticiper à moyen terme les mutations du marché (concentration, fragmentation, externalisation, mutualisation) pour adapter les réglementations et les méthodes de supervision à ces nouvelles réalités ;
- À ces deux objectifs, il paraît naturel d'en ajouter un troisième : tirer parti des techniques d'intelligence artificielle pour l'exercice de leurs propres missions (« suptech[31] »)

Pour ce faire, les autorités peuvent envisager plusieurs axes d'actions :

- En premier lieu, à l'instar des organismes financiers, l'organisation de leur montée en compétence dans le domaine de l'analyse des données et de l'utilisation de l'intelligence artificielle[32].
- La création de mécanismes de coopération accrue entre superviseurs aux niveaux national et international. À cet égard, dans le domaine de l'intelligence artificielle, l'imbrication des problématiques de protection de données personnelles et des questions règlementaires propres aux secteurs financiers rendent sans doute indispensable une coopération plus étroite entre l'ACPR et la CNIL – tant en termes d'articulation des doctrines que de recherche de synergies dans les compétences à acquérir et les contrôles à mettre en œuvre.

[31] Suptech est une contraction de l'expression « Supervisory technology » et fait référence à l'utilisation des nouvelles technologies au service des missions de supervision.

[32] On pourra se reporter à titre d'exemple au programme de recrutement et de formation des personnels, centré sur l'analyse des données, mis en place par la Monetary Authority of Singapore.

- Le soutien aux initiatives de standardisation et de normalisation[33] et plus généralement aux travaux méthodologiques tendant à améliorer l'auditabilité et l' « explicabilité » des algorithmes « intelligents ».

[33] On peut penser par exemple aux normes ISO/IEC AWI 23053[33], tentative de standardisation d'utilisation de l'IA.

4. Annexes

Annexe I: Histoire

Le terme d'IA est apparu pour la première fois en 1956 au Dartmouth College, lors d'une session d'été à laquelle assistent les futurs ténors de la discipline[34]. Selon les organisateurs de l'époque, leur but est «de procéder comme si tout aspect de l'apprentissage ou de toute autre caractéristique de l'intelligence pouvait être décrit d'une manière suffisamment précise pour être simulé par une machine.»

La notion moderne d'IA a émergé dans les années 50 notamment grâce à Alan Turing[35] : une intelligence artificielle imite la façon de réfléchir des humains mais avec les capacités qui lui sont propres. L'IA est alors étudiée en lien avec l'intelligence humaine, parti pris des recherches modernes. En utilisant les mots d'Alan Turing, l'étude de l'IA ne doit pas être guidée par la question: « Les machines peuvent-elles penser ? » mais plutôt par la question : « Un ordinateur digital peut-il tenir la place d'un être humain dans le jeu de l'imitation ?» Le jeu de l'imitation consiste à se faire passer pour un homme ou une femme face à un interlocuteur humain à la suite d'une série de questions posées. Finalement, notons que l'on est passé de la machine à l'ordinateur digital, un parti pris d'Alan Turing, justifié par l'engouement suscité par cette nouvelle technologie à son époque.

Cette approche logiciste se distingue de l'approche neuronale qui consiste à imiter les processus biologiques cérébraux. Cette approche neuronale est davantage en vogue aujourd'hui car elle a réussi à démontrer sa performance dans différents cas d'usage[36]. L'approche neuronale était poussée à l'origine par Frank Rosenblatt de l'Université Cornell qui fut en 1957 le concepteur du perceptron, un réseau monocouche et mono-sortie. En termes imagés, le perceptron représente un seul neurone qui applique la fonction la plus simple (linéaire). Le modèle s'est inspiré lui-même des idées développées par le physiologiste Donald Hebb qui énonce en 1949 « la règle de Hebb ». Celle-ci consiste à modifier la valeur des coefficients synaptiques, qui définissent comment les signaux électriques transitent à travers les synapses entre les neurones, en fonction de l'activité des neurones qu'ils relient. Les travaux de recherche mentionnés sont aujourd'hui considérés comme les précurseurs des réseaux neuronaux[37], une branche du *machine learning*, qui est lui-même une sous-catégorie de l'intelligence artificielle.

