

Louvain School of Management

L'intelligence artificielle et la robotic process automation au service de la gestion des risques dans le secteur bancaire :

Tendances et défis

Auteur : Alexandre Senden
Promoteur : Luc Henrard
Année académique 2020-2021
Travail de fin d'études (TFE) en vue d'obtenir le titre de
Master [120] en sciences de gestion, à finalité spécialisée
Horaire de jour

Je tiens à remercier Luc Henrard, en sa qualité de promoteur, pour ses observations et conseils d'une grande valeur dans la réalisation de ce mémoire.

Je remercie également ma famille : mon père pour ses relectures, corrections et conseils toujours appréciés, ma mère pour son soutien moral et affectif, ma sœur pour son soutien moral et son aide à la retranscription des entretiens.

J'adresse mes remerciements aux personnes interrogées qui ont pris le temps de s'entretenir avec moi. Notamment, Ruben Olieslagers qui m'a conseillé des lectures et m'a permis d'obtenir un entretien supplémentaire.

Finalement, je remercie mes amis pour avoir montré à maintes reprises leur support inconditionnel. Particulièrement, Maxime Dom pour ses éclaircissements techniques.

TABLE DES MATIÈRES

TABLE DES MATIÈRES	III
INTRODUCTION	5
MÉTHODOLOGIE.....	7
PARTIE 1 : INTELLIGENCE ARTIFICIELLE VERSUS ROBOTIC PROCESS AUTOMATION	9
Introduction	9
Section 1 : Intelligence artificielle	10
Sous-section 1.1 : Historique.....	10
Sous-section 1.2 : Définitions.....	15
Sous-section 1.3 : Les capacités de l'IA	17
Sous-section 1.4 : Perspectives IA globales et dans le secteur bancaire.....	19
Sous-section 1.5 : Critiques, éthique et risques de l'IA.....	20
Section 2 : Robotic Process Automation	25
Sous-section 2.1 : Définitions.....	26
Sous-section 2.2 : Les lois de la robotique	26
Sous-section 2.3 : Perspectives RPA pour la fonction finance et dans le secteur bancaire	26
Conclusion.....	29
PARTIE 2 : LA TAXONOMIE DES RISQUES	30
Introduction	30
Section 1 : Gestion des risques	30
Sous-section 1.1 : Définition, dimensions, objectifs et cycle	30
Sous-section 1.2 : Mesures de risque.....	33
Sous-section 1.3 : Appétit pour le risque.....	38
Section 2 : Les types de risques	40
Sous-section 3.1 : Risque de marché (« market risk »)	41
Sous-section 3.2 : Risque de crédit (« credit risk »)	41
Sous-section 3.3 : Risque opérationnel (« operational risk »)	41
Sous-section 3.4 : Risque de liquidité (« liquidity risk »)	41
Sous-section 3.5 : Autres risques.....	42
Sous-section 3.6 : Risque de réputation (« reputational risk »)	43
Sous-section 3.7 : Risques émergents (« emerging risks »)	43
Section 3 : Comment une banque assure la gestion des risques en pratique ?	43
Sous-section 3.1 : Principes de gouvernance.....	44
Sous-section 3.2 : Contrôle interne.....	46
Sous-section 3.3 : Auditeurs externes.....	47
Section 4 : Quelle sélection de risques pour ce mémoire ?	47
Conclusion.....	49
PARTIE 3 : TENDANCES ET DÉFIS PRINCIPAUX	51
Introduction	51
Section 1 : Tendances principales.....	51
Section 2 : Défis principaux.....	56
Conclusion.....	60
PARTIE 4 : RÉSULTATS	61

Introduction	61
Section 1 : L'IA ou un domaine toujours abstrait.....	61
Section 2 : La RPA ou un domaine bien plus clair	63
Section 3 : Aperçu des approches IA et RPA des banques de notre échantillon.....	64
Section 4 : Éthique.....	65
Section 5 : Le cycle de gestion des risques	67
Section 6 : Impact de la gouvernance d'entreprise	69
Section 7 : Les données	70
Section 8 : Applications IA et RPA dans les banques interrogées	71
Sous-section 8.1 : BGL BNP Paribas	71
Sous-section 8.2 : BNP Paribas Fortis.....	74
Conclusion	76
CONCLUSION.....	80
BIBLIOGRAPHIE	83
ANNEXE	92
Annexe 1 : Liste des personnes interrogées	92
Annexe 2 : Laurent Denis – Responsable Enterprise Risk Architecture à la BGL BNP Paribas.....	93
Annexe 3 : Orce Marinkovski – Responsable Robotic Process Automation & Concepteur et Développeur de produits à la BGL BNP Paribas	107
Annexe 4 : Ruben Olieslagers – Responsable du CFO Office (Data Management, Validation Committees, & Environment and Socializing Governance) chez BNP Paribas Fortis	117
Annexe 5 : Augustin Borsu – Responsable Analytics & AI et déploiement support chez BNP Paribas Fortis	122
Annexe 6 : Marc Aguilar – Chief Data Officer à la BGL BNP Paribas.....	129
Annexe 7 : Texte original de la proposition de projet de recherche estival de Dartmouth sur l'IA.....	140
Annexe 8 : Dialogue entre ELIZA et une utilisatrice	141
Annexe 9 : Répartition des risques les plus représentés pour chaque catégorie de risque	142
Annexe 10 : Carte thermique des indicateurs de risque pour le Q1 2021 (EBA, 2021, p. 5).....	143
Annexe 11 : Taxonomie des risques détaillée – catégories de risque et sous-risques : définitions.....	144
Annexe 12 : Zooms sur les risques émergents.....	145
Annexe 13 : Les principes d'évaluation des systèmes de contrôle interne classé par sources de déficiences	151
Annexe 14 : Degré d'utilisation d'applications IA pour la gestion du risque	152
Annexe 15 : Degré d'utilisation d'applications IA pour les activités de back office	153
Annexe 16 : Les applications IA et RPA sur les risques de crédit, fraude, et conformité pour les deux banques de notre échantillon.....	154

INTRODUCTION

Depuis quelques années, les institutions financières réorganisent leurs modèles d'entreprise traditionnels pour faire face aux nouveaux défis du 21^{ème} siècle. Les nouvelles technologies sont parties intégrantes de ce remodelage. Les banques entrevoient des possibilités et des challenges liés à ces nouvelles technologies. Parmi les plus intéressantes, nous retrouvons l'intelligence artificielle (IA) et la robotic process automation (RPA). De plus en plus, les banques et autres acteurs du système financier incluent l'IA et la RPA dans leurs nouvelles méthodes de travail. D'une part, l'IA vue comme un domaine en forte expansion dont l'évolution est floue mais suggère de grandes promesses. « *AI is the 'new electricity' ... just as electricity transformed many industries roughly one hundred years ago; AI will also now change every major industry.* » (Andrew Ng, 2007). D'autre part, la RPA perçue comme la technologie phare et conductrice de l'automatisation à grande échelle.

Ce mémoire va étudier les tendances et défis principaux à la suite de l'apparition de ces nouvelles technologies dans le secteur bancaire. Nous allons évaluer ces tendances et défis dans le prisme de la gestion des risques. Plus particulièrement, nous nous concentrerons sur trois risques de la taxonomie des risques : risque de crédit, risque de fraude, et risque de conformité. Également, cette étude vise à évaluer les tendances et défis principaux sur deux places financières européennes : la place financière belge et la place financière luxembourgeoise.

Nous commencerons par détailler la méthodologie et le raisonnement retenus qui nous ont conduit à nos résultats.

Ensuite, nous allons brosser le portrait de ce que sont l'intelligence artificielle et la robotic process automation. Nous aborderons des notions historiques, leurs définitions respectives, les perspectives qu'elles impliquent et les sujets sensibles liés à ces technologies.

Une fois ces concepts étudiés, nous allons nous intéresser à la taxonomie des risques dans la deuxième partie. Nous débiterons par des explications relatives au domaine de la gestion des risques pour comprendre l'environnement dans lequel la taxonomie des risques évolue. Les catégories principales de la taxonomie seront alors détaillées. Ensuite, nous expliquerons comment une banque aborde la gestion des risques en pratique et nous terminerons en développant le chemin de pensée qui nous a mené à sélectionner les risques considérés dans ce mémoire.

La partie suivante permettra d'appréhender d'une part les tendances principales, d'autre part les défis principaux auxquels les institutions financières sont confrontées en matière d'IA et de RPA. Ceci permettra de mettre en lumière les domaines où les possibilités IA et RPA semblent être les plus pertinentes aujourd'hui mais pour lesquelles il existe également des challenges tangibles.

Ces éléments considérés, nous analyserons nos données au regard de notre revue de la littérature et développerons nos résultats. Nous suivrons au plus près la logique de rédaction de ce mémoire lors de la mise en évidence de ces résultats.

Finalement, nous terminerons par une conclusion qui résumera les éléments les plus importants et pertinents.

MÉTHODOLOGIE

Pour ce mémoire, nous avons choisi de nous concentrer sur une recherche primaire qualitative. La collecte de données a été réalisée à l'aide d'entretiens semi-directifs.

Une approche quantitative a été considérée mais rapidement écartée pour plusieurs raisons. Tout d'abord, une évaluation quantitative des tendances et défis de l'IA et la RPA sur la gestion des risques en secteur bancaire est particulièrement délicate dans la mesure où la quantité d'informations publiques disponibles est faible. Les comptes annuels des banques ne fournissent, en effet, pas beaucoup de détails quantitatifs ni d'analyses d'impact de leurs utilisations d'outils basés sur de l'IA et/ou de la RPA. De plus, l'automatisation via des systèmes d'IA et de RPA étant relativement récente, une approche qualitative semblait être la meilleure solution pour notre sujet. Également, nous évoquons la réalisation d'enquêtes quantitatives auprès de différentes banques pour évaluer les tendances et défis de l'IA et de la RPA. Cependant, des enquêtes n'auraient pas permis à nos interviewés de transmettre pleinement leur message puisque des enquêtes, par leur nature, manquent généralement de nuances pour comprendre profondément les subtilités du sujet traité. Les éléments ci-dessus ont permis de conclure qu'une approche qualitative était la meilleure option disponible.

La technique de collecte de données retenue dans ce mémoire est donc l'entretien semi-directif. En effet, cette technique permet de récolter des éléments de réflexion riches et nuancés que les interviewés n'auraient pas nécessairement aimé partager par le biais d'une enquête pour des questions de confidentialité. En outre, cette technique donne les moyens à l'enquêteur de comprendre le sens que les personnes interrogées donnent à leurs actions et aux événements auxquels elles sont confrontées. Les entretiens semi-directifs permettent également d'analyser un problème spécifique en étudiant les données disponibles, les différents points de vue sur les sujets et les questions en jeu. Enfin, ils permettent de reconstruire les processus d'action, d'expériences et d'événements du passé (Van Campenhoudt, Quivy, & Marquet, 2011, pp. 170-172). En tant que telle, cette technique est l'outil idéal pour évaluer les tendances et défis de l'IA et la RPA sur la gestion des risques dans le secteur bancaire.

Ces entretiens semi-directifs ont été constitués de la manière suivante. Nous avons scindé les entretiens en trois sections. La première section abordait des aspects généraux sur le profil de nos interviewés et sur les grandes lignes de l'IA et la RPA. Les deux autres sections traitaient tour à tour de l'IA et de la RPA et de leurs utilisations sur les trois risques considérés.

Les profils interrogés étaient variés et comprenaient tant des spécialistes techniques en termes d'IA et RPA que des responsables ayant une vue plus globale et des affinités avec ces technologies. Les annexes 1 à 6 (pp. 92-139) proposent une liste des interviewés et les retranscriptions de nos entretiens.

Afin d'analyser nos données, nous avons utilisé la méthode d'analyse de contenu thématique qui consiste, dans un premier temps, à déstructurer les données en codes et, dans un deuxième temps, à restructurer les données en concepts (De Moerloose, 2020). Les codes attribués ont été basés sur la revue de la littérature.

PARTIE 1 : INTELLIGENCE ARTIFICIELLE VERSUS ROBOTIC PROCESS AUTOMATION

Introduction

L'informatique a connu des progrès considérables ces dernières décennies. À l'origine, un simple calculateur capable de résoudre de brèves opérations. Au fil de temps, ce domaine a évolué pour offrir toujours plus de possibilités. Aujourd'hui, l'informatique est extrêmement vaste et regroupe un tas de sciences, techniques et applications différentes. Pour la comprendre dans sa globalité, il est nécessaire de parcourir la taxonomie de l'informatique.

Où se positionnent l'IA et la robotique dans cette sphère nébuleuse que désigne l'informatique ? Nous pouvons utiliser un diagramme d'Euler pour représenter cette taxonomie (voir figure 1). RPA et IA sont donc des sous-domaines de l'informatique avec la RPA étant elle-même un sous-domaine de l'IA.

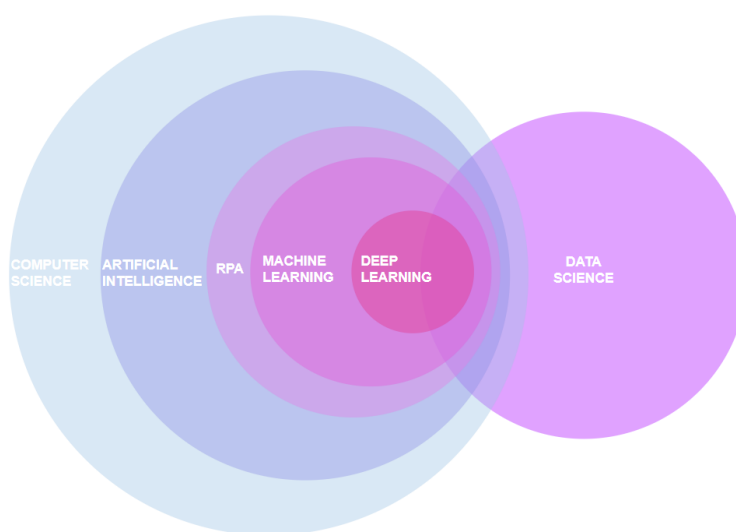


Figure 1 : Diagramme d'Euler représentant la taxonomie de l'informatique

Source : inspiré du cours en ligne Elements of AI développé par Reaktor et l'Université d'Helsinki
(complètement référencé en bibliographie)

Cependant, une distinction s'impose entre IA et RPA. En effet, bien que la RPA puisse être caractérisée comme un sous-domaine de l'IA, elle n'utilise pas toujours les techniques qui lui sont associées.

Section 1 : Intelligence artificielle

Sous-section 1.1 : Historique

Cette sous-section va retracer l’historique de l’intelligence artificielle, se focalisant sur ses avancées notables qui ont permis d’arriver à ce qu’elle est aujourd’hui – bien qu’une définition unanime n’existe pas encore, comme nous le verrons dans la section suivante.

Esprit-corps et analogie avec l’IA. Pour retracer les racines de l’IA, il est bon de parler de René Descartes (1596-1650), mathématicien, physicien et philosophe français du 17^{ème} siècle. Descartes était un dualiste et proposait une distinction claire entre l’esprit et le corps, autrement appelés substances mentales et substances corporelles (O’Regan, 2016, p. 253). C’est justement cette distinction qui est très pertinente pour l’IA dans la mesure où une analogie apparaît entre l’esprit et le cerveau humains en tant que logiciel fonctionnant sur un ordinateur, comme suggéré par O’Regan dans son ouvrage. Descartes parle alors de chose pensante (*res cogitans* ou esprit/âme) qui est distincte du reste de la nature (*res extensa*). Cette chose pensante interagit avec le monde par le biais des sens pour acquérir des connaissances qui, elles, sont acquises par des opérations mentales. C’est pourquoi on octroie à Descartes la création de l’école rationaliste de la philosophie, où la connaissance est dérivée uniquement par le raisonnement humain (O’Regan, 2016, p. 253). Entre ici l’analogie de l’esprit avec l’intelligence artificielle. L’esprit humain serait un programme d’IA fonctionnant sur un ordinateur et dont les connaissances sont acquises par la perception des sens à l’aide de capteurs et par déduction logique. O’Regan écrit alors :

The significance of Descartes in the field of artificial intelligence is that the Cartesian dualism that humans seem to possess would need to be reflected among artificial machines. Humans seem to have a distinct sense of ‘I’ as distinct from the body, and the ‘I’ seems to represent some core sense or essence of being that is unchanged throughout the person’s life. It somehow represents personhood, as distinct from the physical characteristics of a person that are inherited genetically. The long-term challenge for the AI community is to construct a machine that (in a sense) possesses Cartesian dualism: i.e. a machine that has awareness of itself as well as its environment. (O’Regan, 2016, p. 254)

Le test de Turing. Dans cette réflexion sur les origines de l’intelligence artificielle, nous pouvons nous appuyer sur les prémices de l’informatique. L’éminent mathématicien Alan

Turing (1912-1954), bien connu pour avoir contribué au décryptage de la machine Enigma, permettant ainsi de décoder les messages des Allemands durant la seconde guerre mondiale mais aussi pour ses avancées en mathématiques et informatique, proposait en 1950 un test déterminant dans la conception de l'intelligence artificielle. « Une machine peut-elle penser ? » était le questionnement de départ de Turing (Bertrand, 1987, p. 35). Pour le prouver, Turing a développé ce qu'il a appelé le « jeu de l'imitation » ou, plus populairement aujourd'hui, le Test de Turing. Le test consiste à faire interagir, via un système de chat, une personne avec une machine capable d'imiter une conversation humaine. Une personne, appelée interrogateur, est alors confrontée à la machine et à une autre personne et doit converser avec eux. L'interrogateur les connaît sous les labels X et Y, sans connaître qui est qui au début du test. Une fois le test terminé, il est demandé à l'interrogateur de dire s'il a pu distinguer la machine de la personne, par exemple : « X est la machine et Y est la personne » ou « X est la personne et Y est la machine » (Oppy & Dowe, 2020, p. 4). Nous posons ensuite les questions suivantes : « Que se passera-t-il lorsqu'une machine prendra la place d'une personne dans ce jeu ? L'interrogateur se trompera-t-il aussi souvent lorsque le jeu se déroule ainsi que lorsqu'il s'agit d'un jeu entre un homme et une femme ? ». Ces questions remplacent ensuite la question initiale « Une machine peut-elle penser ? » (Kok, Boers, Kusters, van der Putten, & Peol, 2009, p. 3). Finalement, si l'interrogateur n'a pas été en mesure de distinguer la machine de l'autre personne, on considère que la machine a passé le test avec succès. À propos de ce jeu, Turing (1950) écrivait ceci :

I believe that in about fifty years' time it will be possible to programme computers, with a storage capacity of about 10^9 , to make them play the imitation game so well that an average interrogator will not have more than 70 per cent, chance of making the right identification after five minutes of questioning. (Turing, 1950, p. 10)

Pourtant, aucune machine à ce jour n'a été capable de passer le test de Turing avec succès même si un prix¹ est accordé chaque année à la machine qui s'en rapproche le plus.

Turing pensait donc que le fonctionnement de la pensée était équivalent à celui d'une machine à états discrets. Ses travaux et la perception qu'un ordinateur, muni du programme adéquat, aurait des propriétés mentales humaines sont connus sous le terme d'intelligence artificielle forte (O'Regan, 2016, p. 257).

¹ Prix Loebner, https://fr.wikipedia.org/wiki/Prix_Loebner

Intelligence artificielle ? Depuis le début de ce mémoire, nous parlons d' « intelligence artificielle » sans questionner l'origine du terme. McCarthy (1927-2011) et l'année 1956 sont les deux éléments conduisant à la locution intelligence artificielle. En effet, l'intelligence artificielle a été dénommée pour la première fois dans la proposition de projet de recherche estival de Dartmouth rédigée par McCarthy (voir annexe 7, p. 140) en 1955 et dont le projet a eu lieu en 1956. Cette période a été très prospère pour l'intelligence artificielle puisque les spécialistes de l'époque, étant convaincus que les machines bientôt imiteraient l'intelligence humaine, réussissaient à convaincre des agences de financement et l'armée d'accorder des subventions de recherche (O'Regan, 2016, p. 254).

Logic Theorist & The advice taker. À la suite de cette période prospère, de nombreux programmes révolutionnaires ont vu le jour. Simon et Newell développaient en 1956 le premier vérificateur de théorèmes grâce à un programme appelé « Logic Theorist » ou « LT ». Ce programme montrait que les ordinateurs étaient capables d'encoder des connaissances et informations et d'y appliquer des opérations intelligentes (O'Regan, 2016, p. 255). McCarthy également développait the advice taker, un programme apte à tirer des conclusions selon un ensemble de postulats. À ce propos, McCarthy rapportait : « *a program has common sense if it automatically deduces for itself a sufficiently wide class of immediate consequences of anything it is told and what it already knows.* » (McCarthy, 1959, p. 2).