[34] J. McCarthy (Dartmouth), Minsky (Princeton), C. Shannon (Bell Labs/MIT), N. Rochester (IBM), T. More (Princeton), A. Newell (Carnegie Tech), H. Simon (Carnegie Tech), A. Samuel (IBM), R. Solomonoff (MIT), O. Selfridge (MIT).

[35] COMPUTING MACHINERY AND INTELLIGENCE, 1950, Alan Turing

[36] Exemple de prouesses de l'IA : Victoire d'AlphaGo sur les champions humains au jeu de Go.

[37] *Une petite histoire du Machine Learning*, Octobre 2015, *Quantmetry*, Héloïse Nonne

Annexe II : Glossaire thématique

Typologie sommaire des techniques d'intelligence artificielle

- Intelligence artificielle (IA) : ensemble des techniques et des applications qui permettent de créer une machine capable d'imiter, de manière autonome, l'intelligence humaine. Dans le cadre du rapport, nous nous limitons à celles ayant au minimum la capacité d'apprentissage automatique.

- *Machine learning* : ensemble d'algorithmes destinés à résoudre des problèmes et dont la performance s'améliore avec l'expérience et les données sans intervention humaine a posteriori[38]. Le *deep learning* est une sous-catégorie du *machine learning*. Le *machine learning* est notamment utilisé pour des besoins de marketing, de détection de fraude, de gestion de portefeuille et d'évaluation des risques (par exemple le scoring de risque).

- *Natural Language Processing* (NLP)/Traitement automatique des langages : permet d'analyser les données textuelles non structurées. Combinés à des techniques de traitement des sons, ces outils permettent également d'analyser des données vocales.

- Biométrie : techniques d'identification des personnes fondées sur des caractéristiques biologiques telles que les empreintes digitales, les traits du visage… ou des caractéristiques comportementales telles que la reconnaissance vocale, la signature, la démarche… Domaine de recherche scientifique en lien avec les techniques d'intelligence artificielle

- Neuroscience : science du système nerveux, tant du point de vue de sa structure que de son fonctionnement, depuis l'échelle moléculaire jusqu'au niveau des organes, comme le cerveau, voire de l'organisme tout entier. Cette discipline est étroitement liée à l'IA puisqu'elle permet de mieux comprendre comment l'humain agit, c'est-à-dire ce que l'IA cherche précisément à faire reproduire aux machines.

- Représentation des connaissances et modélisation des raisonnements : permet de vérifier si les algorithmes proposés remplissent l'objectif poursuivi.

- Décision et gestion de l'incertitude : élaboration d'outils qui permettent d'analyser les données dont la valeur est incertaine.

- Satisfaction de contraintes et satisfiabilité d'une formule logique : recherche plus fondamentale sur la logique.

- Planification et recherche heuristique : recherche sur la construction de planificateur qui permet de produire des plans typiquement utilisés par un robot ou tout autre agent pour l'exécution d'une tâche. Le planificateur définit les entrées, les sorties et les actions possibles et cherchent de manière heuristique le meilleur enchaînement d'actions.

- Agents autonomes et systèmes multi-agents : peuvent être utiles pour simuler l'état de marché.

[38] On trouve dans la littérature également des définitions qui incluent la notion de connaissance et d'apprentissage. Une œuvre a inspiré beaucoup d'entre elles: celle de Russel & Norvig (*Artificial Intelligence: A Modern Approach*, 2003, Russell & Norvig)

- IA et Web : web sémantique, particulièrement important dans le domaine des objets connectés (internet of things).

Les métiers de l'IA

Gouvernance des données

- *Chief Data Officer* : est en charge de faciliter l'accès aux données pour différents métiers de l'entreprise et de repérer parmi toutes les données disponibles les plus pertinentes pour aider au développement des projets et à la prise de décisions de l'entreprise.

- *Data Privacy Officer :* est chargé de veiller au respect des règles de protection des données personnelles par l'entreprise.

- *Chief Data Quality Officer:* est en charge de s'assurer de la qualité des données utilisées par l'entreprise.

Métiers de l'intelligence artificielle

- *Data scientist* : expert qui élabore les algorithmes de *machine learning*.

- *Data analyst* : expert qui crée les bases ou lacs de données nécessaires à l'entreprise puis s'assure de leur bon fonctionnement. Les *data analysts* gèrent l'administration et l'architecture des bases et sont aussi en charge de la modélisation des données.