Unimate. Étroitement liée à l'IA, la robotique voit également le jour au cours des années 60 avec pour pères Joseph Engelberger et George Devol. Ensemble, ils fondent Unimation, la première entreprise de production de robots et en 1961, ils vendent leur premier robot appelé « Unimate » (Sudarshan, Abhishek, & Gupta., 2017, p. 2). Le géant américain de l'industrie automobile General Motors a été l' « early adopter » de cette nouvelle technologie qui s'est avérée être un franc succès de par sa fiabilité et sa performance. Elle a également permis à General Motors d'économiser de l'argent en remplaçant du personnel par des machines (O'Regan, 2016, p. 268).

ELIZA. En 1966 au MIT², l'informaticien allemand Joseph Weizenbaum (1923-2008) créait ELIZA, l'un des premiers programmes de traitement de langage naturel. Eliza était capable d'interagir en anglais avec un utilisateur assis devant une machine à écrire électrique. Le programme était paramétré pour décomposer les messages utilisateurs et y répondre de telle

² Massachusetts Institute of Technology

façon à ce que le dialogue continue. La particularité d'Eliza était que le programme semblait être capable de compréhension réelle, comme le rapportaient de nombreux utilisateurs à l'époque (voir annexe 8 pour un exemple de dialogue avec Eliza, p. 141). Cette conviction d'une interaction humaine avec un programme a conduit à poser des questions éthiques sur les effets de l'IA. Cet aspect éthique sous-tendant l'IA poussait plus tard Weizenbaum à devenir un fervent critique de l'IA (O'Regan, 2016, p. 259). Nous verrons ses positions sur le caractère éthique de l'IA dans la sous-section 1.5 sur les critiques, l'éthique et les risques de l'IA.

IA forte et faible. Plus tôt, nous mentionnons que la perception de Turing d'une machine était qualifiée comme IA forte. Mais qu'est-ce que l'IA forte ? De plus, s'il y a une IA forte, il doit également y avoir une IA faible, autrement la forme forte n'aurait raison d'exister. Cette distinction a été conceptualisée par Searle en 1980.

- IA forte : « *The computer is not merely a tool in the study of the mind, rather the appropriately programmed computer really is a mind in the sense that computers given the right programs can be literally said to understand and have other cognitive states. [Searle's 1980 Definition]* » (O'Regan, 2016, p. 257) ;
- IA faible : « *discipline scientifique ... qui se contente de simuler des facultés cognitives spécifiques comme la reconnaissance de la parole, la compréhension du langage naturel ou la conduite automobile* » (Ganascia, 2019, p. 73).

Systèmes experts. Le développement des systèmes experts, ou SE, a commencé dans les années 60 aux États-Unis et a connu un essor en entreprise dans les années 80. Ils ont été une grande réussite dans le domaine de l'intelligence artificielle (O'Regan, 2016, p. 270). Les SE utilisent les connaissances humaines pour résoudre des problèmes qui, normalement, requièrent de l'intelligence humaine (Tripathi, 2011, p. 19). À cette définition, Piechowiak (2003, p. 4) ajoute que les SE utilisent des connaissances directement liées aux domaines mais également des capacités de raisonnement acquises par les spécialistes au cours de leur activité. En ce sens, les SE font appel aux connaissances génériques du domaine étudié et aux connaissances d'experts qui ne relèvent pas des connaissances publiques. Ces experts établissent un ensemble de règles que le SE va appliquer sur une base de données pour ensuite inférer sur les possibles résolutions du problème. La structure fondamentale des SE a été posée par Shortliffe en 1976 avec « Mycin » et « E-Mycin ». Le SE était composé d'un ensemble de connaissances sur un domaine donné et d'un logiciel, appelé moteur d'inférence, qui contenait les règles de

traitement de ces connaissances (Blanc, Charron, & Freyssenet, 1989, p. 10). O'Regan (2016, p. 270) explicite les composants d'un SE :

- Base de connaissances : les connaissances sont représentées sous un ensemble de règles sous la forme « si *conditions*, alors *conclusions* » ;
- Moteur d'inférence : prend en charge le raisonnement par lequel le SE parvient à une conclusion ;
- Système explicatif : explique comment une conclusion a été atteinte ;
- Interface : interface entre le SE et l'utilisateur ;
- Base de données : interpréter des mesures fournies par l'utilisateur et puiser directement dans les données.

AI Winters. L'attrait pour l'IA a connu des hauts et des bas. Pour les bas, on parle d' « hivers de l'IA », terme emprunté de l'anglais « AI Winters » et inventé par Marvin Minsky et Roger Schank lors du meeting annuel de 1984 de l'American Association of Artificial Intelligence (aujourd'hui l'Association for the Advancement of Artificial Intelligence ou AAAI). Deux périodes entrent en compte comme hivers de l'IA : 1974 à 1980 et 1987 à 1993. Umbrello (2021, pp. 7-8) fournit les facteurs principaux de ce pessimisme autour de l'IA à ces époques. L'élément majeur est attribuable aux promesses trop ambitieuses faites à l'époque qui se sont avérées être de loin trop humbles par rapport aux attentes, provoquant des pertes perceptibles de confiance en l'IA. Un autre facteur était la disponibilité insuffisante des capacités informatiques, amenant l'IA vers ses hivers (Umbrello, 2021, p. 8 ; Sudarshan *et al.*, 2017, p. 2). On aperçoit également un chevauchement des ces hivers avec des périodes de marasmes économiques, limitant l'étendue de la recherche sur des investissements plus tangibles. Finalement, ces périodes étaient marquées par de la survalorisation et de la promotion d'avancées simples (Sudarshan *et al.*, 2017, p. 2). Les facteurs susmentionnés ont véhiculé un certain cynisme dans la communauté des chercheurs en IA, menant ainsi à des réactions indésirables de la part des organismes de financement et à des désinvestissements (Umbrello, 2021, pp. 7-8).

Deep Blue. Amateurs d'échecs, esquissez un sourire. En 1997, le célèbre programme d'échecs Deep Blue arrivait à bout de Garry Kasparov³. Grand maître et champion du monde d'échecs à 12 reprises consécutives à l'heure du rendez-vous avec Deep Blue, Kasparov s'incline 3,5-2,5

³ À savoir qu'un premier match entre Kasparov et Deep Blue avait eu lieu en 1996, cette fois remporté par Kasparov 4-2. En 1997, le programme Deep Blue avait subi des améliorations.

puisque le match se jouait en six manches – une victoire équivalant à un point et une partie nulle à 0,5 points (deux victoires pour Deep Blue, une pour Kasparov et trois manches nulles). Cette anecdote nous permet de mettre en exergue le rôle des échecs qui ont été largement utilisés pour étudier les mécanismes d'inférence et de représentation au cours des premières décennies des travaux sur l'IA (Buchanan, 2005, p. 54).

IA du 20^{ème} siècle à aujourd'hui. Brièvement, nous pouvons consigner les quelques points majeurs de l'IA de ce début de siècle à l'aide de l'article de Sudarshan *et al.* (2017, p. 2). Les auteurs font état d'une ligne du temps succincte sur l'évolution de l'IA. En se concentrant sur les années 2000 à aujourd'hui, on observe des avancées marquantes dans le domaine de l'IA. Notamment en 2004 où a lieu le premier Darpa Challenge, une compétition où des véhicules autonomes sans pilote doivent parcourir un circuit avec succès. Les auteurs notent également la première version de Siri, l'application de commande vocale développée par Apple et lancée en 2011. Finalement, les auteurs font référence à l'ère du Deep Learning (ou DL) commençant en 2012, en considérant que l'engouement actuel pour l'IA est majoritairement conduit par le DL. On voit alors l'apparition du système de DL de Microsoft qui bat l'humain en reconnaissance d'images ou encore l'introduction par Facebook de M, un assistant virtuel.

Arrivés au terme de cette section historique, nous pouvons réutiliser les arguments de Umbrello (2021, p. 8) au sujet de l'enthousiasme contemporain autour de l'IA. Umbrello discute du possible déclenchement d'un troisième hiver de l'IA suivant l'engouement (peut-être) démesuré pour le domaine. Cependant, il prône également que les avancées technologiques actuelles en recherche sur l'IA ont solidifié la croissance pour de futures innovations. Ceci tout en considérant le problème du pipeline qui fait valoir que l'absence de recherche fondamentale en IA mènerait à une quantité limitée de résultats appliqués. De manière optimiste, il termine par dire qu'une « *feedback loop between applied innovation and fundamental research will provide the pipeline enough pressure for continued progress* » (Umbrello, 2021, p. 8).

Sous-section 1.2 : Définitions

L'intelligence artificielle (ou IA) fait l'objet de nombreuses définitions pour deux raisons principales. Premièrement, son étendue reste difficile à caractériser. Deuxièmement, les experts ont tendance à invalider la composante intelligente d'un programme qui se voudrait doté d'IA, faisant ainsi mouvoir sa définition. Nous allons ici parcourir les idées de différents auteurs.

Pour commencer, nous pouvons (et devons) revenir à Turing et son test discuté plus tôt. En résumé, par ce test, Turing cherchait à prouver que les machines peuvent penser et en est arrivé au constat suivant : « n'est intelligente que l'intelligence ». En d'autres termes, l'intelligence serait à évaluer selon la capacité d'autrui à la distinguer d'une autre intelligence. C'est précisément cette conception de l'IA qui va façonner son évolution définitionnelle pour les décennies suivantes.

Le livre de Kok *et al.* (2009, p. 2) compile plusieurs définitions pour finalement exposer que l'IA imite les comportements humains intelligents. Les auteurs continuent et argumentent qu'au lieu de chercher une définition générale de l'IA, nous pouvons faire appel à la définition de systèmes artificiellement intelligents et les classer en quatre catégories :

- Des systèmes qui pensent comme des humains
- Des systèmes qui agissent comme des humains
- Des systèmes qui pensent rationnellement
- Des systèmes qui agissent rationnellement.

Se référer à la définition de systèmes artificiellement intelligents justifie l'imitation par l'IA des comportements humains intelligents dans la mesure où les humains sont dotés d'intelligence et sont rationnels, au moins du point de vue économique⁴.

Dans le rapport de Contri, Galaski, Baumann, Stier, et Celner (2018, p. 4), les auteurs proposent une définition plus élaborée mais non-technique tout en précisant la variété des définitions associées au terme IA. Selon eux, « *artificial intelligence is a suite of technologies, enabled by adaptive predictive power and exhibiting some degree of autonomous learning, that dramatically advance our ability to: recognize patterns, anticipate future events, create good rules, make good decisions, communicate with other people.* » (Contri *et al.*, 2018, p. 4).

Rao et Verweij (2017) suggèrent une définition assez large de l'intelligence artificielle : « *AI is a collective term for computer systems that can sense their environment, think, learn, and take action in response to what they're sensing and their objectives* » (Rao & Verweij, 2017, p. 2). À cette définition, ils ajoutent quatre manières dont l'IA fonctionne (voir figure 2) qui permettent de dissocier le degré de robotisation par rapport au degré d'adaptabilité. Nous observons ici que l'intelligence artificielle se conçoit souvent en termes de capacités plutôt

⁴ Hypothèse de rationalité économique qui veut que l'humain fonctionne de manière rationnelle.

qu'en lui assignant une définition figée. Nous reviendrons sur les capacités de l'IA dans une section qui leurs seront dédiées.

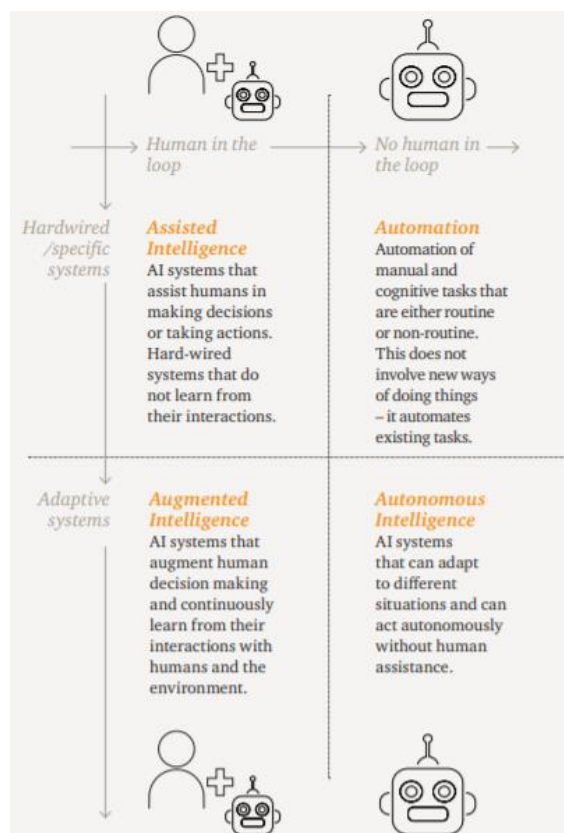


Figure 2 : Les quatre manières dont l'IA fonctionne selon le degré de robotisation par rapport au degré d'adaptabilité

Source : Rao & Verweij, 2017, p. 2

Une définition encore plus large est celle de Christopher *et al.* (2019, p. 7) : « *Artificial Intelligence is the capability of a machine to imitate intelligent human behavior* » ; qui se rapproche de la définition que nous allons considérer dans ce mémoire. En effet, plus simplement, l'IA peut être définie comme une machine dotée d'intelligence non humaine capable d'apprentissage lui permettant de reproduire des logiques et comportements humains.

Sous-section 1.3 : Les capacités de l'IA

Nous avons longuement abordé les définitions de l'IA ce qui a permis d'arborer son étendue et d'en sortir une définition large mais efficace. Maintenant, plutôt que de discuter de ses définitions, nous allons l'exprimer en termes de capacités, rendant ainsi plus précise son application pratique pour un lecteur non aguerri.

À ce sujet, Contri *et al.* (2018, p. 6) rapportent une sélection de termes qui reviennent encore et toujours dans la discussion sur l'IA. Rao et Verweij (2017, p. 26) parlent des domaines de l'IA suivant une méthodologie similaire à celle de Contri *et al.* Nous pouvons donc regrouper leurs découvertes sous un tableau récapitulatif (voir figure 3).

	Terme	Description
Contri <i>et al.</i> (2018, p. 6)	Customization	Generate rules from specific profiles and apply general data to optimize outcomes
	Decision making	Generate rules from general data and apply specific profiles against those rules
	Foresight	Determine the probability of future events
	Interaction	Communicate with humans through digital or analog mediums
	Pattern detection	Recognize regularities in data
Rao & Verweij (2017, p. 26)	Large-scale Machine Learning	Design of learning algorithms, as well as scaling existing algorithms, to work with extremely large data sets
	Deep learning	Model composed of inputs such as image or audio and several hidden layers of sub-models that serve as input for the next layer and ultimately an output or activation function
	Natural Language Processing (NLP)	Algorithms that process human language input and convert it into understandable representations
	Collaborative Systems	Models and algorithms to help develop autonomous systems that can work collaboratively with other systems and with humans
	Computer Vision (Image Analytics)	The process of pulling relevant information from an image or sets of images for advanced classification and analysis
	Algorithmic Game Theory and Computational Social Choice	Systems that address the economic and social computing dimensions of AI, such as how systems can handle potentially misaligned incentives, including self-interested human participants or firms and the automated AI-based agents representing them
	Soft Robotics (Robotic Process Automation)	Automation of repetitive tasks and common processes such as IT, customer servicing and sales without the need to transform existing IT system maps

Figure 3 : Tableau récapitulatif des capacités de l'IA

Source : Adapté de Contri *et al.* (2018, p. 6) et Rao & Verweij (2017, p. 26) (complètement référencés en bibliographie)

Sous-section 1.4 : Perspectives IA globales et dans le secteur bancaire

L'enquête mondiale 2019 auprès de CEOs de PwC a montré que l'intérêt pour l'IA était en hausse. En effet, 85% des CEOs rapportaient que l'IA impacterait significativement la façon dont ils font du business dans les cinq prochaines années (Stijn & de Liedekerke, 2019). Cela ne veut pas dire pour autant que la pénétration de l'IA en entreprise est impressionnante (voir figure 4). Les perspectives au niveau de l'implémentation de solutions IA apparaissent donc comme grandes puisqu'au niveau mondial, seulement 3% des entreprises considéraient les initiatives IA comme fondamentales à leur organisation.

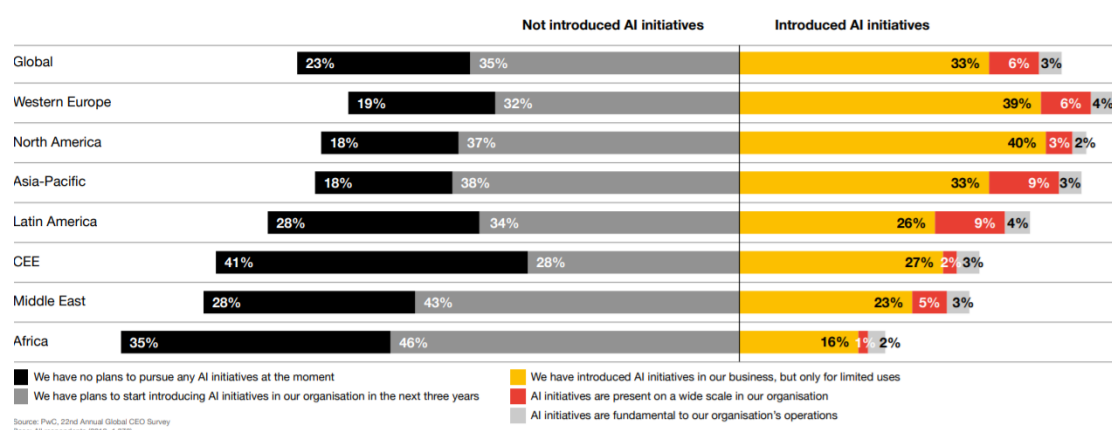


Figure 4 : Pénétration de l'IA en entreprise par niveaux géographiques

Source : PwC 22nd Annual Global CEO Survey (complètement référencé en bibliographie)

En s'intéressant de plus près au secteur bancaire, on observe que les perspectives sont également abondantes. Tout d'abord, il faut savoir que l'IA n'est pas seulement intéressante pour le secteur bancaire, les institutions financières sont aussi intéressées par l'IA. Le prouve les travaux de Buchanan dans lesquels on peut lire qu'en 2018 l'industrie des services financiers, après le secteur des technologies, est le plus dépensier en termes de services IA (Buchanan, 2019, p. 11).

Concernant les technologies disruptives que l'IA permettrait aux banques d'atteindre, McKinsey a identifié quatre résultats prépondérants : 1) des bénéfices plus élevés ; 2) une personnalisation à grande échelle ; 3) des expériences multicanales distinctives ; et 4) des cycles d'innovation rapides (Biswas, Carson, Chung, Singh, & Thomas, 2020, pp. 2-3). Les auteurs notent également une création de valeur potentielle à hauteur de 1000 milliards de dollars pour les banques. Pour ce faire, les banques proposeront alors une expérience et des offres (Biswas *et al.*, 2020, p. 5) :

- Intelligentes : actions recommandées, anticipation et automatisation des tâches et décisions clés ;
- Personnalisées : pertinentes sur le moment et basées sur une compréhension détaillée du contexte et du comportement passé du client ;
- Multicanales : couverture articulée de manière transparente que ce soit physiquement ou en ligne et sur plusieurs appareils.

Sous-section 1.5 : Critiques, éthique et risques de l'IA

Jusque-là, nous avons montré l'IA comme quelque chose d'attrayant, semble-t-il capable d'à peu près toute réalisation puisque dotée d'intelligence. Cependant, comme tous domaines en évolution, l'IA possède ses détracteurs, ses risques et ses questionnements éthiques. Nous allons dans cette section fournir des éléments allant à l'encontre d'une vue utopique de l'IA.

Critiques

Plus tôt, nous parlions des termes IA forte et faible définis par Searle en 1980. Cette même année, Searle a également imaginé une expérience de pensée : la chambre chinoise. Searle se questionnait sur la capacité d'un programme informatique à posséder un esprit capable de comprendre. Autrement dit, il se questionne sur la possibilité pour un programme d'être dit d'IA forte comme le veut la définition du terme.

L'expérience se présente comme suit (O'Regan, 2016, pp. 257-258). Une personne est placée dans une chambre fermée et reçoit des inputs sous la forme de symboles chinois. Un manuel d'apprentissage du chinois est également donné à cette personne. Ce manuel montre comment manipuler les symboles pour produire de l'output en chinois. Cette personne ne sait pas ce que les symboles signifient mais, avec le manuel, elle est capable de produire de l'output en chinois. Ceci permet donc à la personne de communiquer et de répondre à n'importe quelle question qui lui serait posée, sans aucune compréhension de ce qu'elle fait ou de ce que les symboles signifient. Les outputs sont déposés dans un emplacement à cet effet de telle façon à ce que la personne à l'extérieur de la chambre puisse les lire. La personne à l'extérieur va alors penser que la personne à l'intérieur de la chambre parle chinois alors qu'elle ne suit que les règles d'un manuel. Ce processus est similaire à celui d'un ordinateur qui reçoit un input, va le traiter et fournir un output. Avec cette expérience, Searle a construit une machine qui ne peut jamais être mentale puisque modifier le programme impliquerait modifier le manuel et ceci n'augmente en

rien sa capacité de compréhension. Cependant, l'IA forte nous dit qu'un programme adéquat tournant sur une machine serait mental. Searle pose donc que la thèse de l'IA forte serait fausse puisque son expérience montre qu'un programme n'aurait aucune capacité de compréhension. En ce sens, les arguments de Searle sont une réfutation de l'IA forte puisqu'aucune personne, c'est-à-dire une machine, ne serait capable de comprendre la signification des éléments manipulés, même étant fournie un manuel c'est-à-dire un programme. La machine agit comme si elle savait alors qu'elle ne sait que ce qu'elle a été programmée pour savoir. Ceci diffère alors des humains qui sont conscients de la situation dans laquelle ils se trouvent (O'Regan, 2016, pp. 257-258).