- *Data ingénieur* : ingénieur qui prépare les données utilisées par les algorithmes de *machine learning* en produisant des nouvelles variables à partir des variables existantes et en participant à la politique de stockage et de traitement des données.

- Ontologiste : expert qui identifie, crée et manipule les graphes de connaissances.

- *Expert en traitement automatique du langage naturel* : expert qui a à la fois des compétences en linguistique et en *data science*.

- *Expert en reconnaissance de formes* : *data scientist* spécialisé dans le traitement des images et des vidéos.

- *Expert en interaction homme-machine* : expert qui conçoit les systèmes et les interfaces facilitant l'usage des outils d'intelligence artificielle par des humains.

Annexe III : Questionnaire

Description du développement de l'intelligence artificielle dans le secteur financier (partie 1 et 2 du document)

1. Avez-vous des commentaires sur la définition de l'intelligence artificielle privilégiée par le document ? (partie 1.1.1)

2. Identifiez-vous d'autres facteurs de développement de l'intelligence artificielle dans le secteur financier que ceux listés dans le document (parties 1.1.2 et 1.2)? Identifiez-vous à l'inverse des freins possibles à ce développement ?

3. Avez-vous des commentaires sur les considérations du document de réflexion sur le recours au *cloud* (parties 1.2.3, 2.2.3 et 2.2.4) ?

4. Avez-vous des commentaires ou des compléments à apporter à la liste des usages identifiés dans la partie 2.1 du rapport ? Le cas échéant, vous pouvez décrire rapidement des projets concrets, en précisant leur niveau d'avancement (étant noté que les informations individuelles resteront strictement confidentielles).

5. Partagez-vous l'analyse des risques de biais des algorithmes exposée dans la partie 2.2.1 ? Quels compléments lui apporteriez-vous ?

6. Même question pour l'analyse des risques de cyber-sécurité (partie 2.2.2)

Enjeux pour les superviseurs (partie 3 du document)

7. Pensez-vous qu'il existe des modèles d'affaires utilisant de l'IA qui ne peuvent pas se développer à cause des règlementations du secteur financier ? Si oui, pouvez-vous préciser la problématique et la ou les dispositions réglementaires en cause ?

8. Au-delà des exigences liées au RGPD, avez-vous connaissance de processus de « gouvernance des algorithmes » développés en cohérence avec la gouvernance générale des organismes du secteur financier ? Si oui, pour quelle activité ? (partie 3.1.1)

9. Quelle définition de l' « explicabilité » des algorithmes vous paraît la plus utile pour la mise en œuvre d'une gouvernance et d'un contrôle des algorithmes dans le secteur financier ? (partie 3.1.2) Connaissez-vous des méthodes pratiques déjà opérationnelles pour assurer cette « explicabilité » ?

10. Quelles sont, selon vous, les méthodes les plus prometteuses pour assurer la fiabilité des algorithmes ? (partie 3.1.2)

11. Avez-vous pris en considération, dans la définition de processus opérationnels ou de contrôle, les spécificités des interactions humains-algorithmes intelligents ? (partie 3.1.2)

12. Quelles mesures de contrôle interne spécifiques appelle, selon vous, l'usage de l'IA ? (on pourra préciser en fonction du domaine dans lequel est employée l'IA, vente au client, tarification, gestion, LCBFT, modèles internes pour le calcul des exigences réglementaires, etc.)

13. Pensez-vous possible, dans le secteur financier, de confier des contrôles de « niveau 1 », de « niveau 2 » - voire de « niveau 3 » (contrôle périodique) - à des algorithmes intelligents ?

14. Pensez-vous qu'il soit utile de préciser ou d'illustrer certains principes réglementaires en raison de l'émergence des technologies d'intelligence artificielle ? Si oui, lesquels ?

15. Avez-vous des commentaires sur les phénomènes possibles d'évolution du marché décrits dans les parties 3.2.1 et 3.2.2 ?

16. Pensez-vous que les phénomènes de mutualisation des ressources technologiques doivent être mieux reconnus, voire encouragés par les autorités de contrôle ? Si oui, dans quels domaines ? de quelle façon ?