Une réfutation bien connue aux positions de Searle se trouve dans l'argument du « System reply », ou en français « Réponse du système ». Cette réponse avance que si un résultat intelligent est produit, alors de l'intelligence doit être trouvée quelque part dans le système (O'Regan, 2016, p. 258). On voit alors une analogie entre le cerveau humain et ses constituants et l'expérience de la chambre chinoise : aucun des constituants ne possède de l'intelligence mais le système (i.e. le cerveau) compris en tant que tout montre intelligence. Les éléments constitutifs de la chambre chinoise manquent peut-être d'intelligence, mais pas le système en tant que tout.

Éthique

Dans la section historique de l'IA, nous abordions Weizenbaum et le programme ELIZA, capable de converser avec des humains à tel point qu'il trompait nombreux d'entre eux sur ses capacités de compréhension réelle. Nous disions notamment que Weizenbaum, réalisant les considérations éthiques liées à l'IA, était devenu un fervent critique de celle-ci. O'Regan (2018, p. 259) rapporte : « *Weizenbaum was shocked to discover that so many users were convinced that the program had real understanding, and users spent hours sharing their personal problems with the program.* ». Il s'est alors questionné sur l'éthique et les implications du domaine de l'intelligence artificielle et de la capacité d'un programme relativement banal à tromper un utilisateur naïf pour qu'il révèle des informations personnelles. Il a alors argumenté que l'IA est une menace à la dignité humaine et que l'IA ne devrait pas remplacer les humains dans des positions où respect et attention sont requis. Il expose également que les machines manquent d'empathie et que nous arriverions à une aliénation et dévaluation de la condition humaine si l'IA venait à remplacer les humains à des postes comme policiers ou juges.

Un autre questionnement éthique a été posé par le célèbre astrophysicien Stephen Hawking (1942-2018) lors du Web Summit 2017 qui s'est tenu à Lisbonne. Il posait la question suivante : « *Will we be infinitely helped by AI or ignored by it and side-lined, or conceivably destroyed by it?* » (Hawking, 2017, 1:56). Il continue : « *AI could develop a will of its own, a will that is in conflict with ours and which could destroy us. In short, the rise of powerfully AI will be either the best or the worst thing ever to happen to humanity.* » (Hawking, 2017, 2:42). Hormis ces dramatiques allégations, Hawking finit par dire :

I am an optimist and I believe that we can create AI for the good of the world... that it can work in harmony with us. We simply need to be aware of the dangers, identify them, employ the best possible practice in management, and prepare for its' consequences well in advance. (Hawking, 2017, 6:33)

Somme toute, l'IA invite à questionner largement l'éthique et même des grands penseurs contemporains comme Hawking émettent des préoccupations quant à son évolution. Le fait est qu'aujourd'hui, le domaine est encore à ses premiers stades mais il nécessite grande prudence dans la manière dont nous l'utiliserons. L'avertissement de Jean Rostand reste d'ailleurs d'actualité : « *La science a fait de nous des dieux, avant même que nous méritions d'être des hommes.* » (Rostand, 1954).

Risques

Afin de contempler les risques liés à l'IA, nous allons nous référer au rapport annuel 2020 de Deloitte sur l'état de l'IA en entreprise. Ce rapport a sondé 2737 responsables informatiques et opérationnels d'octobre à décembre 2019 pour un total de neuf pays représentés. De plus, toutes les sociétés participantes avaient adopté des technologies basées sur l'IA (Ammanath, Novak, Anderson, & Kulkarni, 2020, p. 11). Ce rapport constitue donc une base solide pour parcourir les risques de l'IA.

Le rapport établit que plus de 75% des interviewés pensent que l'IA transformera substantiellement leur organisation dans les trois années à venir et presque 75% d'entre eux également rapportent que l'IA est stratégiquement importante. Cependant, cette tendance à la hausse de l'IA en entreprise est également plombée par un malaise croissant puisque 56% des répondants révèlent qu'ils planifient de ralentir ou ralentissent déjà les adoptions IA en raison des inquiétudes quant à l'émergence de risques (Ammanath *et al.*, 2020, p. 2).

Pour comprendre au mieux d'où proviennent ces appréhensions, les autres ont listé des inquiétudes qui devaient être évaluées de « minimale » à « extrême » par les répondants. À partir de là, les auteurs ont été en mesure d'identifier trois catégories de risques : 1) la confiance en l'IA ; 2) l'éthique ; et 3) les incertitudes de marché.

Confiance en l'IA. Ce premier risque traite du questionnement sur la fiabilité des outils IA, notamment sur la qualité des informations et décisions fournies par l'IA, la confiance dans la sécurité des systèmes et la capacité à comprendre, justifier ou expliquer le processus de décision de l'IA (Ammanath *et al.*, 2020, p. 3).

Éthique. Ce deuxième risque revêt des questionnements sur une utilisation de l'IA qui serait bonne ou mauvaise pour la société, notamment sur la confidentialité des données, l'équité, la partialité et le risque de perte d'emploi (Ammanath *et al.*, 2020, p. 3).

Incertitudes de marché. Ce troisième risque intervient sur des facteurs hors du contrôle direct d'une société, on voit donc ici les changements au niveau des réglementations, l'opinion publique et celle des employés (Ammanath *et al.*, 2020, p. 3).

Parmi ces trois catégorisations, on observe que le risque de confiance est le risque pour lequel les inquiétudes sont les plus élevées, et particulièrement les inquiétudes qualifiées d'extrêmes (voir figure 5).

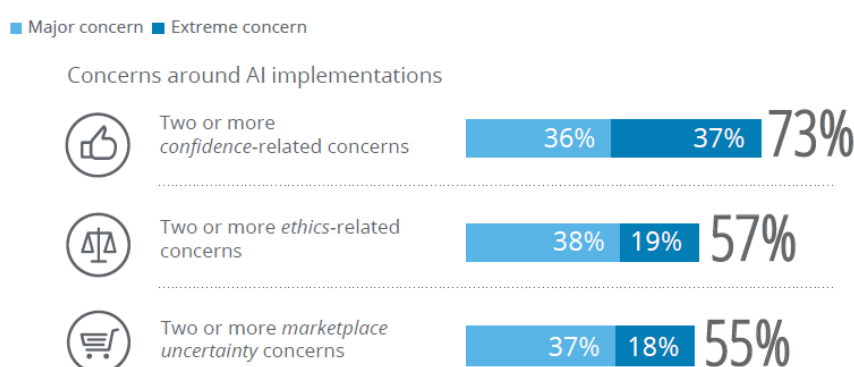


Figure 5 : Les trois catégories de risques de l'IA selon leur degré d'inquiétude en pourcentages

Source : Ammanath *et al.*, 2020, p. 3

Le rapport fournit également la répartition des risques les plus représentés pour chaque catégorie de risque (voir annexe 9 pour le détail, p. 142). Concernant la confiance en l'IA, le rapport a notamment identifié des risques liés à la vulnérabilité de la cybersécurité, aux défaillances de l'IA affectant les opérations commerciales, *etc.* Toujours au sujet de la

confiance, les auteurs ont également pointé un challenge afférant aux systèmes IA : le compromis entre interprétabilité et puissance (Ammanath *et al.*, 2020, p. 5). En effet, les outils IA sont parfois si complexes que même des scientifiques des données très qualifiés rencontrent des difficultés pour comprendre le processus de décision IA. Cependant, Ammanath *et al.* (2020, p. 5) rappellent que l'Explainable AI (XAI) aide à résoudre ce challenge puisque l'objectif de ce domaine de l'informatique en expansion est de chercher à créer des modèles d'IA qui sont plus aptes à s'expliquer d'eux-mêmes.

Au sujet de l'éthique, les auteurs rapportent que le risque le plus représenté est imputable aux données. Premièrement, en termes de confidentialité pour l'utilisation des données personnelles mais aussi en termes d'équité et biais. En effet, les données qui sont utilisées pour produire de l'output IA peuvent être au préalable incomplètes, biaisées ou inégales impliquant ainsi des biais involontaires, même pour une société bien intentionnée (Ammanath *et al.*, 2020, p. 6). De plus, si ce n'est pas la base de données qui est biaisée en entrée, les humains qui développent des solutions IA peuvent être la proie de préjugés involontaires. S'ils ne sont pas atténués, leurs solutions IA seraient à leur image, faites de préjugés et conduisant à des biais (Ammanath *et al.*, 2020, p. 6). C'est d'ailleurs ce qui a été vu dans le domaine des soins de santé lorsqu'un algorithme de prédiction du risque, utilisant les dépenses en soins de santé comme proxy pour les soins, a démontré un biais racial dans ses résultats. Les personnes de couleur blanche avaient de meilleures chances de profiter d'un programme de soins supplémentaire que les personnes de couleur noire. L'algorithme était à même d'établir des dépenses en soins de santé des deux groupes mais n'était pas capable d'évaluer les désavantages économiques auxquelles les personnes noires font face (Ammanath *et al.*, 2020, pp. 6-7).

Sous le couvert des incertitudes de marché, on retrouve principalement des challenges liés aux changements de régulations sur l'IA, à la confidentialité des données, à la reconnaissance faciale, aux potentielles réactions négatives des clients et aux perceptions négatives des employés lorsque de l'IA est utilisée (Ammanath *et al.*, 2020, p. 7).

Un autre point important dans la perception des risques de l'IA est le degré de maturité. Effectivement, le rapport montre que le niveau d'inquiétude pour les trois catégories de risque est plus faible et pour les sociétés débutantes (i.e. *starters*) et pour les sociétés expérimentées (i.e. *seasoned*) alors que les sociétés qualifiées (i.e. *skilled*) présentent des niveaux d'incertitude très élevés (voir figure 6).

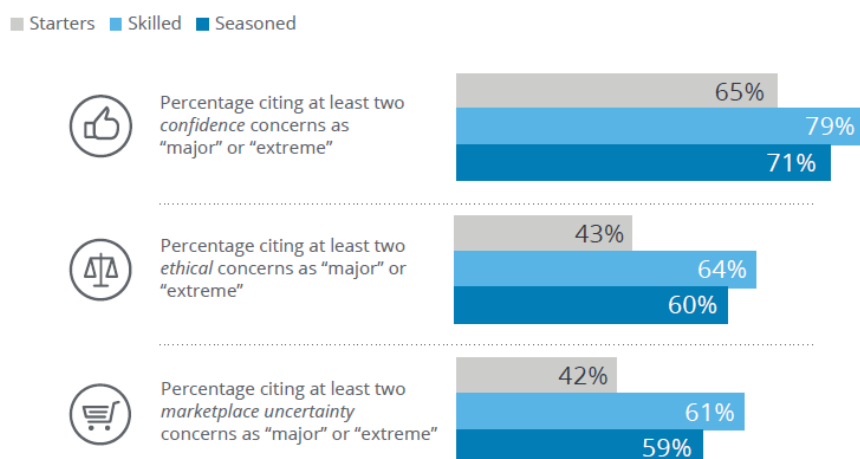


Figure 6 : La perception des risques selon le degré de maturité des solutions IA

Source : Ammanath *et al.*, 2020, p. 5

La logique sous-jacente à ces observations se comprend aisément. Au statut de débutantes, les entreprises n'ont pas encore pu évaluer toute l'étendue des risques associés à l'IA. Au niveau qualifié, les challenges deviennent apparents sans pour autant avoir développé les capacités pour les traiter. Finalement, au stade expérimenté, les entreprises ont appris à développer les capacités nécessaires pour traiter les risques, poussant ainsi le niveau d'incertitude à la baisse (Ammanath *et al.*, 2020, p. 5).

Section 2 : Robotic Process Automation

La RPA comprise seule est un domaine à part entière. Effectivement, l'automatisation peut revêtir un caractère intelligent si elle est associée à d'autres domaines de l'informatique comme le machine learning, le deep learning, *etc.* Seule, elle sert plutôt d'outils permettant d'automatiser en répliquant des comportements humains de base.

C'est pourquoi nous entendons souvent parler de « bots » ou robots. Ceux-ci ne sont pas toujours dotés d'intelligence mais sont d'une grande utilité lorsqu'il s'agit de réaliser des tâches répétitives à faible caractère intellectuel. Dans son livre, O'Regan retrace la naissance du terme « robot » et nous dit que la première utilisation du terme a été faite par un dramaturge tchèque, Karel Capek, dans son œuvre *Les Robots Universels de Rossum*. La pièce explore le caractère éthique d'exploiter des travailleurs artificiels et la réponse de ces robots à leur exploitation, d'où le fait que le terme robot est dévié du mot tchèque signifiant travail forcé (O'Regan, 2016, p. 267).

Sous-section 2.1 : Définitions

Une définition largement acceptée d'un robot a été proposée en 1979 par la Robotic Institute of America : « *a robot is a reprogrammable multifunctional manipulator designed to move material, parts, tools, or specialized devices through variable programmed motions for the performance of a variety of tasks.* » (Hunt, 1983, p. 7).

En allant un peu plus loin, nous pouvons jeter un œil à la définition de la Robotic Process Automation avec Christopher *et al.* (2019, p. 7) qui relatent que la RPA permet aux organisations de configurer un logiciel informatique ou un « bot » pour capturer et interpréter des applications existantes pour traiter une transaction, manipuler des données, déclencher des réponses et communiquer avec d'autres systèmes numériques.

Sous-section 2.2 : Les lois de la robotique

Dans les années 40, Asimov a créé un ensemble de lois pour un comportement adéquat des robots. Elles sont connues aujourd'hui comme les Trois lois de la robotique bien qu'Asimov ait ajouté une quatrième loi par la suite.

Loi Zéro. Un robot ne peut pas faire de mal à l'humanité, ni, par son inaction, permettre que l'humanité soit blessée.

Première Loi. Un robot ne peut porter atteinte à un être humain, ni, restant passif, permettre qu'un être humain soit exposé au danger, sauf contradiction avec la Loi Zéro.

Deuxième Loi. Un robot doit obéir aux ordres que lui donne un être humain, sauf si de tels ordres entrent en conflit avec la Première Loi ou la Loi Zéro.

Troisième Loi. Un robot doit protéger son existence tant que cette protection n'entre pas en conflit avec la Première ou la Deuxième Loi ou la Loi Zéro.

Sous-section 2.3 : Perspectives RPA pour la fonction finance et dans le secteur bancaire

La fonction finance des organisations est en voie de modernisation. En effet, grâce aux possibilités d'automatisation de plus en plus étendues, cette fonction se voit remodelée pour réduire les coûts et augmenter l'efficacité. Une analyse McKinsey a d'ailleurs montré que 27% des activités financières pourraient être automatisées en utilisant les technologies déjà disponibles (voir figure 7). D'ailleurs, parmi ces automatisations, un tiers pourrait être réalisées

via des technologies basiques comme la RPA qui peut se greffer facilement sur les solutions IT existantes (Edlich, Ip, & Whiteman, 2018, p. 3).

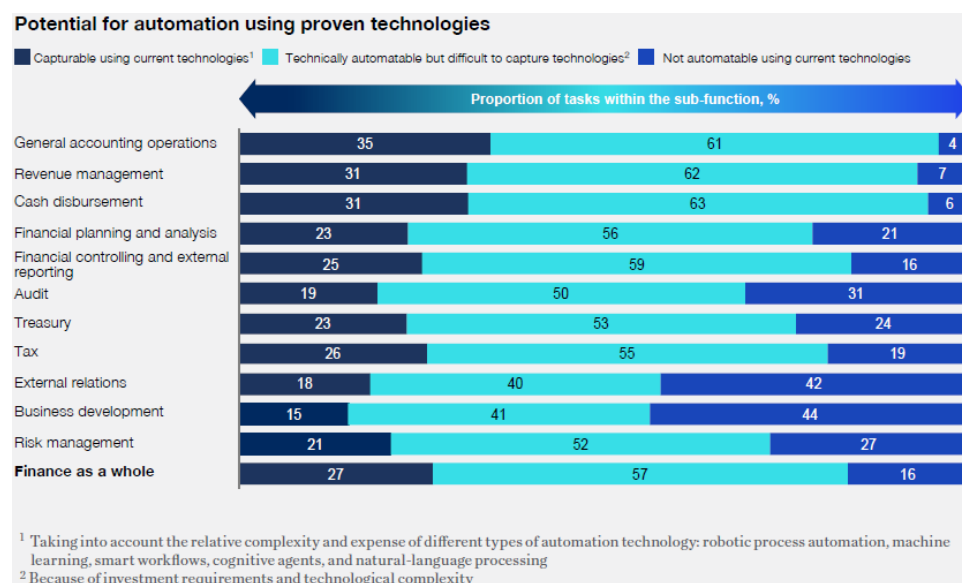


Figure 7 : Le degré d'automatisation des activités financières

Source : Edlich *et al.*, 2018, p. 3

Dans le secteur bancaire, Taulli (2020, p. 94) a identifié huit zones spécifiques où la RPA pourrait être d'une grande aide. Ces huit sphères peuvent être complétées de six autres identifiées par Gogineni (2019) :

1. Traitement des prêts
2. Ouverture de compte
3. Fermeture de compte
4. Traitement des transactions
5. Gestion des risques
6. Approbations
7. Confirmations
8. Détection de fraudes
9. Service client
10. Gestion des fournisseurs
11. Traitement des cartes de crédit
12. Processus KYC⁵

⁵ Know Your Customer est le processus permettant de vérifier l'identité des clients d'une entreprise afin de combattre la fraude, la corruption, le blanchiment d'argent et le financement du terrorisme.

13. Gestion du grand-livre⁶

14. Automatisation des rapports

Plus concrètement, nous pouvons déjà citer quelques exemples d'applications RPA dans le secteur bancaire.

Par exemple, la British Bank faisait face à un problème : le temps de traitement moyen par transaction était trop long, environ 30 minutes. Ils ont alors décidé d'implémenter un outil RPA dans le but de réduire ce laps de temps. Pour ce faire, ils ont engagé un développeur spécialisé en robotique pour programmer un robot et mettre en place un nouveau processus. Il s'en est suivi un temps de traitement par transaction réduit à seulement 10 minutes et une augmentation drastique du ROI⁷ durant les six premiers mois (Valgaeren, 2019, p. 8).

La Deutsche Bank a également emboité le pas vers plus d'automatisations grâce à la RPA. Leur objectif est de gérer plus efficacement les tâches répétitives. Ils ont d'ailleurs rapporté 30 à 70% d'automatisations dans les domaines où des logiciels RPA ont été intégrés (Wilds, 2018). Dans son rapport annuel 2017, la Deutsche Bank mentionne d'ailleurs :

We are modernizing our IT and pursuing the digitalization of our business. Today, our private clients can open an account online in a matter of minutes – and not seven days as before. Our mobile services are leaders in the German market. We have launched robo-advisers (WISE) in the asset management business and in the Private & Commercial Bank (ROBIN). WISE and ROBIN use algorithms to compile a suitable portfolio for our clients. In our other businesses, too, we are utilizing robotics and artificial intelligence to automate what were previously manual processes – this will minimize errors and lower costs. (Deutsche Bank Annual Report 2017, p. 5)

Un autre exemple est la SunTrust Bank qui a formé une équipe au sein de son département IT spécialisée dans le déploiement de technologies RPA. Les résultats des utilisations robotiques ont montré une accélération de la vitesse moyenne de transaction de 3,8, un temps de formation moyen amélioré par 4 et un taux d'erreur moyen réduit de 65% (Wilds, 2018).

⁶ Notion comptable : « le grand-livre regroupe l'ensemble des comptes d'une entité. Il reprend donc les écritures comptables du livre-journal ou des livres auxiliaires, mais ventilées par compte. Il est utilisé pour classer et récapituler les opérations et pour préparer les états financiers » (Cerrada, De Rongé, De Wolf, & Gatz., 2011, p. 49)

⁷ Return on investment

Conclusion

Au travers de cette première partie, nous avons parcouru ce que sont l'intelligence artificielle et la robotic process automation. L'intelligence artificielle n'a pas de définition exacte à ce jour, c'est pourquoi nous en avons proposé plusieurs et que nous avons abordé l'IA en termes de capacités.

Les capacités de l'IA ont permis d'étudier l'étendue du domaine mais seulement en partie étant donné que personne ne s'accorde sur une définition, il est inadéquat de parler d'exhaustivité. Les perspectives de l'IA au niveau global et dans le secteur bancaire ont suivi.

Ensuite, nous nous sommes exprimés sur les critiques, les aspects éthiques et les risques de l'IA. La critique majeure revient à Searle et son expérience de la chambre chinoise qui en effet pose question sur l'existence d'une IA forte. Cependant, ce point de vue ne fait pas l'unanimité auprès des scientifiques. L'éthique est évidemment un aspect crucial dans le développement de l'IA. Celle-ci nécessite une connaissance approfondie des experts pour pouvoir maîtriser les dangers de l'IA comme le rappelait Hawking en 2017.

Nous avons également passé en revue les risques de l'IA à l'aide du rapport de Deloitte sur l'état de l'IA en entreprise. Les trois catégories de risques principales sont la confiance en l'IA, l'éthique et les incertitudes de marché.

Finalement, nous avons défini ce qu'est la RPA ainsi que les lois de la robotique. Au nombre de quatre, ces lois devraient permettre à tout robot d'adopter un comportement adéquat. La section RPA a également permis d'évaluer les perspectives pour la fonction finance et le secteur bancaire avec l'identification des zones d'intérêt pour la RPA et des exemples d'application à la British Bank, la Deutsche Bank et la SunTrust Bank.

Pour faire court, la principale distinction entre IA et RPA réside dans la composante intelligente de l'un, absente chez l'autre. En effet, l'IA aurait la capacité d'apprendre et de répliquer des comportements humains intelligents là où la RPA ne serait seulement capable de répliquer des tâches non-intelligentes, sans possibilité d'apprentissage.

PARTIE 2 : LA TAXONOMIE DES RISQUES

Introduction

Dans cette deuxième partie, nous allons progressivement aborder la gestion des risques et son fonctionnement. Ensuite, nous nous attaquerons aux types de risque ce qui permettra de mettre en avant la taxonomie des risques. Nous verrons également comment une banque gère ces risques en pratique. Finalement, nous parcourrons les risques qui seront mis à l'étude et à l'analyse au travers de ce mémoire et les motivations qui ont mené au choix de ces risques. Nous concluons en fournissant les principaux éléments de chacune des sections qui suivent.

Section 1 : Gestion des risques

Sous-section 1.1 : Définition, dimensions, objectifs et cycle

Définition

La gestion des risques est la capacité d'une entité à prendre des décisions et à implémenter des activités conduisant à atteindre un niveau de risque acceptable, appelé appétit pour le risque (Meshkova, Wawrzyniak, & Wójcik-Mazur, 2018, p. 30). Nous reviendrons sur cette notion d'appétit du risque ci-après. Suivant cette définition, il faut bien comprendre que la gestion des risques n'a pas pour but d'empêcher de prendre des risques mais plutôt d'être capable de comprendre et de gérer les risques de telle façon à ce que des rendements optimaux soient atteints (Olieslagers, 2019). L'attitude envers le risque est donc ambivalente puisqu'elle vise à trouver la meilleure évaluation et le meilleur ajustement entre dangers et opportunités. En ce sens, la gestion des risques est de plus en plus appréhendée comme un avantage concurrentiel dans la mesure où une gestion saine conduira à sélectionner le meilleur arbitrage entre menaces et opportunités et donc à se démarquer des concurrents (Henrard, 2020 ; Bessis, 2011).

Dimensions

On octroie à la gestion des risques deux dimensions principales, deux axes : probabilité et impact. L'axe probabilité revient à se poser la question suivante : « Quelle est la probabilité pour un risque de se matérialiser en une perte ? ». L'axe impact revient à questionner ceci : « Quelle pourrait être l'importance de l'impact ? » (Olieslagers, 2019). Ces deux dimensions déterminent alors l'importance de la menace perçue du risque et si une mesure est prise pour empêcher un risque de se transformer en perte.

Objectifs

Suivant les deux dimensions mentionnées, l'objectif principal de la gestion des risques est de réduire la probabilité d'occurrence en mettant en place des actions précautionneuses et/ou de réduire et évaluer son impact en cas d'occurrence (Türsoy, 2018, p. 4 ; Olieslagers, 2019). Un autre objectif est l'évaluation des réponses réglementaires et non réglementaires aux risques (Olieslagers, 2019).

Plus généralement, la gestion des risques permet donc d'identifier, analyser, atténuer et surveiller les principaux risques tout en protégeant et en créant de la valeur pour toutes les parties prenantes (Olieslagers, 2019). Il existe sept parties prenantes clés : les clients, les actionnaires, les autres banques, le personnel, les détenteurs de dépôts, les régulateurs (banques centrales et superviseurs) et le gouvernement.

Cycle

Plusieurs cycles de gestion des risques existent aujourd'hui et diffèrent dans une moindre mesure (Olsson, 2007, p. 745). Cependant, ils s'accordent tous sur quelques composantes, notamment l'identification, l'évaluation et la mesure, et l'atténuation des risques. Pour aller plus loin, on peut ajouter une quatrième composante : suivre et signaler les risques (Culp, 2002, p. 211).

Identification. L'identification du risque est « *the process by which a company recognizes and, in some cases, detects the different financial risks to which it is exposed through the normal course of conducting its business* » (Culp, 2002, p. 210).

Évaluation et mesure. Cette composante consiste à quantifier les expositions aux risques en comparaison avec les tolérances de risques définies par l'entreprise. Ce processus de quantification est critique pour la gestion des risques puisque, sans bonne mesure, la difficulté pour déterminer la substantialité du risque empêche l'entreprise d'évaluer si un niveau sain de risque est pris (Culp, 2002, p. 211).

Atténuation. Il convient ici de mettre en place un plan d'actions correctives favorisant une amélioration de l'environnement de contrôle. En d'autres mots, il s'agit de transférer le risque en l'assurant ou d'abandonner l'activité si le risque ne peut être assuré (Olieslagers, 2019).

Suivi et signalement. Le suivi s'opère via des tableaux de bord adéquats offrant une vue d'ensemble de l'exposition aux risques (Olieslagers, 2019). Ceci s'effectue à l'aide de l'approche par les indicateurs de base, ou « key risk indicators » (Pierandrei, 2019, p. 238).

Le cycle de gestion des risques gravite autour de quatre éléments déterminants (voir figure 8) : la gouvernance, les personnes, les processus et la technologie.

Gouvernance. Ce premier élément implique que la tolérance pour le risque et la culture d'entreprise soit alignée sur la stratégie, les rôles et les responsabilités (Olieslagers, 2019).

Personnes. Les personnes impliquées dans le processus de gestion du risque doivent englober la direction et les fonctions de risque en charge tout en gardant une propriété du risque au niveau des business units (Olieslagers, 2019).

Processus. Toutes les procédures et les politiques doivent être claires et correctement documentées (Olieslagers, 2019).

Technologie. Il y a ici nécessité d'utiliser des outils adéquats et proportionnels à la complexité et à la taille de l'organisation (Olieslagers, 2019).

Le cycle de gestion des risques est un processus itératif pour trois raisons. Premièrement, au plus tôt un risque est identifié, au plus tôt des plans d'action peuvent être mis en place pour corriger le tir et gérer les risques. Deuxièmement, les risques et le nombre de risques évoluent à travers le temps, notamment parce que les standards financiers européens évoluent également et deviennent généralement plus restrictifs. Troisièmement, les mises en œuvre technologiques et méthodologiques doivent être réévaluées de telle façon à implémenter les innovations bénéfiques à l'amélioration du processus de gestion des risques. Appliquer ce processus itératif correctement conduit à améliorer l'organisation en fournissant à la direction de meilleures connaissances sur les risques et leur impact (Olieslagers, 2019).

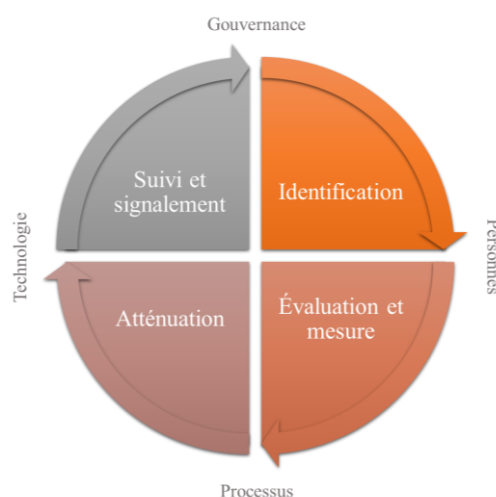


Figure 8 : Le cycle de la gestion des risques

Source : Adapté de Principles of banking and finance (Olieslagers, 2019) (complètement référencé en bibliographie)

Sous-section 1.2 : Mesures de risque

Cette section va détailler les mesures de risque. Il convient de mentionner que nous visons uniquement à couvrir les principales méthodes et mesures et à fournir un aperçu de celles-ci.

Tout d'abord, il faut évoquer qu'il existe deux méthodes pour mesurer le risque : une évaluation qualitative et une évaluation quantitative (Sghaier, Hergon, & Desroches, 2015, p. 160). La méthode qualitative implique de donner une appréciation. On cherchera donc à déterminer qualitativement quelles occurrences sont possibles. Pour ce faire, l'impact et la probabilité sont donc évalués de manière verbale en utilisant des termes comme très faible, faible, moyenne ou forte probabilité (Sghaier *et al.*, 2015, p. 161). Cette méthode est pratique pour évaluer les niveaux de risque quand on compare plusieurs alternatives ou que la disponibilité des données est insuffisante et ne permet pas d'évaluation numérique (Sghaier *et al.*, 2015, p. 161 ; Olieslagers, 2019), ou encore lorsque les connaissances sont peu formalisées (Sghaier *et al.*, 2015, p. 161). La méthode quantitative permet de quantifier numériquement la probabilité ou l'impact d'un risque en se basant sur les données historiques. Plusieurs outils quantitatifs existent mais l'outil le plus utilisé est la Value at Risk ou VaR (Olieslagers, 2019). Nous allons ci-après détailler quelques outils quantitatifs.

Avant d'entrer dans le vif du sujet, deux considérations doivent être posées. Il faut préciser que la VaR et l'expected shortfall sont des mesures qui ne s'appliquent pas à tous les risques de la taxonomie qui sera abordée dans la section suivante. Principalement, elles permettent de

calculer le risque de marché. Une autre considération survient lorsque l'on discute de ces mesures : il est parfois entendu les termes « credit VaR » ou « operational VaR ». En fait, ces termes font référence à d'autres méthodologies que celles que nous allons détailler.

Value at Risk

Comme nous l'avons dit précédemment, la Value at Risk « *has been the most frequently used modelling technique that typically measures a bank's aggregate market risk exposure and, given a probability level, estimates the amount a bank would lose if it were to hold specific assets for a certain period of time* » (van Greuning & Bratanovic, 2020, p. 252).

La VaR est une méthode anticipative dans la mesure où le risque est exprimé sous une forme compréhensible par tous, à savoir la monnaie (van Greuning & Bratanovic, 2020, p. 253). Elle mesure la perte maximale qu'un portefeuille subira sur une période donnée dans un niveau de confiance donné dans des conditions normales du marché (van Greuning & Bratanovic, 2020, p. 253 ; Olieslagers, 2019).

Pour mieux comprendre le concept de VaR, nous pouvons utiliser un petit exemple. Considérons un portefeuille de titres d'une valeur de 100 millions d'euros et un intervalle de confiance à 95% sur une période d'un mois. Si on se trouve hors de l'intervalle de confiance, la perte subie sera de 2%. Quelle est la perte mensuelle maximale encourue ?

La perte mensuelle maximale encourue est de $VaR = 100M€ * 2\%$, c'est-à-dire 2 millions d'euros. Autrement dit, il y a 95% de chances de ne pas perdre plus de 2 millions d'euros sur le mois mais 5% de chances de perdre plus de 2 millions d'euros le mois d'après.

Les modèles basés sur la VaR comparent donc la variation potentielle de la valeur de chaque position qui découlerait des mouvements des facteurs de risque sous-jacents avec la probabilité que ces mouvements se produisent (van Greuning & Bratanovic, 2020, p. 253).

La VaR est généralement calculée selon quatre méthodologies : simulation historique, variance/covariance, les simulations de Monte Carlo, et l'approche par les copules.

Simulation historique. Cette méthode calcule le changement de valeur hypothétique du portefeuille actuel en se basant sur les mouvements historiques des facteurs de risque (van Greuning & Bratanovic, 2020, p. 253).

Variance/covariance. Cette méthode suppose que les rendements des actifs du portefeuille suivent une distribution normale. Il ne faut donc calculer que deux facteurs : la moyenne et l'écart-type des actifs. Ceci permet ensuite de tracer une courbe de distribution normale (Harper, 2020). La VaR est obtenue en multipliant l'écart-type par un multiplicateur qui lui dépend de l'intervalle de confiance choisi (Olieslagers, 2019).

Simulations de Monte Carlo. Cette troisième méthode consiste à développer des scénarios de prix pour les facteurs de risque et à exécuter ces scénarios à travers un modèle stochastique (Harper, 2020). Chaque scénario fournira une distribution du portefeuille et chaque distribution sera différente. C'est ce qui fait toute la flexibilité de cette méthode puisqu'elle permet de générer des tas de valeurs de portefeuille différentes selon les trajectoires simulées des facteurs de risque, c'est-à-dire les scénarios (Olieslagers, 2019).

Approche par les copules. Les copules permettent de générer des distributions multivariées en identifiant la structure de dépendance des rendements des actifs d'un portefeuille tout en permettant de nombreuses distributions marginales différentes. Selon cette méthodologie, il est alors possible d'identifier les copules pour lesquels la performance de la VaR est la plus élevée (Byun & Song, 2021, p. 59).

Pour aller un peu plus loin sur le concept de VaR, nous pouvons parler de la comonotonie. En effet, il est souvent nécessaire de calculer la fonction de distribution d'un portefeuille constitué de variables aléatoires, où les distributions marginales de chaque actif sont connues mais leur structure de dépendance est trop compliquée à travailler. À cette fin, la comonotonie est une forme de dépendance positive qui peut être utilisée pour déterminer de manière facile et précise les bornes supérieure et inférieure de la distribution et donc de préciser les mesures de risque (Dhaene, Vanduffel, & Goovaerts, 2008).

Dans la pratique, imaginons un portefeuille constitué de deux variables aléatoires. Si ces variables sont comonotones, cela signifie qu'elles sont parfaitement dépendantes positivement. On parle d'additivité en termes mathématiques, que l'on peut comprendre comme le principe de diversification, souvent utilisé dans le domaine de la gestion de portefeuille. Donc, un portefeuille constitué de deux variables aléatoires comonotones et donc additives n'apportera pas d'avantage en termes de diversification et impliquera un montant de capital-risque requis correspondant à la somme des exigences de capital individuelles (Koch-Medina & Munari, 2021, p. 2). Lorsque l'on exige que les variables soient sous-additives, la somme des

exigences en capital individuelles constitue toujours une limite supérieure pour l'exigence en capital d'une position diversifiée (Koch-Medina & Munari, 2021, p. 2).

Expected shortfall

Un autre outil d'évaluation quantitative est l'expected shortfall ou ES. L'ES est une méthode de mesure du risque plus conservatrice et une alternative (Meshkova *et al.*, 2018, p. 70), voire la mesure successive à la VaR (van Greuning & Bratanovic, 2020, p. 252). L'ES quantifie l'importance du risque de queue d'un portefeuille (Chen & Scott, 2020), c'est-à-dire qu'elle évalue la moyenne des pertes extrêmes potentielles au-delà du niveau de confiance de la VaR. Par exemple, si le niveau de confiance donné est de 97,5%, l'expected shortfall va calculer la moyenne des 2,5% de pertes les plus importantes (van Greuning & Bratanovic, 2020, pp. 254-255). En ce sens, l'ES surpasse la VaR puisqu'elle permet de capturer le risque de pertes extrêmes (voir figure 9). À savoir que la figure ci-dessous montre une courbe de Gauss mais, en réalité, la distribution au-delà du niveau de confiance défini n'est pas connue et peut donc prendre d'autres formes.

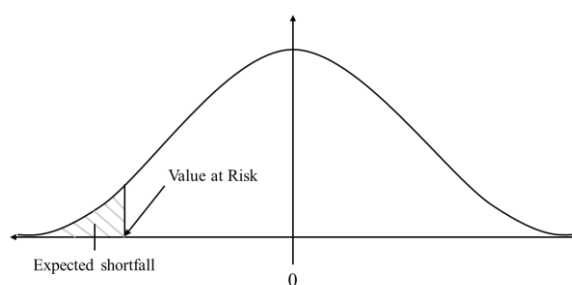


Figure 9 : Illustration de l'expected shortfall

Source : Contribution personnelle de l'auteur

Stress testing

Le stress testing implique d'évaluer comment un objet ou un système se comporte quand on le met sous pression. Dans le secteur bancaire, les stress tests sont conçus pour tester la résilience des banques à des chocs sévères mais plausibles (Dent, Westwood, & Segoviano, 2016, p. 131). Il convient donc de modéliser l'impact d'hypothétiques scénarios défavorables au niveau macroéconomique et financier sur la rentabilité et les bilans de la banque (Dent *et al.*, 2016, p. 131).

L'objectif des stress tests est donc d'identifier les événements et facteurs susceptibles d'occasionner une perte et d'impacter négativement la position de la banque en se focalisant sur l'ensemble des paramètres qui pourraient générer des pertes exceptionnelles (van Greuning & Bratanovic, 2020, p. 258). Les stress tests doivent inclure des critères quantitatifs (e.g. : scénarios plausibles sur les facteurs de risque dans l'environnement de la banque) et qualitatifs (e.g. : évaluation de la capacité de la banque à absorber des pertes inattendues, identification des mesures en vue de réduire le risque une fois qu'il est avéré) (van Greuning & Bratanovic, 2020, p. 258).

Le Basel Committee on Banking Supervision (BCBS)⁸ a développé les principes du stress testing dans le but de « *address key weaknesses in stress testing practices that were highlighted by the global financial crisis* » (BCBS, 2018, p. 1). Ces principes ont été émis en 2009 et ont été révisés en 2018 pour prendre en considération l'évolution du rôle du stress testing et son caractère critique pour la gestion des risques tant pour les banques que pour les superviseurs bancaires et les autorités macroprudentielles (BCBS, 2018, p. 1). Ces principes sont les suivants (BCBS, 2018, pp. 3-11) :

- Les cadres de stress testing doivent avoir des objectifs clairement formulés et formellement adoptés ;
- Les cadres de stress testing doivent prévoir une structure de gouvernance efficace ;
- Les stress tests doivent être utilisés comme un outil de gestion des risques et contribuer à la prise de décisions business ;
- Les cadres de stress testing doivent prendre en compte les risques significatifs et pertinents et appliquer des pressions suffisamment fortes ;
- Les ressources et les structures organisationnelles doivent être adéquates pour atteindre les objectifs du cadre de stress testing ;
- Les stress tests doivent s'appuyer sur des données précises et suffisamment granulaires et sur des systèmes informatiques robustes ;

⁸ Basel Committee on Banking Supervision : « *is the primary global standard setter for the prudential regulation of banks and provides a forum for regular cooperation on banking supervisory matters. Its 45 members comprise central banks and bank supervisors from 28 jurisdictions.* » (<https://www.bis.org/bcbs/>)

- Les modèles et les méthodologies permettant d'évaluer l'impact des scénarios et des sensibilités doivent être adaptés aux besoins ;
- Les modèles, résultats et cadres de stress testing doivent faire l'objet d'une remise en question et d'un examen régulier ;
- Les pratiques et les résultats du stress testing doivent être communiqués au sein des juridictions et entre juridictions.

Sous-section 1.3 : Appétit pour le risque

En 2011, le FSB⁹ remarquait que des cadres d'appétit pour le risque (« Risk Appetite Frameworks » ou RAF) efficaces, exploitables et mesurables n'étaient pas complètement adoptés par les institutions financières et que le développement d'un cadre effectif était nécessaire (FSB, 2013, p. 1).

Ce cadre d'appétit pour le risque possède plusieurs objectifs selon les Principles For An Effective Risk Appetite Framework du FSB. Ce cadre effectif doit être spécifique à une institution et refléter son business model et son organisation. Également, il devrait permettre aux institutions financières de s'adapter aux changements économiques et réglementaires. Un autre objectif est de renforcer la culture du risque dans les institutions financières puisqu'elle est cruciale pour une gestion des risques saine. En retour, une solide culture du risque créerait un environnement propice à la reconnaissance, à la remontée et à la prise en charge en temps utile des risques émergents (FSB, 2013, pp. 1-2).

Dans le but de favoriser une nomenclature commune entre les superviseurs et les institutions financières, les Principles For An Effective Risk Appetite Framework définissent le risk appetite framework, le risk appetite statement, et le risk appetite.