17. Quels modes d'action devrait privilégier, selon vous, l'autorité de contrôle pour accompagner le développement de l'IA dans le secteur financier et faire face aux enjeux évoqués dans la partie 3 ?

18. Avez-vous des commentaires sur les pistes d'action évoquées dans la partie 3.3 du document ?

19. Quels sont, selon vous, les domaines prioritaires où l'autorité de contrôle devrait fournir des indications au marché sur ses attentes pour réduire l'incertitude réglementaire éventuelle dans laquelle se développent les projets utilisant les techniques d'IA ?

5. Liste des membres de la Task Force

Établissement	Prénom	Nom
ACPR	Pierre	BIENVENU
	Olivier	FLICHE
	Didier	WARZEE
	Su	YANG
AFEPAM	Jérôme	TRAISNEL
AG2R	Tanguy	VINCENT
Allianz	Mathilde	GAROTIN
AMF	Alexandre	BARRAT
	Louis	CHARPENTIER
Aviva	Gilles	PAVIE-HOUDRY
AXA	Martin	DETYNIECKI
	Marie-Neige	COURIAUT
	Cécile	WENDLING
BNPP	Olivier	VANDENBILCKE
BPCE	Loïc	BRIENT
	Bibi	N'DIAYE
CNIL	Sophie	GENVRESSE
CNP Assurance	Romain	MERIDOUX
Crédit Agricole	Alexis	BINAY
	Marie	LHUISSIER
DIGIT/Banque de France	Renaud	LACROIX
	Alexis	LAMING
	Andrés	LOPEZ-VERNAZA
	Farid	OUKACI
	Imène	RAHMOUNI-ROUSSEAU
Direction Générale du Trésor	Geoffroy	CAILLOUX
	Eliott	COMBE-MAZERON

	Sébastien	RASPILLER
FBF	Frédérique	FAGES
	Béatrice	LAYAN
FFA	Jérôme	BALMES
	François	ROSIER
Générali	Sylvain	MOLLET
	David	WASSONG
Groupama	Nicolas	MARESCAUX
Groupe Crédit Mutuel	Marc	RAINTEAU
HSBC	Remi	BOURRETTE
	Julien	MIQUEL
ING	Thierry	DE LA SALLE
	Nicolas	SERRE
La Banque Postale	Fabien	MONSALLIER
Macif	Mehdi	LAHCENE
Nalo	Guillaume	Piard
Orange Bank	Djamel	MOSTEFA
Paylead	Alexis	DEUDON
	Charles	DE GASTINES
	Jérémie	GOMEZ
Société Générale	Marianne	AUVRAY-MAGNIN
	Bernard	GEORGES
Treezor + Hi Pay	Omar	SAADOUN
Younited-Credit	Romain	MAZOUE
Tracfin	-	-

La Task Force s'est appuyée sur la participation de bien d'autres contributeurs de chacun des établissements cités ainsi que les établissements suivants : Deloitte, DoYouDreamUp, Dreamquark, Microsoft, Quantcube, Shine, Zelros, l'université de Strasbourg… Et une vingtaine d'autres spécialistes du domaine.

6. Bibliographie

- La révolution numérique dans les banques et les assurances françaises, ACPR, mars 2018. Les études sectorielles (banque et assurance) sont disponibles sur le site de l'ACPR.
- Donner un sens à l'intelligence artificielle, Cédric Villani, mars 2018.
- *Artificial intelligence and machine learning in financial services*, Financial Stability Board, novembre 2017.
- La norme de pratique NPA 5, Institut des actuaires, novembre 2017.
- Recommendations on outsourcing to *cloud* service providers, European Banking Authority.
- *The new physics of financial services, World Economic Forum*, août 2018.
- Big Data meets artificial intelligence, *BaFin,* Juillet 2018.
- COMPUTING MACHINERY AND INTELLIGENCE, Alan Turing, 1950.
- *Artificial Intelligence: A Modern Approach*, Russell & Norvig, 2003.
- *Principles to Promote Fairness, Ethics, Accountability and Transparency (FEAT) in the Use of Artificial Intelligence and Data Analytics in Singapore's Financial Sector*, Monetary Authority of Singapore, novembre 2018.
- *OECD work on artificial intelligence*, OECD, Octobre 2018.