Risk appetite framework (RAF). « *The overall approach, including policies, processes, controls, and systems through which risk appetite is established, communicated, and monitored. It includes a risk appetite statement, risk limits, and an outline of the roles and responsibilities of those overseeing the implementation and monitoring of the RAF. The RAF should consider material risks to the financial institution, as well as to the institution's reputation vis-à-vis*

⁹ Financial Stability Board : « *is an international body that monitors and makes recommendations about the global financial system.* » (<https://www.fsb.org/about/>)

policyholders, depositors, investors and customers. The RAF aligns with the institution's strategy. (FSB, 2013, p. 2).

Risk appetite statement. « The articulation in written form of the aggregate level and types of risk that a financial institution is willing to accept, or to avoid, in order to achieve its business objectives. It includes qualitative statements as well as quantitative measures expressed relative to earnings, capital, risk measures, liquidity and other relevant measures as appropriate. It should also address more difficult to quantify risks such as reputation and conduct risks as well as money laundering and unethical practices. » (FSB, 2013, p. 2).

Risk appetite. « The aggregate level and types of risk a financial institution is willing to assume within its risk capacity to achieve its strategic objectives and business plan. » (FSB, 2013, p. 3).

Afin d'évaluer l'appétit pour le risque, l'EBA¹⁰ publie trimestriellement son Risk Dashboard. Le Risk Dashboard de l'EBA « is part of the regular risk assessment conducted by the EBA and complements the Risk Assessment Report. » (EBA, 2021). L'objectif de ce dashboard est de résumer les principaux risques et vulnérabilités du secteur bancaire dans l'Union Européenne en se concentrant sur l'évolution des indicateurs de risque. L'EBA propose donc chaque trimestre une évaluation des métriques principales. En se basant sur le rapport du Q1 2021 (voir annexe 10, p. 143), on peut en sortir une carte thermique classée par catégories clés de risque avec leurs métriques associées (voir figure 10).

	Risk Incators	Thresholds		
Solvency	Tier 1 capital ratio	> 15%	[12% - 15%]	< 12%
	CET1 ratio	> 14%	[11% - 14%]	< 11%
	Leverage ratio	> 8%	[5% - 8%]	< 5%
Credit Risk & Asset Quality	Ratio of non-performing loans and advances (NPL ratio)	< 3%	[3% - 8%]	> 8%
	Coverage ratio of non-performing loans and advances	> 55%	[40% - 55%]	< 40%
	Forbearance ratio for loans and advances	< 1.5%	[1.5% - 4%]	> 4%
Profitability	Return on equity	> 10%	[6% - 10%]	< 6%
	Cost to income ratio	< 50%	[50% - 60%]	> 60%
Funding & Liquidity	Loan-to-deposit ratio for households and non-financial corporations	< 100%	[100% - 150%]	> 150%

Figure 10 : Le benchmarking de l'EBA des principaux indicateurs de risque

Source : Adapté de Risk Dashboard – Data as of Q1 2021 (EBA, 2021) (complètement référencé en bibliographie)

¹⁰ European Banking Authority : « is an independent EU Authority which works to ensure effective and consistent prudential regulation and supervision across the European banking sector. Its overall objectives are to maintain financial stability in the EU and to safeguard the integrity, efficiency and orderly functioning of the banking sector. » (<https://www.eba.europa.eu/about-us/eba-at-a-glance>)

Section 2 : Les types de risques

C'est précisément dans cette section que nous allons aborder la taxonomie des risques. Une taxonomie des risques est en fait une catégorisation compréhensible, commune et relativement stable des types de risque dans une organisation (Gouvernement du Canada, 2016). Dans le cadre de ce mémoire, on se réfèrera plutôt à la taxonomie des risques dans le secteur bancaire (et non simplement à une organisation) même si une taxonomie des risques doit être adaptée à une organisation pour être complètement alignée avec les besoins spécifiques. Elle est généralement représentée sous forme d'arbre où les risques plus élevés dans la hiérarchie sont décomposés en sous risques (voir figure 11). La taxonomie des risques comporte donc cinq grandes catégories qui elles-mêmes sont constituées de sous-risques. Nous faisons le choix dans cette section de parcourir en détail les catégories de risque et non pas les sous-risques qui leur sont associées parce qu'ils sont généralement des extensions spécifiques de leur catégorie respective qui ne nécessitent pas d'être couvertes dans leurs intégralités (cependant, l'annexe 11 fournit un détail pour chacun des risques et sous-risques de la taxonomie, p. 144). Ceci fait exception de la catégorie « autres risques » et du risque réputationnel étant donné que ces risques ont tendance à avoir une portée plus globale, c'est-à-dire un impact qui peut être diffus sur les autres catégories de risque. Les risques émergents, de plus en plus à considérer dans la taxonomie des risques, seront également mentionnés.

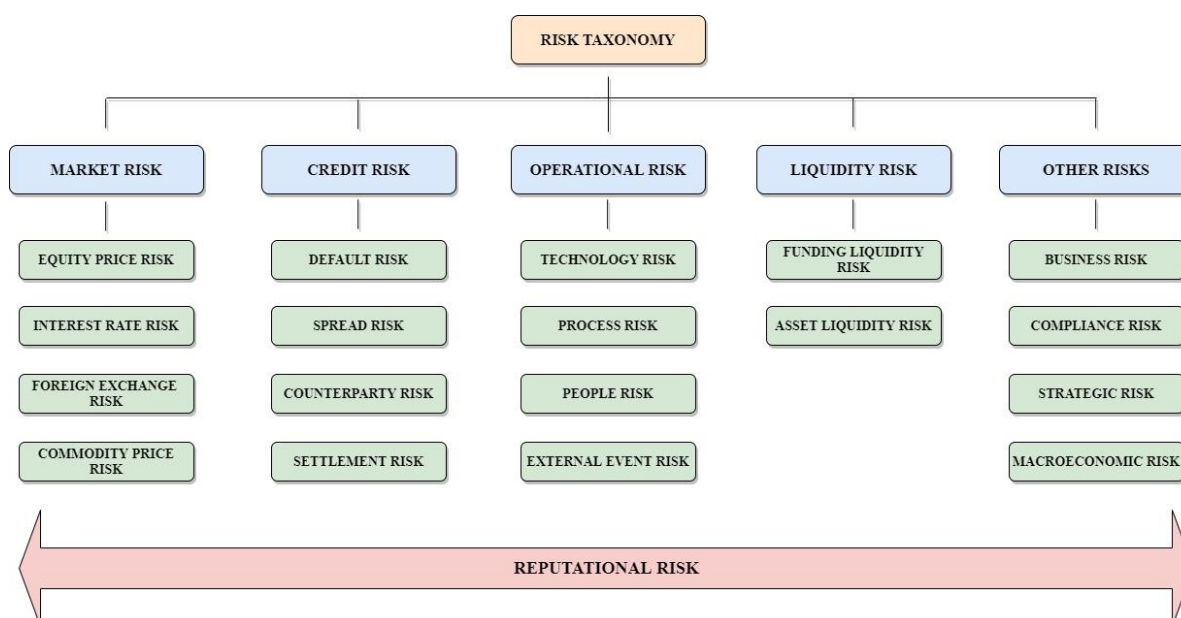


Figure 11 : La taxonomie des risques dans le secteur bancaire : catégories et sous-risques

Source : Contribution personnelle de l'auteur

Sous-section 3.1 : Risque de marché (« market risk »)

Le BCBS (2019, p. 1) définit le risque de marché comme étant le risque de pertes à la suite des changements de prix d'instruments financiers comme les obligations, les actions ou les monnaies. Les composantes principales du risque de marché sont : le prix des produits de base, le prix des actions, le taux d'intérêt, le taux de change, et le crédit spread (BCBS, 2019, p. 1).

Sous-section 3.2 : Risque de crédit (« credit risk »)

Le risque de crédit est l'éventualité qu'un emprunteur ou une contrepartie bancaire ne parviendra pas à remplir ses obligations conformément aux conditions convenues (BCBS, 2000, p. 1). L'objectif de la gestion du risque de crédit est de maximiser le taux de rendement ajusté au risque d'une banque en maintenant l'exposition au risque de crédit à un niveau acceptable (BCBS, 2000, p. 1). Les sous-risques liés au risque de crédit sont le risque de défaut, le risque de spread, le risque de contrepartie et le risque de règlement de transaction (Olieslagers, 2019).

Sous-section 3.3 : Risque opérationnel (« operational risk »)

Le BCBS (2011, p. 3) définit le risque opérationnel comme étant le risque d'occasionner des pertes découlant d'une gestion inadéquate ou défailante des processus internes, des personnes, des systèmes ou d'événement externes. Ce risque a une présence plurielle dans le secteur bancaire : produits, activités, processus, systèmes. C'est pourquoi une gestion saine de ce risque passe par une efficacité du comité de direction et du senior management dans l'administration des éléments où le risque opérationnel est présent (BCBS, 2011, p. 3). Il est à noter que, contrairement aux risques de marché, crédit et liquidité, cette catégorie de risque n'inclut que des risques non-financiers en soi, même si leurs impacts peuvent se transformer en perte financière.

Sous-section 3.4 : Risque de liquidité (« liquidity risk »)

La définition proposée dans les Principles for Sound Liquidity Risk Management and Supervision (BCBS, 2008, p. 1) indique que le risque de liquidité est la capacité d'une banque à financer l'augmentation de ses actifs et à faire face à ses obligations lorsqu'elles arrivent à échéance, sans subir de pertes inacceptables. L'incapacité à convertir un titre ou un actif illiquide en espèces sans perte de capital ou revenu est généralement la cause du risque de liquidité (Lessambo, 2020, p. 161).

Sous-section 3.5 : Autres risques

Cette section va s'attaquer à détailler les autres risques de la taxonomie des risques sur le secteur bancaire. Ces risques ont généralement une portée plus globale que les sous-risques des catégories précédentes, c'est-à-dire que leur impact sera généralement étendu à plusieurs catégories de la taxonomie.

Risque commercial ou business risk

Le risque commercial est le risque de perte lié à des changements inattendus de l'environnement compétitif ou à des tendances qui nuisent à la franchise et/ou à l'économie d'exploitation de l'entreprise (Lam, 2014, p. 246).

Risque de conformité ou compliance risk

Le risque de conformité est le risque auquel une organisation s'expose lorsqu'elle se trouve dans l'incapacité de répondre à ses obligations, c'est-à-dire aux réglementations, règles de conformité et standards propres à l'organisation, aux lois et au code de conduite applicable aux activités bancaires (BCBS, 2005, p. 7). Auquel cas, les retombées sur l'organisation peuvent être financières (ex : sanctions réglementaires, pertes financières substantielles), organisationnelles ou encore réputationnelles (BCBS, 2005, p. 7).

Risque stratégique ou strategic risk

Le risque stratégique est le risque associé à la sélection initiale, exécution ou modification dans le temps d'une stratégie sans pour autant que cette stratégie atteigne ses objectifs globaux (Chapman, 2011).

Risque macroéconomique ou macroeconomic risk

La Global Risk Institute (2021) définit le risque macroéconomique comme le comportement des industries et des gouvernements et des relations entre eux résultant des politiques monétaire et fiscale, des flux commerciaux et d'investissement et des développements politiques nationaux et internationaux, ainsi que les effets de ces facteurs sur les portefeuilles financiers et les valorisations des entreprises.

Sous-section 3.6 : Risque de réputation (« reputational risk »)

Le risque de réputation est « *the risk arising from negative perception on the part of customers, counterparties, shareholders, investors or regulators that can adversely affect a bank's ability to maintain existing, or establish new, business relationships and continued access to sources of funding.* » (BCBS, 2009, p. 19). Le risque de réputation est en quelque sorte « *le risque des risques* » (Olieslagers, 2019) parce que, comme pointé par Lessambo (2020, p. 175), « *the velocity of reputation risk is much faster than ever before.* ». De fait, un risque de réputation défavorable peut avoir un impact sur toutes les catégories de risques de la taxonomie. De plus, Lessambo (2020, p. 175) rappelle que le Basel Committee a souligné de manière consistante l'impact positif d'une réputation forte. En effet, celui-ci permet à la direction de répondre efficacement et de manière efficiente à une crise et c'est pourquoi il est nécessaire de mettre en place des outils de mesure et des méthodologies robustes du risque réputationnel en termes des autres risques (crédit, liquidité, marché, et autres), de sorte à maintenir la confiance du marché.

Sous-section 3.7 : Risques émergents (« emerging risks »)

L'objectif de cette section est d'appréhender l'émergence de risques dans la sphère de la gestion des risques. On parle de risques émergents parce que leur probabilité et impact se sont considérablement accentués au cours des dernières années. Ces « nouveaux » risques exercent une pression croissante sur la stabilité financière et les business models des institutions financières. Un autre aspect important qui nous pousse à considérer ces risques est, qu'à ce jour, ils sont peu explorés au travers de la gestion des risques, représentant donc de potentielles lacunes dans le secteur bancaire. Pourtant, comme tout risque, ils requièrent une gestion saine composée des quatre étapes du cycle de gestion des risques abordé plus tôt.

Olieslagers (2019) a identifié cinq risques émergents : le risque de taux d'intérêt bas, le risque lié au changement climatique, le risque de pandémie, le risque cybernétique, et le risque géopolitique. Ces risques ne seront pas détaillés ici mais l'annexe 12 (pp. 145-150) propose des zooms sur chacun de ces risques. À savoir, le risque cybernétique est déjà fortement traité dans le secteur bancaire et des cadres de gestion de ce risque sont déjà mis en place.

Section 3 : Comment une banque assure la gestion des risques en pratique ?

Cette section va permettre d'appréhender comment une banque applique les principes de gestion des risques pour maintenir des niveaux de risque acceptables. Il y a alors trois

considérations à prendre en compte : les principes de gouvernance, le contrôle interne, et le contrôle externe via les auditeurs externes.

Sous-section 3.1 : Principes de gouvernance

La gouvernance d'entreprise est l'ensemble des processus, coutumes, politiques, lois, et institutions qui affectent la manière dont une entreprise est dirigée, administrée ou contrôlée. Elle comprend également les relations entre les nombreuses parties prenantes impliquées et les objectifs qui gouvernent l'entreprise (Henrard, 2020).

La gouvernance d'entreprise s'inscrit dans l'organisation d'une société qui, dans le secteur bancaire, est un système à deux niveaux composé du conseil d'administration (ou « Board of Directors ») et de la direction générale (ou « Executive Management »). Henrard (2020) définit ces organes comme suit :

- Le conseil d'administration : *« is a body of elected or appointed people that represent the shareholders (or according to better governance, the stakeholders) of the company. They oversee its strategy, business plan and budgets, they approve high-level executive appointments. They ensure overall availability of financial resources, set the compensation of senior Management, and are responsible for organizing the annual (and occasionally, exceptional) shareholders' meetings. Its role is non-executive and according to good corporate governance, it includes a minority of executives as well as independent directors. »* (Henrard, 2020) ;
- La direction générale : *« is a body of people who have been elected by the Board of Directors in order to lead the organization. It includes the CEO, the CFO, as well as some other, senior heads of businesses, functions, geographies. Its composition varies freely according to industry sector, company size and structure, and business imperatives. Its functioning is much less regulated than the Board of Directors. »* (Henrard, 2020).

Une gouvernance saine et une définition claire des rôles du conseil d'administration et de la direction générale contribuent à la valeur globale d'une entreprise. En effet, ces deux impératifs permettent d'accroître la transparence du management et le contrôle des risques, d'augmenter la responsabilisation, de garantir un comportement conforme à la stratégie et aux valeurs de

l'entreprise, et d'agir comme une garantie de préservation des intérêts de toutes les parties prenantes (Henrard, 2020).

Pour assurer une gouvernance saine, il convient de séparer l'organisation par type d'activités. Au nombre de quatre, nous avons premièrement le business. Ensuite, viennent les opérations (gestion de l'IT, des paiements, des comptes clients, de la sécurité, *etc.*). Un troisième type d'activités sont les fonctions de support, c'est-à-dire les départements finance, ressources humaines, juridique et fiscal, communication, *etc.* Finalement, nous retrouvons les fonctions de contrôle composées de l'audit et des départements risque et conformité (Henrard, 2020).

Une banque, en pratique, est constituée de nombreux comités à qui le conseil d'administration délègue des missions et des responsabilités (Henrard, 2020). Parmi ces comités, on retrouve le comité d'audit qui passe en revue au moins une fois par an les règles et procédures de l'organisation (règles d'évaluation comptable, procédures d'évaluation du capital, système de contrôle interne, *etc.*), le comité du risque et du capital chargé de superviser la gestion des risques (accent mis sur le profil de risque, l'appétit pour le risque, les règles réglementaires en matière de risques, *etc.*), le comité des récompenses et des rémunérations chargé de superviser le régime de rémunération, le comité de nomination et de désignation chargé de superviser le recrutement, le licenciement et la promotion des cadres supérieurs (Henrard, 2020).

La gestion des risques s'articule autour des principes de gouvernance d'une organisation. Cependant, depuis la crise des subprimes de 2008, la gestion des risques a considérablement évolué, à tel point qu'elle a conduit à reconsidérer les principes de base de la gouvernance pour en édicter de nouveaux en termes de risques. Henrard (2020) rapporte sept nouveaux principes de gouvernance d'entreprise au niveau de la gestion des risques :

- La sphère de responsabilité de la gestion des risques s'étend et nécessite une coordination croissante avec d'autres rôles exécutifs.
- La gestion des risques est de plus en plus reconnue comme une source d'avantage concurrentiel. Il convient donc d'intégrer la gestion des risques dans les activités journalières et la stratégie d'une organisation.
- La gestion du risque soutient la gestion de la valeur et du capital en supportant la croissance, les coûts de financement, les coûts du risque et les coûts du capital.

- Une gouvernance du risque lie les rôles et les responsabilités à la structure, aux processus et à l'infrastructure de l'organisation.
- Les fonctions de gestion des risques exercent de plus en plus d'activités supplémentaires, au-delà de l'accent traditionnel mis sur le contrôle des risques. On passe d'une approche minimaliste où la gestion des risques est vue uniquement comme une unité de contrôle à une approche maximaliste où la gestion des risques est une unité de pilotage.
- La gestion des risques est incluse dans les lignes de reporting supérieures et n'est plus vue comme une fonction consultative ou comme une simple ligne de reporting vers les fonctions financières.
- L'alignement et l'interaction entre les business units et le groupe pour la centralisation de la gestion des risques dépend du degré de centralisation de l'organisation.

Sous-section 3.2 : Contrôle interne

Le BCBS a développé un cadre pour les systèmes de contrôle interne dans les organisations bancaires (« Framework for Internal Control Systems in Banking Organisations ») dont l'objectif est de mettre en évidence un certain nombre de principes que les autorités de contrôle peuvent utiliser pour évaluer les systèmes de contrôle interne des banques (BCBS, 1998, p. 1). Le contrôle interne constitue une composante critique de la gestion d'une banque et la base sur laquelle est fondé le fonctionnement fiable et solide des organisations bancaires. Le BCBS a identifié cinq sources principales de déficiences au niveau du contrôle (BCBS, 1998, p. 6). Les principes, au nombre de 13, s'articulent autour de ces cinq sources de déficiences (voir annexe 13 pour les sources et principes en détail, p. 151).

Le BCBS (1998, p. 8) définit le contrôle interne comme un processus continu mis en œuvre par le conseil d'administration, la direction générale et tous les niveaux du personnel. Le conseil d'administration et la direction générale sont responsables de l'établissement d'une culture appropriée pour faciliter un processus de contrôle interne efficace et du suivi de son efficacité sur une base continue en s'assurant également que chaque individu de l'organisation participe au processus. Les objectifs du contrôle interne ont été répartis en trois catégories : des objectifs de performance (comme l'efficacité et l'efficience des activités), des objectifs en matière d'information (notamment la fiabilité, l'exhaustivité et la ponctualité des informations financières et de gestion), et des objectifs de conformité (s'assurer d'être conforme avec les lois

et réglementations applicables, les exigences des superviseurs et les politiques et procédures de l'organisation) (BCBS, 1998, p. 8).

En pratique, le contrôle interne s'opère selon trois niveaux (Henrard, 2020). Le premier niveau de contrôle se trouve au niveau des business lines et est effectué par les équipes opérationnelles (middle office, back office, *etc.*) et leurs managers. Le second niveau de contrôle s'effectue au niveau des équipes de conformité et risque. Les contrôles sont effectués d'un côté par des fonctions de contrôle permanent intégrées à l'organisation et, d'un autre côté, par des fonctions de contrôle permanent indépendantes de l'organisation. Ces deux premiers niveaux de contrôle sont des niveaux permanents, c'est-à-dire effectué de manière journalière. Le troisième niveau de contrôle, lui, est périodique et concerne les fonctions d'audit interne (Henrard, 2020).

Sous-section 3.3 : Auditeurs externes

Par définition, les auditeurs externes ne font pas partie de l'organisation d'une banque et n'entrent donc pas dans le cadre du contrôle interne. Cependant, le BCBS rapporte qu'ils ont un impact important sur la qualité des contrôles internes via leurs activités d'audit, des discussions avec la direction et des recommandations qu'ils proposent pour améliorer les contrôles internes (BCBS, 1998, p. 25).

En ce sens, les auditeurs externes évaluent l'efficacité des systèmes de contrôle interne d'une banque afin de déterminer s'ils peuvent y appliquer leurs propres procédures d'audit. Ceci requière donc une compréhension approfondie des systèmes de contrôle interne afin de poser un diagnostic informé (BCBS, 1998, p. 25). De plus, dans certains pays l'audit externe n'est pas uniquement réalisé pour donner un avis sur les comptes annuels d'une banque mais est étendu pour fournir des évaluations de la portée, de l'adéquation et de l'efficacité du système de contrôle interne, y compris le système d'audit interne qui est partie intégrante du contrôle interne (BCBS, 1998, p. 25).

Section 4 : Quelle sélection de risques pour ce mémoire ?

Dans le cadre de ce mémoire, nous avons décidé de nous concentrer sur trois risques : risque de crédit, risque de conformité et risque de fraude. Les deux premiers ont été détaillés plus tôt. Pour rappel, le risque de crédit est l'éventualité qu'un emprunteur ou une contrepartie bancaire ne parviendra pas à remplir ses obligations conformément aux conditions convenues (BCBS, 2000, p. 1) et le risque de conformité est le risque auquel une organisation s'expose lorsqu'elle

se trouve dans l'incapacité de répondre à ses obligations, c'est-à-dire aux réglementations, règles de conformité et standards propres à l'organisation, aux lois et au code de conduite applicables aux activités bancaires (BCBS, 2005, p. 7).

Le risque de fraude est un risque opérationnel puisqu'il se concentre sur les risques associés aux erreurs et aux événements défavorables qui nuisent à la bonne conduite journalière d'une organisation (CIMA, 2008, p. 21). Le risque de fraude est le risque d'une perte découlant d'actions frauduleuses de la part d'une ou plusieurs personnes internes ou externes à une organisation (Open Risk Manual, 2021). Ce risque est généralement scindé en deux : fraude interne et fraude externe. Ces notions sont définies comme suit par le BCBS :

- Fraude interne : « *Losses due to acts of a type intended to defraud, misappropriate property or circumvent regulations, the law or company policy, excluding diversity/discrimination events, which involves at least one internal party.* » (BCBS, 2020, p. 7).
- Fraude externe : « *Losses due to acts of a type intended to defraud, misappropriate property or circumvent the law, by a third party.* » (BCBS, 2020, p. 7).

Les motivations sous-jacentes menant au choix de sélectionner ces trois risques sont, d'une part, qu'ils répondent tous les trois à des règles, règlements, standards prédéfinis et précis (Henrard, 2020). Dès lors, une fois que des règles précises sont posées, il est possible de les formaliser relativement facilement d'un point de vue informatique et donc de concevoir des outils basés sur de l'IA et de la RPA dont les perspectives, autant pratiques qu'économiques, sont abondantes. D'autre part, ces risques sont déjà greffés aux opérations journalières des banques. Par conséquent, les perspectives d'implémentation de systèmes IA et RPA sur ces risques consistent à automatiser de plus en plus de processus en remplaçant ou en se joignant à ceux déjà existants plutôt que de tenter de développer des outils *ab initio*. Évidemment, automatiser plutôt que créer à la base implique des coûts plus faibles et des développements plus rapides et plus efficaces. C'est d'ailleurs sur base de ces notions que de nouveaux projets sont lancés. On parle de « use cases » et de « business cases ». Les use cases visent à définir la valeur ou l'utilité qu'un outil aura pour les personnes impliquées. Les business cases étudient l'impact économique d'un outil pour aider à la décision.

Un autre facteur qui nous amène à nous concentrer sur ces risques est la disponibilité des données. En effet, la RPA et surtout l'IA nécessitent des données de qualité et sur de longues

périodes. Or, les données de crédit, fraude et conformité existent et sont généralement facilement accessibles (Fliche & Yang, 2018, p. 9), ce qui en retour facilite les développements.

Finalement, il a été montré que les trois canaux principaux où utiliser de l'IA (et *a fortiori*, de la RPA) sont le front office (gestion des transactions), le middle office (détection de la fraude et gestion des risques) et le back office (souscription) (Digalaki, 2021). Digalaki (2021) indique également des opportunités d'économies de coût supérieures pour le middle office que pour le front office et le back office.

Conclusion

Cette deuxième partie a permis d'étudier le fonctionnement de la gestion des risques dans le secteur bancaire, en parcourant notamment ses dimensions – probabilité et impact, ses objectifs – avec pour but premier d'atténuer et d'évaluer les dimensions susmentionnées et son cycle en quatre temps – identification, évaluation et mesure, atténuation, et suivi et signalement. Ensuite, nous avons identifié les mesures principales du risque, à savoir le stress testing, la value at risk (VaR), et l'expected shortfall (ES) qui d'ailleurs remplace progressivement la VaR (van Greuning & Bratanovic, 2020, p. 252). Rappelons que la VaR et l'ES sont principalement des mesures de gestion du risque de marché et que des VaR ou ES au niveau des risques opérationnel et de crédit suivent d'autres méthodologies que celles que nous avons détaillées. L'appétit du risque a également été appréhendé afin de se donner les moyens de comprendre l'image globale dans laquelle la gestion des risques s'inscrit.

Par la suite, nous nous sommes penchés sur les types de risque et avons dressé la taxonomie des risques qui permet une catégorisation compréhensible, commune et relativement stable des types de risque dans une organisation (Gouvernement du Canada, 2016). Les principales catégories de risques sont le risque de crédit, le risque de marché, le risque de liquidité, le risque opérationnel et les autres risques qui n'entrent pas dans les catégories précédentes mais qui ont généralement une portée plus globale et un impact réparti sur plusieurs des autres catégories. La taxonomie des risques est aussi surplombée du risque de réputation qui, en sa qualité de « risque des risques » (Olieslagers, 2019), peut avoir un impact sur toutes les catégories de risque. Il était également opportun de traiter des risques émergents qui ont vocation à entrer dans cette taxonomie à l'avenir puisque ces risques ont connu un accroissement de leur probabilité et impact durant la dernière décennie. Ces risques sont le risque de taux d'intérêts

bas, le risque lié au changement climatique, le risque de pandémie, le risque cybernétique et le risque géopolitique.

Au travers des principes de gouvernance d'entreprise et du contrôle interne, nous avons vu comment une banque est capable d'assurer une gestion des risques saine. Également, n'oublions pas l'impact important des auditeurs externes sur la qualité des systèmes de contrôle interne.

Finalement, nous avons avancé les motivations qui nous ont conduites à mettre à l'étude et l'analyse les risques de crédit, fraude et conformité dans ce mémoire. Les principales étant l'efficience sur les plans pratiques et économiques de leur formalisation informatique, les coûts faibles et développements rapides et efficaces que des automatisations au niveau de ces risques engendrent, la disponibilité des données et enfin, les opportunités d'économies de coût supérieures pour ces risques.

PARTIE 3 : TENDANCES ET DÉFIS PRINCIPAUX

Introduction

À l'entame de cette troisième partie, il est opportun d'en définir son contenu et ses objectifs. Nous allons examiner les principales tendances et principaux défis du marché en matière d'IA et de RPA, c'est-à-dire les zones principales qui ont été mises en évidence et où les possibilités IA et RPA semblent être les plus pertinentes aujourd'hui mais pour lesquelles il existe également des challenges tangibles. Nous allons nous concentrer sur des institutions financières européennes et des institutions financières internationales qui opèrent en Europe. Ce ciblage est en ligne avec les entretiens réalisés dans le cadre de ce mémoire. En effet, nous avons pris le parti de nous concentrer sur deux places financières européennes : la Belgique et le Luxembourg. De plus, se focaliser sur des institutions financières sur le marché européen fait sens puisqu'elles évoluent dans un environnement économique commun et répondent aux mêmes standards et régulations. L'objectif de cette section est donc de dépeindre les grandes tendances et les défis en matière d'IA et RPA dans l'Union européenne (UE). Ceci permettra par la suite d'analyser si les tendances et défis sont confirmés dans le périmètre des banques que nous avons interrogées et dans le périmètre des risques que nous considérons.

Section 1 : Tendances principales

L'EBF¹¹ (2019, pp. 6-7) a identifié quatre catégories d'opportunités IA dans le secteur bancaire :

- Amélioration de l'interaction et de l'expérience client (e.g. : chatbots, robots conseillers, authentification et autorisation biométriques, segmentation des clients, etc.)
- Amélioration de l'efficacité des processus bancaires (e.g. : automatisation/optimisation des processus, maintenance prédictive en informatique, extraction automatisée des données, traitement des documents KYC, credit scoring¹², etc.)

¹¹ European Banking Federation : « *is the voice of the European banking sector, uniting 32 national banking associations in Europe that together represent some 5,981 banks – large and small, wholesale and retail, local and international – employing about 2,6 million people.* » (<https://www.ebf.eu/about-us/>)

¹² « *Credit scoring is a statistical analysis performed by lenders and financial institutions to determine the creditworthiness of a person or a small, owner-operated business. Credit scoring is used by lenders to help decide whether to extend or deny credit. A credit score can impact many financial*

- Amélioration de la sécurité et du contrôle des risques (e.g. : renforcement du contrôle des risques, surveillance de la conformité, détection des anomalies, détection et surveillance de la lutte contre le blanchiment d'argent, prédiction des limites de capacité des systèmes, soutien de l'assurance de la qualité des données, prévention et détection de la fraude, surveillance des transactions de paiement, prévention des risques liés à la cybersécurité, *etc.*)
- Création de nouvelles opportunités commerciales et génération de nouvelles sources de revenus (e.g. : gestion des finances personnelles, analyse des investissements, répartition des actifs, génération de prospects, la réduction du taux de désabonnement, *etc.*).

Une étude du Parlement européen a, quant à elle, mis en évidence sept applications IA et RPA (Calzolari, 2021, pp. 14-18) qui s'inscrivent dans une ou plusieurs des catégories ci-dessus et qui conduisent à transformer les institutions financières traditionnelles et leurs business models. Avant de les détailler, il convient de mentionner que ces applications sont toutes considérées comme IA selon l'étude mais que certaines n'ont pas de capacité d'apprentissage. Auquel cas, elles relèvent plutôt du caractère robotique selon la conception de la distinction entre IA et RPA que nous avons faite en fin de première partie et que nous avons retenue pour ce mémoire. Cette remarque vaut également pour les défis principaux.

Prévision des prêts et des risques de crédit. Généralement, les institutions financières possèdent des informations limitées sur les emprunteurs potentiels et leur degré de risque. Ces asymétries d'information peuvent représenter un problème fondamental dans la mesure où elles créent des inefficacités du marché, voire conduisent à son effondrement (Calzolari, 2021, pp. 14-15). Or, l'arrivée des big data fournit d'autres sources d'information qui peuvent être agrégées et utilisées dans les modèles de prédiction de risque via des techniques comme le machine learning¹³. Ces autres sources d'information sont connues sous le nom de données alternatives et comprennent les médias sociaux, les factures des services publics, les données de télécommunications, les données de nos smartphones ou des achats passés, *etc.* Une quantité de données plus grande et des meilleurs outils de prédiction (machine learning) conduisent à

transactions, including mortgages, auto loans, credit cards, and private loans. », https://www.investopedia.com/terms/c/credit_scoring.asp

¹³ Pour rappel, le machine learning est un sous-domaine de l'intelligence artificielle comme nous l'avons vu en introduction de la première partie de ce mémoire.

des décisions de prêt plus rapides et de meilleures prévisions des risques individuels grâce à une segmentation plus fine des emprunteurs potentiels (Calzolari, 2021, p. 15). Pour les banques, de meilleures évaluations, mesures et prédictions des risques de crédit permettent d'économiser sur les exigences en capital et les coûts associés (Aloso & Carbó, 2021, p. 34).

Assurance. Pour les assurances également, des techniques comme le machine learning accompagnées de données alternatives permettent aux compagnies d'assurance d'obtenir une évaluation plus précise des risques, une meilleure personnalisation des contrats et un meilleur accès à l'assurance (Calzolari, 2021, p. 15).

Systèmes de paiement. L'IA est déjà largement adoptée au niveau de la gestion des paiements, notamment en aidant à la détection de la fraude, en luttant contre le blanchiment d'argent, et en rendant les réseaux de paiement plus efficaces. En effet, il a été noté que les actions frauduleuses de paiements ont augmenté au cours des dernières années. Or, les solutions IA permettent de sauver des coûts et d'atteindre une meilleure performance que l'intervention humaine (Calzolari, 2021, p. 15).

Robot-conseillers et assistants virtuels. Les robot-conseillers permettent d'assister les investisseurs privés en interagissant avec les marchés financiers de sorte à fournir aux clients des recommandations personnalisées dans la gestion de leur portefeuille.

Les assistants virtuels aident les clients à interagir et à opérer avec leurs institutions financières de manière fluide, parfois même sans intervention humaine. Ces assistants fournissent aux clients des informations à jour qu'elles soient sollicitées ou non, ce qui peut créer des opportunités et pour les clients et pour les institutions financières. De plus, les institutions financières bénéficient de données additionnelles suite à ces interactions entre assistants virtuels et clients (Calzolari, 2021, pp. 15-16).

Gestion des actifs et des risques. Au niveau de la gestion des actifs, l'IA semble être devenue un outil indispensable. En effet, elle peut être utilisée pour identifier les actifs à échanger, pour optimiser des portefeuilles, ou pour exécuter des transactions automatiquement (Calzolari, 2021, pp. 16-17). Calzolari (2021, p. 16) rapporte d'ailleurs que certains fonds sont complètement gérés avec de l'IA (e.g. : Numerai, Aidiya Holdings, Taaffeite Capital Management).

Concernant la gestion des risques, l'IA offre des solutions pratiques pour classer les risques et pour aider à la décision pour la gestion des risques. Ici, l'automatisation joue un rôle important dans le processus décisionnel grâce à la prise de décision automatisée qui rend le processus fluide et continu. Les modèles de risque traditionnels peuvent également être évalués grâce au machine learning et ainsi identifier les prédictions extrêmes et irréalistes (Calzolari, 2021, p. 17). À ce sujet, l'EBA réalise des questionnaires d'évaluation des risques (« Risk Assessment Questionnaires (RAQs) ») semestriels dans lesquels on peut retrouver les perceptions des répondants sur les utilisations IA de leur organisation en termes de gestion des risques. Par organisation, nous entendons les banques européennes puisque ce sont celles qui ont été interrogées. Le RAQ du printemps 2019 (EBA, 2019, p. 38) montre que les scoring de risques et les modélisations de risques sont les catégories pour lesquelles il existe le plus d'applications en utilisation ou en phase de test ou en développement. En effet, les répondants rapportaient 63% d'applications en utilisation ou en phase de test ou en développement pour les scoring de risques, et 55% pour les modélisations de risques. Les catégories intermédiaires sont les aspects de conformité réglementaire avec 36% et la gestion des risques cybernétiques avec 34%. Finalement, les deux catégories pour lesquelles les répondants ont mentionné soit des applications au stade de discussion, soit aucune activité pour le moment sont le calcul des exigences en matière de capital réglementaire et l'évaluation des outils externes/des outils du fournisseur avec 72% et 79%, respectivement, d'applications au stade de discussion, soit aucune activité (voir annexe 14 pour la ventilation de ces résultats, p. 152).

Trading algorithmique. Le trading algorithmique a été un des premiers domaines dans lequel on a retrouvé des applications automatisées parce qu'il répond à des règles précises et pré-spécifiées. Ces applications offrent des capacités pour trader et interagir avec les marchés à très haute fréquence, et ainsi d'obtenir des petites marges d'arbitrage sur des ordres importants. Aujourd'hui, le domaine est largement parsemé d'applications IA qui permettent d'évaluer les positions d'un portefeuille, de prédire les prix du marché et l'exposition au risque et enfin, d'identifier les meilleures actions et ajuster de manière autonome les positions risquées ou non rentables (Calzolari, 2021, p. 17).

Autres applications. Il existe également d'autres applications IA qui sont souvent utilisées dans les activités back office (Calzolari, 2021, p. 18). Le RAQ du printemps 2019 (EBA, 2019, p. 38) rapporte plus de 40% d'applications en utilisation pour la détection de la fraude, environ 19% pour le processus d'onboarding des clients, 27% pour les processus de lutte contre le

blanchiment d'argent et le financement du terrorisme (AML/CFT¹⁴), et 17% pour l'amélioration de la qualité des données (voir annexe 15 pour la ventilation de ces résultats, p. 153).

Zoom sur les opportunités au niveau crédit, fraude et conformité. Concernant les activités de crédit, l'utilisation de l'IA semble concerner principalement l'optimisation des systèmes de scoring (Fliche & Yang, 2018, p. 13). Ceci est d'autant plus vrai pour le crédit à la consommation pour lesquels « *les clients sont plus sensibles à la fluidité et la vitesse d'exécution* » (Fliche & Yang, 2018, p. 13). Les perspectives IA au niveau du scoring résident principalement sur le score de crédit (ou « credit score »). Le score de crédit détermine le montant et les conditions pour un emprunteur, c'est donc un problème de régression particulièrement adapté au machine learning d'après Fliche et Yang (2018, p. 13). En ce sens, l'IA permettrait de coupler les données bancaires, généralement utilisées pour attribuer le score de crédit, à des données externes (e.g. : activité sur les réseaux sociaux, utilisation du smartphone, données sur les comportements des clients) afin de rendre le score plus précis mais également de calculer ce score lorsque l'historique bancaire de l'individu est faible ou inexistant (Fliche & Yang, 2018, p. 13 ; FSB, 2017, p. 12). Que l'on parle de données externes, pour Fliche et Yang ou, comme nous l'avons vu plus tôt avec Calzolari, de données alternatives, ces deux concepts sont similaires. Cependant et comme le rappelle le FSB (2017, p. 12), l'utilisation de données personnelles soulève d'autres questions de politique générale sur la confidentialité des données et la protection des données. En Europe, la GDPR, entrée en vigueur en 2018, devrait permettre de couvrir ses questions, au moins partiellement même si les régulateurs « *should keep in mind that cross-border supervision, cooperation and investigation and other regulatory issues may be expected to arise with AI and machine learning applications active across jurisdictions* » (FSB, 2017, p. 38).

Au niveau de la fraude, il est dit que « *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.* » (Fliche & Yang, 2018, p. 14), en utilisant des techniques IA pour la reconnaissance, l'analyse et la validation des documents. La détection des transactions frauduleuses revêt également du domaine des paiements. Là aussi, le champ d'application de l'analyse des données en temps réel via l'IA est notable (Fliche & Yang, 2018, p. 14).

¹⁴ Anti-Money Laundering/Combat the Financing of Terrorism

Finalement, en termes de conformité, Fliche & Yang (2018, p. 16) notent que l'IA pourrait améliorer la performance de la conformité en automatisant certains processus, notamment les processus Know Your Customer (KYC), de lutte contre le blanchiment d'argent et le financement du terrorisme.

Section 2 : Défis principaux

Outre les applications dont nous venons de traiter, l'étude du Parlement européen a également identifié les principaux défis qui sous-tendent l'intelligence artificielle, notamment parce que les applications basées sur l'IA sont relativement récentes et que ces solutions nécessitent une combinaison de compétences spécifiques liées à l'IA et au secteur financier (Calzolari, 2021, p. 28).

Obstacles à l'adoption. Calzolari, (2021, pp. 28-29) identifie quatre sources d'obstacles à l'adoption. Premièrement, il mentionne le manque de données adéquates en termes de qualité et de quantité. Or, nous l'avons vu, le plein potentiel de l'IA s'atteint lorsqu'on combine les données financières aux données alternatives qui sont, à ce jour, peu intégrées dans les institutions financières. Deuxièmement, on constate un manque de compétences liées à l'IA pour répondre à une demande de main-d'œuvre en forte croissance. À ce sujet, l'Europe serait en retard par rapport aux autres pays en termes de formation et de rétention des jeunes ayant des compétences en IA comme l'ont montré Anderson, Viry, et Wolff (2020). Troisièmement, les banques traditionnelles semblent avoir du mal à adopter des approches IA et à les intégrer dans leurs solutions préexistantes, notamment lorsque l'IA implique d'automatiser des tâches qui substituent du personnel. Cette résistance au changement de la part du personnel peut d'ailleurs être si forte que des institutions financières ne parviennent pas à adopter l'IA ou doivent l'adopter via des acquisitions externes, d'après Calzolari (2021, p. 28). Quatrièmement, les institutions financières doivent s'assurer de leur conformité avec les réglementations déjà existantes lorsqu'il s'agit de systèmes basés sur l'IA.

Injustice et discrimination. L'utilisation du machine learning basée sur des datasets conduit parfois à des décisions jugées injustes et discriminantes (Calzolari, 2021, p. 29). Nous avons d'ailleurs abordé un exemple de résultat injuste et discriminant avec Ammanath *et al.* (2020, pp. 6-7) dans la section sur les risques de l'IA. Calzolari (2021, p. 29) propose des exemples similaires dans le domaine financier. Ces décisions injustes et discriminantes se produisent avec des algorithmes d'IA qui respectent strictement les lois anti-discrimination sans utiliser de

variables sensibles comme le sexe, l'origine ethnique, ou la religion. Un autre aspect important qui peut conduire à des décisions injustes sont les données de départ. En effet, il se peut qu'un dataset contiennent des biais de telle façon à ce que, une fois l'outil IA entraîné sur ces données, il tend à simplement répliquer les biais contenus dans le dataset (Calzolari, 2021, p. 29 ; Ammanath *et al.*, 2020, p. 6).

Interactions des systèmes d'IA avec le marché. Les systèmes d'IA, en plus d'avoir à interagir avec les humains, doivent également interagir entre eux (Calzolari, 2021, pp. 29-30). On appelle cela des systèmes multi-agents. Or, il est déjà délicat pour les humains de comprendre le fonctionnement d'une seule IA autonome. Cet apprentissage s'avère encore plus ardu lorsqu'on fait face à de systèmes d'IA autonomes interagissant entre eux et produisant parfois des résultats inattendus.

Explicabilité de l'IA. Les humains font face à un défi de taille avec l'IA. On parle du problème de la boîte noire ou de l'explicabilité de l'IA (Calzolari, 2021, p. 30 ; Ammanath *et al.*, 2020, p. 5). Ce problème fait référence à la difficulté ultime d'expliquer les prédictions auxquelles un système d'IA aboutit. À ce sujet, Calzolari (2021, p. 30) mentionne une différence importante entre explicabilité et interprétation : l'explicabilité est la possibilité de comprendre comment un algorithme fonctionne alors que l'interprétation est la capacité de comprendre pourquoi certaines décisions spécifiques ont été prises par l'algorithme pour un cas donné.

Problèmes de confidentialité et acceptation par le public. Nous l'avons dit, les datasets contiennent de plus en plus de données pour plus d'efficacité des applications IA. Cependant, cela soulève des questions de confidentialité parce que les individus ne sont pas toujours conscients ou au courant que ces sources de données sont utilisées (Calzolari, 2021, p. 31). Il y a donc un compromis entre l'efficacité et la rentabilité des systèmes d'IA et les données qu'ils utilisent pour obtenir des performances prédictives supérieures. Pour résoudre ce défi, les institutions financières se doivent d'être transparentes dans les données qu'elles utilisent de sorte à susciter l'acceptation de l'IA par le public (Calzolari, 2021, p. 31).

Modification des relations avec les clients et les régulateurs. L'intelligence artificielle conduit également à remodeler les relations entre les clients et les régulateurs (Calzolari, 2021, p. 31). En effet, on évolue de plus en plus vers des interactions complètement digitales avec les clients qui se substituent aux interactions humaines (Calzolari, 2021, p. 31). Cependant, cette substitution représente un défi en ce sens qu'elle peut conduire à un décalage important et

reléguer certains clients à des services financiers médiocres, surtout pour les générations plus âgées. Concernant les générations plus jeunes, elles pourraient également rencontrer le risque de ne pas comprendre le fonctionnement des systèmes d'IA et de se reposer trop sur elles pour prendre leurs décisions. Au sujet des relations avec les régulateurs, le risque ici est une augmentation de la fragmentation avec des solutions différentes et éventuellement incompatibles pour un même problème (Calzolari, 2021, p. 31). Une piste de solution est peut-être à trouver dans une coordination internationale forte de la réglementation autour de l'IA, qui manque pour le moment d'après Calzolari (2021, p. 31).

Risque pour la stabilité financière. L'IA représente également un risque tangible pour la stabilité du système financier. Calzolari (2021, pp. 32-33) a distingué cinq sources capables de mettre en péril la stabilité financière. Premièrement, il argumente que les systèmes IA financiers ne sont pas testés sur des scénarios de crise financière, notamment parce que réaliser des tests sur le marché est coûteux et constituent une source d'instabilité en soi. Deuxièmement, des systèmes d'IA peuvent rencontrer le problème de surapprentissage¹⁵, c'est-à-dire des systèmes qui sont entraînés sur des données qui correspondent aux conditions du marché pendant la phase d'entraînement mais qui, pendant la phase d'apprentissage, définissent des paramètres qui ne correspondent pas ou qui ne sont pas adaptés aux changements des conditions du marché générés par un choc persistant et inattendu. Auquel cas, ces systèmes s'adaptent mal aux nouvelles conditions de marché et conduit parfois à réentraîner les modèles, processus coûteux que les institutions financières préfèrent parfois retarder. Troisièmement, l'instabilité peut survenir des suites d'une uniformisation des systèmes d'IA qui, en retour, conduirait à des comportements coordonnés non désirés et à un nouveau type d'interconnexion des marchés financiers. Cette uniformisation peut provenir d'adoption de types d'algorithmes similaires qui identifieraient des schémas communs dans les variables explicatives utilisées pour les prédictions, d'algorithmes entraînés sur les exactes mêmes données (dans le cas où les applications IA sont externalisées vers des acteurs tiers) ou encore être le fruit des régulations qui créeraient des sources d'homogénéité. Cette homogénéisation est particulièrement dangereuse parce qu'elle pourrait conduire à la création de déséquilibres sur le marché si des millions d'individus prennent des décisions similaires. Quatrièmement, l'IA soulève régulièrement le problème de la « feedback loop » ou boucle de rétroaction, en français. Ce problème stipule que « *when AI algorithms populate financial markets massively, financial data*

¹⁵ <https://fr.wikipedia.org/wiki/Surapprentissage>

will incorporate the algorithms' decisions, which will use these data to learn and update their predictions and decisions. » (Calzolari, 2021, p. 33). Il peut conduire à des prophéties autoréalisatrices et engendrer un risque de générer des bulles financières. Cinquièmement, la finance de l'ombre (ou « shadow banking ») est également amenée à utiliser des systèmes IA ce qui pose un problème dans la mesure où les banques de l'ombre ne sont pas assujetties aux réglementations et sont donc capables de prendre des niveaux de risques dans leurs applications IA beaucoup trop élevés (Calzolari, 2021, p. 33).

Risques cybernétiques. Avec une utilisation de plus en plus grande d'outils IA, les institutions financières s'exposent aux risques de manipulations malveillantes et non observées, notamment des manipulations de données (Calzolari, 2021, pp. 33-34). D'autant plus qu'il a été montré que la manipulation de données sur des techniques de machine learning n'était pas si compliquée et que les banques s'appuient de plus en plus sur des services tiers. Ces deux points conduisent les banques à être des cibles d'intérêt pour des manipulations malveillantes.

Structure de marché changeante et concentrée. Calzolari (2021, p. 34) rapporte que les acteurs importants du secteur financier développent leurs solutions IA en interne mais que de nombreux petits et moyens acteurs ont recours à des services tiers. Or, se reposer sur des services tiers est une source de risque parce que cela complique le suivi et la surveillance des entités réglementées. Également, l'IA conduit à des changements dans le secteur financier où, pour le moment, la concurrence est limitée. Ces changements pourraient conduire à augmenter la concurrence, ce qui réduirait la rentabilité des banques et augmenterait les faillites dans le secteur (Calzolari, 2021, p. 35). De plus, les GAFAM ou Bigtech représentent une menace pour le secteur financier parce que ces géants sont prêts à y entrer et à y répliquer leur chemin vers la concentration dans certaines activités du secteur financier (Calzolari, 2021, p. 35).

Financement de l'IA pour le secteur financier et en général. « *Europe is currently in a second line for developing AI applications* » d'après Calzolari (2021, p. 35), et ce parce que le marché des actions est sous-développé, que le marché du capital-risque est insuffisant et que l'Europe ne compte aucune Bigtech. Or, ces facteurs sont des leviers de financement fort pour la croissance du secteur financier et du marché des applications IA (Calzolari, 2021, p. 35).

Conclusion

Tout au long de cette troisième partie, nous avons mis en évidence les opportunités en termes d'IA et de RPA pour le secteur financier ainsi que les défis principaux que l'IA et la RPA impliquent.

Nous avons d'abord identifié les quatre zones d'opportunités/améliorations : interaction et expérience client, efficacité des processus bancaires, sécurité et contrôle des risques, et création de nouvelles opportunités commerciales et génération de nouvelles sources de revenus. Ces quatre zones ont été complétées d'applications IA et RPA dans des domaines plus précis qui représentent les tendances principales actuelles dans le secteur. Une attention particulière a été posée sur les aspects crédit, fraude et conformité puisqu'ils constituent les objets à l'étude dans ce mémoire. Ces tendances ont été suivies par les défis principaux qui émergent des suites de l'évolution grandissante des concepts d'IA et RPA dans le monde financier.

Fort de l'identification de ces tendances et défis, nous allons maintenant mettre à profit nos découvertes pour analyser et étudier si ceux-ci se retrouvent ou non dans le périmètre des banques que nous avons interrogées.

PARTIE 4 : RÉSULTATS

Introduction

Cette dernière partie a pour objectif d'analyser et d'étudier les données que nous avons récoltées et de les mettre en perspective par rapport à la revue de la littérature. Notre échantillon est constitué de cinq entretiens semi-directifs réalisés dans deux banques européennes, dont une au Luxembourg, BGL BNP Paribas, et une en Belgique, BNP Paribas Fortis. Toutefois, dans une situation idéale, nous aurions conduit des interviews dans cinq banques avec, chaque fois, des spécialistes IA et RPA. Nous allons tant que possible suivre la même structure que celle retenue dans ce mémoire en abordant des concepts dans l'ordre dans lesquels nous les avons vus. Nous allons également répertorier les applications IA et RPA en cours d'utilisation dans chacune des banques. Enfin, nous concluons en proposant une comparaison des deux banques de notre échantillon. Comme expliqué dans la méthodologie, nous avons opté pour une recherche primaire qualitative en sélectionnant la technique d'entretien semi-directif pour la collecte de données. Également, la méthode d'analyse retenue est l'analyse de contenu thématique qui déstructure les données en codes (basés sur la revue de la littérature pour ce mémoire) puis restructure les données en concepts (De Moerloose, 2020).

Section 1 : L'IA ou un domaine toujours abstrait

Dans la première partie de ce mémoire, nous définissions l'intelligence artificielle au pluriel. Effectivement, ce domaine de l'informatique a parcouru bien des chemins et une définition claire et précise ne fait pas l'unanimité tant les avis divergent auprès de la communauté scientifique, l'un ayant pris l'habitude de réfuter l'autre lorsqu'il s'agit de poser une définition de l'IA.

Cette observation a par ailleurs été retrouvée parmi nos interviewés. Laurent Denis, lorsqu'il aborde un nouveau modèle de credit scoring pour les PME au sein de la BGL BNP Paribas, la caractérise de la manière suivante : *« on pensait tous qu'il était basé sur de l'IA [...]. Mais en fait [...], c'est une simple régression linéaire multivariée donc le modèle ne contient aucun autoapprentissage »*. Selon lui, on pourrait donc parler d'intelligence artificielle lorsqu'un système est associé à de l'autoapprentissage.

Pour Orce Marinkosvki, la conception de l'IA est la suivante : *« de ce que j'ai appris, l'IA est un algorithme qui lui-même peut s'autocorriger lorsqu'il constate par lui-même qu'il a commis*

une erreur. Donc, l'IA est dotée d'une possibilité de constater des erreurs et d'une possibilité d'agir, de réajuster. [...] À partir du moment où l'algorithme ne peut pas se corriger lui-même, ce n'est pas de l'intelligence artificielle. ». Au regard de cette conception, un système d'IA est effectivement de l'IA s'il est capable d'autocorrection.

Marc Aguilar, quant à lui, distingue un système informatique « classique » d'un système d'IA par la notion d'intelligence. Pour lui, c'est cette notion d'intelligence qui permet de conceptualiser ce qu'est l'IA : *« on prend de la data et on la transforme de façon à ce qu'on retire de l'intelligence. », « [les] développements informatiques [ne seront] plus réalisés avec des algorithmes classiques procéduraux et prédéfinis mais avec des algorithmes différents avec de l'intelligence. », « l'IA ce sont des algorithmes mathématiques qui vont dégager de l'information de la data, information qui n'est pas prévisible sans cette intelligence. ».* À ce sujet, Marc Aguilar suggère que si l'on veut mettre de l'intelligence dans l'univers, cela devra se faire sur un support technologique et non biochimique, c'est-à-dire sur des machines et non sur des êtres humains comme nous. Cependant, il ne s'étend pas sur une définition de l'intelligence, un terme qui a fait et fait encore l'objet de nombreuses discussions scientifiques et philosophiques (Sternberg, 2000, p. 3).

Un exemple flagrant de cette conception abstraite se retrouve dans la façon dont nos trois interviewés de la BGL BNP Paribas parlent d'une application de détection de fraude au sein de leur banque. En effet, deux d'entre eux partagent la même opinion et la considèrent dotée d'IA mais pas le troisième. Marc Aguilar nous dit : *« On a aussi des algorithmes [basés sur de l'IA] de détection de la fraude. »* et Laurent Denis nous dit : *« [en matière d'IA, nous avons] un module qui permet la détection de la fraude. ».* Orce Marinkovski ne partage pas ce point de vue et relate : *« On a quelque chose pour détecter la fraude, mais c'est plutôt un algorithme très poussé, ce n'est pas encore de l'IA. ».*

Au regard de ces constats et vu sa complexité, même pour des spécialistes, il semblerait qu'il est toujours préférable de traiter de l'IA en termes de capacités comme nous l'avons vu en première partie. Cependant, on peut tout de même affiner ses caractéristiques et suggérer que l'IA est IA lorsqu'elle est capable d'autoapprentissage et d'autocorrection et qu'elle possède de l'intelligence. Reste à savoir ce qu'on entend par intelligence.

Une autre constatation qui ressort de ces résultats est que, souvent, les experts sont capables de dire ce qui n'est pas de l'IA mais ont plus de difficulté lorsqu'il s'agit de s'accorder sur ce que

l'IA est. Nous faisons donc face à une définition négative¹⁶, un type d'erreur dans l'élaboration d'une définition.

Section 2 : La RPA ou un domaine bien plus clair

L'observation précédente ne vaut pas pour la RPA. Notre analyse de données a montré que la conception de la RPA était beaucoup plus affinée auprès de nos interviewés. Il semblerait qu'ils s'accordent tous sur une seule et même conception : la RPA est un outil capable d'améliorer les processus sur des tâches répétitives et à peu de valeur ajoutée sans pour autant détenir un caractère intelligent. En effet, Augustin Borsu de BNP Paribas Fortis nous dit que « *les robots permettent de prendre le pas sur des tâches répétitives et pour lesquelles un faible niveau intellectuel est requis.* ». Orce Marinkovski, de la BGL BNP Paribas, rapporte que la RPA « *est déjà utilisée mais principalement sur des tâches répétitives, sans intelligence derrière.* ». Son collègue, Laurent Denis ajoute que « *la RPA pourrait améliorer le quotidien et qu'éventuellement vous pourriez mettre des gens sur des tâches à plus de valeur ajoutée ou autre part dans la banque* ».

Cependant, on entrevoit par moments des chevauchements entre IA et RPA. En d'autres mots, des outils composés de IA et de RPA. Comme constaté dans la section précédente, même si une conception de l'IA n'est pas partagée, nos interviewés étaient en mesure de distinguer lorsqu'un outil est composé de RPA seulement ou s'il contient de l'IA également. La perception de nos interviewés sur le fait que la RPA n'est pas associée à de l'intelligence à moins qu'elle soit complétée par des techniques plus poussées d'IA telles que le machine learning ou le deep learning rejoint également ce que nous disions en première partie de ce mémoire.

Nous avons également constaté un argument intéressant parmi un de nos interviewés. Pour le moment, la RPA est vue comme la nouvelle façon de programmer et d'implémenter des automatisations dans les processus. Or, Orce Marinkovski suggère une autre approche quant à l'utilisation d'outils RPA. Pour lui, la RPA est une béquille temporaire qui répond à un besoin et dont l'implémentation est rapide et facile, un MVP (« Minimum Viable Product ») en quelque sorte. Il argumente que la RPA ne doit pas modifier l'ensemble du processus et qu'elle n'est là que pour répliquer ce qui est fait manuellement par un utilisateur pour le faire automatiquement. Il explicite cet argument « *[modifier l'ensemble d'un processus via la*

¹⁶ Voir séminaire d'accompagnement du mémoire en gestion > E. Écrire > E1. Rédiger un mémoire (syllabus) (2020, p. 8)

RPA] ça peut être dangereux parce qu'on aura alors une dépendance d'une sous-couche, l'applicatif, et si lui évolue, il faut aussi faire évoluer la RPA. Donc, dans ce cas-là, on se retrouve dans une situation où ça coûte beaucoup plus cher. ».

Section 3 : Aperçu des approches IA et RPA des banques de notre échantillon

À la BGL BNP Paribas, nos interlocuteurs ont fait état de deux vecteurs pour des applications RPA et d'un département spécialisé en matière d'IA.

Pour l'IA, la BGL BNP Paribas s'est dotée, il y a quatre ans, d'un département appelé le Data Lab en charge de conduire des recherches sur le développement de modèles basés sur de l'IA. Ce département est une toute petite équipe composée de quatre à cinq personnes qui travaille principalement avec des chercheurs et des doctorants de l'Université du Luxembourg. Cependant, il a été noté par Laurent Denis qu'« *[il] n'y a pas de stabilité dans l'équipe donc c'est un peu la critique [...]. [Ils ont] du mal à avancer dans le temps parce que les personnes font du va-et-vient, ils sont là pour six mois puis quittent la banque et il faut recommencer presque à zéro.* ». Également, Laurent Denis émet quelques réserves : « *les outils statistiques qu'ils utilisent sont peut-être plus performants [...] mais avec ce que j'ai vu maintenant [...], j'ai de moins en moins confiance sur la présence d'IA au sein du data lab.* ».

Pour la RPA, la BGP BNP Paribas possède deux vecteurs. Le premier vecteur est une équipe responsable de la transition par l'automatisation dans la banque à l'aide d'outils RPA. Cette équipe est appelée le Center of Excellence Automation. Laurent Denis nous a fait savoir que cette équipe est en place depuis deux à trois ans et qu'elle est composée d'une dizaine de personnes. Il émet à nouveau une réserve : « *Ils ne sont pas à la pointe de la technologie mais bon ils se mettent dans les clous, enfin dans les starting blocks de la compétition.* ». Le second vecteur fonctionne différemment. C'est en réalité un système complètement décentralisé interne au département RISK de la BGL BNP Paribas où une personne compétente est directement à côté du métier et développe des solutions RPA pour automatiser les processus et les tâches du métier. En d'autres mots, la fonction risque s'entoure d'experts (en l'occurrence, un seul) qui a une vue directe sur le métier et les applications probantes à développer. On parle ici d'un fonctionnement complètement décentralisé dans la mesure où l'expert en question est interne au département risque, proche du métier. Cependant, le Data Lab et le Center of Excellence Automation sont également décentralisés par rapport au département IT mais ne sont pas aussi proches du personnel opérationnel, en tout cas pour le moment puisque la banque « *[fait] la*

promotion du concept agile depuis début janvier, ils veulent vraiment revenir à un mode de fonctionnement où ils vont détacher les gens de leur département pour les mettre en place dans ce qu'ils appellent une squad donc c'est vraiment une équipe dédiée à la mise en place, à l'aboutissement d'un projet. » (Laurent Denis).

À la BNP Paribas Fortis, nous avons distingué deux équipes, une spécialisée en IA et l'autre en RPA.

Il a été noté que l'IA s'inscrit dans le cadre de la gestion des données (« data management »), c'est-à-dire tout ce qui traite de la qualité des données, des nouveaux développements, *etc.* Autrement dit, ce qui relève de la norme BCBS 239 édictée par le Basel Committee on Banking Supervision dans le but de renforcer les capacités d'agrégation des données sur les risques et les principes internes de détection des risques (Olieslagers, 2020). Ruben Olieslagers indique que dans l'équipe data management, ils ont un gros pilier IA avec une « *vingtaine/trentaine d'experts* », surtout « *pour des applications crédits, fraudes ou compliance.* ». Augustin Borsu, responsable de cette équipe spécialisée en IA explique que l'objectif de cette équipe est d'accompagner l'intégration des projets IA dans les systèmes de la banque en définissant les processus et marches à suivre pour l'implémentation.

Au niveau RPA, Augustin Borsu mentionne que la BNP Paribas Fortis possède un département entier spécialisé en RPA qui tourne autour de dix use cases par an sur la robotique. Les use cases visent à définir la valeur ou l'utilité qu'un outil aura pour les personnes impliquées. Les objectifs de cette équipe sont de mettre en place un centre de compétences en robotique, de déployer un grand nombre de ces use cases, donc d'automatisations, et d'intégrer des capacités d'intelligence artificielle.

Section 4 : Éthique

Plus tôt dans ce mémoire, nous évoquions les aspects éthiques de l'IA. Notamment, nous avons parcouru la position d'Hawking qui appréhendait l'IA comme un domaine dont l'évolution serait soit positive, soit négative pour l'humanité. Toutefois, en tant qu'optimiste, il croit que nous pouvons développer l'IA pour le bien de l'humanité grâce à une conscience de ses dangers et des meilleures pratiques de management.

Marc Aguilar propose une position relativement similaire : « *c'est à l'humanité de mettre des guidelines de façon à ce que cette technologie soit utilisée dans un cadre qui crée de la valeur*

pour les êtres humains, et non pas qui supportent des développements négatifs. ». Cependant, il pose une question : *« L'évolution sera-t-elle contrôlable, toujours [suivre] ce que l'être humain souhaite qu'elle fasse, ou alors elle va nous échapper, devenir incontrôlable et autonome ? ».* Il ouvre donc le débat parce que, d'après lui, la première chose que l'intelligence artificielle non contrôlée cherchera à faire est d'éliminer l'être humain parce qu'il représente une double menace : sur la survie de la planète, et sur la survie de l'IA elle-même. Pas de panique non plus, il rappelle que nous en sommes encore loin et que l'intelligence artificielle est encore élémentaire aujourd'hui.

Un autre aspect éthique que nous avons abordé plusieurs fois est le risque de discrimination¹⁷. Nous avons montré que ce risque d'ordre éthique se produit soit lorsque les algorithmes respectent strictement les lois anti-discrimination sans utiliser de variables sensibles, soit lorsque les données de départ contiennent des biais. Sur ce dernier point, il a été noté que les deux banques de notre échantillon semblent conscientes de cet inconvénient. Augustin Borsu relate : *« on s'inquiète [...] du risque de faire continuer les préjudices et qu'ils soient renforcés. [...] En data science on dit garbage in garbage out : si les data ont un biais en entrée, alors elles auront un biais en sortie puisque les modèles tirent des conclusions basées sur les données. ».* L'aspect éthique sur les données en entrée est dès lors très considéré à la BNP Paribas Fortis. Cependant, Augustin Borsu mentionne également que ceci passe parfois par une création de modèles moins performants mais plus éthiques parce que des paramètres et données qui peuvent mener à de la discrimination ont été retirés du dataset de départ. Orce Marinkovski, pour la BGL BNP Paribas, argumente par l'exemple que la prise en compte de certains paramètres dans des systèmes d'IA devrait être interdite dans la mesure où certains paramètres peuvent conduire à des décisions discriminantes. Il va d'ailleurs un peu plus loin dans la réflexion en expliquant que des modèles basés sur un grand nombre d'informations, donc de données, influencent leur degré de prise de risque lorsqu'ils doivent prendre une décision, à tel point qu'on peut se retrouver avec une minimisation maximale discriminante du risque dans la mesure où certains acteurs économiques seraient écartés. Ceci, en retour, pourrait impacter les comportements de ces acteurs économiques qui n'agiraient plus de manière autonome dans le but d'entrer dans les critères de décision des modèles.

¹⁷ Notamment : Partie 1 > Section 1 > Sous-section 1.5 > Risques ; Partie 3 > Section 2 > Injustice et discrimination

Section 5 : Le cycle de gestion des risques

Nous le disons, la gestion des risques fonctionne de manière cyclique et est un processus itératif. Une des raisons pour lesquelles c'est un processus itératif est la réévaluation des technologies de sorte à implémenter les innovations bénéfiques à l'amélioration du processus de gestion des risques.

Au travers de nos entretiens, nous avons été en mesure d'identifier que la BNP Paribas Fortis était particulièrement sensible sur ce point. En effet, Ruben Olieslagers explique être membre du « New Activity Committee » en charge de prendre les décisions sur chaque nouvelle activité potentielle. Qui plus est, ce comité traite avec plusieurs fonctions : legal & tax, risk, compliance, finance, *etc.* De plus, il semblerait que la BNP Paribas Fortis montre une certaine ouverture sur le marché pour améliorer ses processus de gestion des risques puisque Ruben Olieslagers explique que la banque « [...] *regarde aussi ce qui a été développé en IA ailleurs par les Fintechs.* ». Il explique également qu'ils ont travaillé avec Accenture, une entreprise de conseil et de technologies « *spécialisée dans la robotic process automation.* ». Augustin Borsu mentionne aussi que la BNP Paribas Fortis fait du « market watch », c'est-à-dire que, tous les trimestres, la banque invite des Fintechs qui viennent proposer leurs produits. Ceux qui sont jugés suffisamment intéressants sont retenus et des partenariats sont envisagés. Finalement, la banque travaille également avec des universités.

Dans une moindre mesure, la BGL BNP Paribas montre également une certaine ouverture sur le marché au niveau de l'IA puisque l'équipe spécialisée dans cette technologie travaille avec des chercheurs de l'Université de Luxembourg. Également, on observe que la banque améliore sa gamme d'outils en interne en termes de RPA d'après Laurent Denis, qui rapporte qu'« *ils viennent [...] d'acquérir des logiciels OCR un peu plus performants que ceux qu'ils avaient auparavant.* ». Cependant, lorsqu'on aborde la sous-traitance d'activités IA et RPA, via des Fintechs par exemple, il semble que les avis sont partagés au sein de la BGL BNP Paribas. Laurent Denis mentionne que la question des partenariats avec les Fintechs a été évoquée en 2017-2018 mais n'avait pas été retenue et ce pour deux raisons : « *les fintechs sont peu solides [...] et on n'a pas non plus volonté de les acheter.* ». Néanmoins, il explique que ceci est un feedback qui date de 2018 qui a pu évoluer depuis et suggère d'en parler avec Marc Aguilar, membre du comité de direction, « *qui a participé à des discussions dont je ne suis même pas au courant* », note Laurent Denis. D'autant plus que Marc Aguilar, lui, mentionne des collaborations avec des acteurs tiers, notamment pour l'acquisition de données et pour accéder

à des personnes aux connaissances pointues et compétentes dans le domaine. Orce Marinkovski pose également une autre remarque : pour lui, sous-traiter de la RPA ne fait pas sens parce que la plus-value de la RPA réside dans la connaissance métier, qui n'est pas présente chez un externe. Au niveau de l'IA cependant, il explique que c'est plus intéressant parce qu'elle « *exige une certaine maîtrise technique [...] pour bien l'implémenter.* ».

Cependant, des considérations générales se présentent sur l'ouverture vers le marché pour une banque. Ce n'est en effet pas chose aisée pour plusieurs raisons. Premièrement, une banque est une organisation très conservatrice comme le rappelle Ruben Olieslagers, impliquant une certaine prudence lorsqu'il s'agit de s'ouvrir au marché. Deuxièmement, les données bancaires sont extrêmement sensibles et il est parfois compliqué de traiter avec des acteurs tiers pour des questions d'accès aux données, nous dit Augustin Borsu. Finalement, l'ouverture est un choix de gouvernance. Il n'est donc pas, dans tous les cas et pour toutes les technologies, souhaitable de passer le marché au crible.

D'autres points de friction ont été pointés par nos interviewés et sont en ligne avec la section sur les défis principaux qui précède. Effectivement, quatre aspects majeurs ont été mis en évidence à la suite des entretiens lorsqu'il s'agit d'adopter des techniques d'IA et de RPA dans le but d'améliorer les processus.

En premier lieu, il a été montré par plusieurs de nos interviewés que l'approche est globalement top-down et pas bottom-up, c'est-à-dire que la volonté pour développer des applications basées sur l'IA et la RPA vient du haut de la hiérarchie plutôt que du bas. À ce sujet, Ruben Olieslagers croit que « *C'est rare qu'il y ait une approche bottom vers le top, c'est plutôt l'inverse, c'est imposé au final.* ». En cause, la difficulté pour les gens de penser out of the box et d'identifier les potentialités des solutions IA et RPA comme le mentionne Laurent Denis : « *globalement tu restes dans ta zone de connaissance, tu n'anticipes pas ce que la RPA pourrait t'apporter sur d'autres processus.* » ; ou Orce Marinkovski : « *si les gens se limitent à l'environnement de leur propre banque, ils n'ont pas de vue sur toute la problématique de la place financière. Ce sera plus difficile pour suivre technologiquement et être au top des évolutions.* ». Pour contrecarrer ce problème, Laurent Denis suggère de créer des sessions de travail conduisant les gens à sortir de leur zone de confort.

Deuxièmement, adopter de nouvelles applications IA et RPA, nous l'avons dit à maintes reprises, notamment avec Calzolari (2021, p. 15), réduit la quantité de tâches répétitives pour

les humains et accélèrent les processus. Cependant, cela ne veut pas dire que ces applications ne vont pas susciter de résistance au changement. Laurent Denis rapporte : « *le changement est encore un peu compliqué, chacun protège encore un peu ses équipes, on n'a pas identifié au sein de la banque de programmes, de processus qui pourraient complètement être informatisés ou robotisés* ». Ruben Olieslagers émet une observation allant dans cette direction : « *la volonté du data management est parfois plus élevée que la volonté du business pour intégrer des technologies IA.* ». Augustin Borsu mentionne également que le défi est de réussir à convaincre les gens des bienfaits de ces technologies.

Un troisième point de friction réside dans les difficultés à intégrer des nouveaux processus dans les systèmes IT existants. Augustin Borsu note qu'il est parfois compliqué d'intégrer leurs projets parce que les data scientists travaillent plutôt avec les langages R et Python alors que le département IT utilise le langage Java. Marc Aguilar reprend la même idée : « *Je pense qu'un problème c'est de faire coopérer ou intégrer cette technologie dans la technologie classique.* ».

Un quatrième et dernier aspect compliquant l'adoption d'applications IA et RPA est la nécessité d'avoir des personnes très compétentes. En effet, Ruben Olieslagers mentionne qu'un des soucis de ces technologies est que, lorsqu'elles sont développées en interne, il faut toujours garder des personnes compétentes pour pouvoir monitorer et suivre ces applications. Augustin Borsu parle de garder des experts qui savent comprendre et gérer ces technologies et savent ce qu'elles font, sinon on s'expose au « *risque qu'un modèle ne soit pas suffisamment compris, que la provenance des données ne soit pas comprise, etc.* ».

Section 6 : Impact de la gouvernance d'entreprise

Grâce à nos entretiens, nous pouvons mettre en avant l'impact de la gouvernance sur une organisation. D'ailleurs, dans la section précédente, nous mentionnons déjà que l'ouverture vers le marché pour une banque est un choix de gouvernance.

Il a été démontré dans nos entretiens que la gouvernance motive également d'autres choix. Notamment, nos interviewés rapportent qu'en termes d'applications IA et RPA, la volonté du groupe BNP Paribas est de se focaliser sur l'automatisation dans les processus existants. Augustin Borsu explique : « *La priorité est plutôt sur l'étendue des services existants, peu sur la création de nouveaux produits. Donc l'objectif est d'améliorer les outils actuels plutôt que de s'attaquer à la création de nouveaux outils.* ». Marc Aguilar suggère également que « *Paris a poussé les choses* », Paris étant la ville dans laquelle le siège du groupe BNP Paribas se trouve.

Ceci entre dans le cadre des trois premières catégories d'opportunités de l'IA et la RPA liées à l'amélioration et identifiées par l'EBF (2019, pp. 6-7) dont nous avons discuté plus tôt. Cependant, cela ne laisse pas pour autant de côté la quatrième catégorie sur la création de nouvelles opportunités, du moins à la BNP Paribas Fortis, puisque nos interviewés de cette banque ont notamment mentionné le développement d'une application pour la gestion de portefeuilles. Toutefois, il n'a pas été fait mention d'autres perspectives conduisant à la création de nouvelles opportunités.

Un autre aspect de gouvernance se retrouve lorsqu'Augustin Borsu aborde le « data risk appetite ». Nous avons vu ce qu'est l'appétit du risque : « *The aggregate level and types of risk a financial institution is willing to assume within its risk capacity to achieve its strategic objectives and business plan.* » (FSB, 2013, p. 3). Il va de soi qu'en tant de banque, il convient de définir également l'appétit du risque lié aux données. À la BNP Paribas Fortis, nous constatons que l'appétit du risque lié aux données défini a des implications. Augustin Borsu explique qu'il est parfois compliqué de faire appel à des sous-traitants pour des raisons d'accès aux données ce qui conditionne parfois le choix d'utiliser des outils développés en interne parce que le « *data risk appetite de la banque [...] est relativement limité.* ». Cependant, il précise que, si l'utilisation des données n'est pas requise, ils peuvent faire appel à des tiers. À la BGL BNP Paribas, on constate une approche un peu différente avec Marc Aguilar lorsqu'il s'agit d'aborder l'appétit du risque lié des données : « *avec les partenariats on a ajusté les méthodes pour préparer les données de façon que la confidentialité des données reste garantie.* ».

Finalement, un dernier aspect de gouvernance, cette fois plutôt lié au fait que les banques de notre échantillon font partie d'un groupe, sont les possibilités de synergies. En effet, nos interviewés, à plusieurs reprises, expliquent qu'en faisant partie d'un groupe, des outils IA et RPA développés dans une des branches, peuvent être réutilisés dans les autres. Toutefois, chaque branche du groupe évolue dans un environnement macroéconomique différent et construit des modèles selon son propre environnement, il n'est donc parfois pas possible de réaliser des synergies au niveau des outils lorsqu'ils sont façonnés à l'image de cet environnement.

Section 7 : Les données

Un point de divergence entre la BGL BNP Paribas et la BNP Paribas Fortis sont les données. En effet, à la BGL BNP Paribas, notamment avec Marc Aguilar et Orce Marinkovski, il a été

fait mention de deux inconvénients. Premièrement, Marc Aguilar explique que le gros problème des algorithmes ce sont les données, c'est-à-dire leur qualité, (consistance de la donnée, donnée unique, mise à jour de la donnée, *etc.*) leur disponibilité, leur historique qui doit être assez profond et les capacités d'extraction des données. Il finit ceci par dire que ce sont ces aspects sur les données qui coûtent cher, environ 80% des coûts, alors que l'algorithmie ne coûterait que 20%. Deuxièmement, et c'est là qu'est la divergence avec la BNP Paribas Fortis, Orce Marinkovski mentionne que « *la masse de données pour une vraie IA au Luxembourg, ce n'est pas là. En Belgique ou en Italie, ils ont des volumes de données plus conséquents pour permettre à une IA d'apprendre.* ». À la BNP Paribas Fortis, la question de la qualité des données est évidemment présente également. Cependant, il semblerait qu'ils aient une quantité de données suffisante pour développer des applications IA et RPA, comme le dit Ruben Olieslagers : « *l'avantage, c'est qu'on a de grosses bases de données.* ».

Un des avantages de la RPA en termes de qualité et quantité de données est que la RPA est un vecteur pour l'acquisition de données d'une part, et une garantie de qualité d'autre part. La RPA en ce sens peut contribuer à l'évolution de l'IA.

Section 8 : Applications IA et RPA dans les banques interrogées

Nous allons dans cette section dresser l'inventaire des applications IA et RPA dans les banques que nous avons interrogées. Nous allons nous concentrer sur les applications en crédit, fraude et conformité puisque ce sont les risques que nous considérons dans ce mémoire. Toutefois, nos entretiens ont montré que d'autres perspectives sont à l'œuvre ou sont envisagées (e.g : utilisation de chatbots, solution de trading, outils de gestion de portefeuille, développements en marketing, *etc.*) et corroborent certaines des tendances que nous avons identifiées plus tôt. L'objectif n'est pas d'être exhaustif étant donné que nos interviewés n'ont très certainement pas mentionné toutes les applications en cours d'utilisation, de développement, ou à l'étude mais de mettre en lumière ce qui est ressorti de nos entretiens. L'annexe 16 (p. 154) propose un tableau synthétique des applications que nous allons mettre en évidence.

Sous-section 8.1 : BGL BNP Paribas

Crédit

En crédit, nous avons distingué plusieurs applications dont certaines encore en développement et d'autres au stade de discussion.

Plus tôt, nous parlions du credit scoring et c'est dans ce cadre que s'inscrivent les deux applications que nous allons détailler maintenant, l'une est basée sur de l'IA et l'autre sur de la RPA. En effet, le credit scoring comme nous le disions se base sur des données bancaires et, pour un score plus précis, sur des données externes. Cependant, pour le second cas, l'application n'a pas trait aux données externes mais bien aux données bancaires.

Laurent Denis rapporte que le Data Lab, le département spécialisé en intelligence artificielle de la BGL BNP Paribas, a développé un nouveau modèle de scoring pour les PME. Cet outil a permis d'affiner les variables utilisées dans le modèle et au final, d'octroyer un score plus précis. On peut émettre l'hypothèse que des données alternatives ont été utilisées mais cela n'a pas été mentionné durant nos entretiens.

Pour appréhender l'application RPA, quelques éléments conceptuels et contextuels sont à aborder. Les données financières prises en compte pour réaliser un credit scoring d'une personne morale incluent notamment les états financiers de celle-ci. Ces états financiers doivent ensuite être encodés dans les outils de gestion de clients de la banque. Au Luxembourg, le dépôt des comptes annuels se fait au Registre de Commerce et des Sociétés (RCS). Or, ces comptes annuels ne respectent pas un schéma standard comme c'est le cas en Belgique par exemple. « *La raison est historique au Luxembourg : absence d'une centrale des bilans complète.* », explique Laurent Denis. De fait, des tas de types de comptes annuels se retrouvent déposés au RCS, tous avec des particularités plus ou moins grandes. Dès lors, ceci complexifie l'encodage qui est déjà une tâche manuelle, répétitive et à faible valeur ajoutée.

Fort de ce constat, le département RISK et plus particulièrement la personne en charge des automatisations des processus a développé un outil doté de RPA et de Reconnaissance Optique de Caractères ou Optical Character Recognition (OCR). L'OCR est définie comme suit : « *technique qui, à partir d'un procédé optique, permet à un système informatique de lire et de stocker de façon automatique du texte dactylographié, imprimé ou manuscrit sans qu'on ait à retaper ce dernier.* » (Futura Tech, 2021). Dans un premier temps, l'OCR « *développée à partir d'expressions régulières [permet] de traiter des états financiers pour les rendre lisibles à travers un fichier Excel.* », explique Laurent Denis. Dans un second temps, « *[on] passe la couche RPA qui ira encoder les informations contenues dans le fichier Excel dans les outils de back office.* », toujours selon Laurent Denis. Cet outil peut donc être considéré comme une aide au middle office puisqu'il permet de transformer une tâche insignifiante mais chronophage et

énergivore en une tâche complètement automatisée et pour laquelle aucune intervention humaine n'est requise.

Une autre application basée sur de l'IA en développement depuis quelques années à la BGL BNP Paribas est un « *outil de validation automatique des dépassements sur compte courant* » d'après Laurent Denis. Marc Aguilar détaille cet outil. Auparavant, certaines transactions étaient bloquées par manque de fonds sur un compte courant. Cependant, il arrive qu'un compte soit vide mais que la personne ou l'entité possède d'autres comptes qui ne le sont pas. Un outil IA est désormais en développement pour gérer ces blocages de transaction. L'outil permettrait de connecter les systèmes et d'y injecter de l'intelligence, c'est-à-dire exécuter une transaction si le client dispose d'autres fonds sur un autre compte de sorte à ce que le blocage initial ne retombe pas sur le gestionnaire de la relation client en charge qui devait auparavant visualiser le problème et libérer les fonds manuellement comme l'explique Marc Aguilar.

Trois autres opportunités en termes d'IA ont été mentionnées. Premièrement, Marc Aguilar suggère qu'avec l'IA, il y a possibilité de proposer de nouveaux crédits aux clients (surtout des crédits à la consommation), notamment grâce à un profil client bien établi. Cependant, il ne savait tout simplement pas si c'est déjà en application au Luxembourg. Deuxièmement, Marc Aguilar nous a fait part d'une opportunité sur la tarification des clients et la capacité à savoir ce qui s'adapte le mieux pour eux en termes de taux appliqué sur un crédit par exemple. Il n'est pas entré plus dans le détail. Finalement, Laurent Denis note que la RPA pourrait être utile dans le cadre des demandes de crédit, et ce en préparant des documents et en réalisant des encodages. Néanmoins, il n'est pas plus exhaustif.

Fraude

Dans le cadre des activités de détection de fraude, la BGL BNP Paribas s'est dotée d'un outil basé sur de l'intelligence artificielle. Marc Aguilar explique : « *l'algorithme va [...] donner une probabilité de fraude. Une fois que tu as cette info, tu prends la transaction et tu décides ou pas de l'exécuter. Si tu estimes que le risque de fraude reste assez faible, grâce à la probabilité qui a été donnée, tu autorises la transaction. Mais si tu considères que non, tu bloques la transaction.* ». On remarque que cet outil n'est pas complètement autonome puisqu'il requiert une intervention humaine pour prendre la décision finale. Cependant, il a été couronné de succès d'après Laurent Denis puisqu'il « *[a été] monétisé [...] sur la place du Luxembourg, [...] c'est quelque chose qui a été mis en place au sein de la BGL et qui a été vendu à des partenaires,*

enfin à des autres institutions bancaires au Luxembourg. ». Laurent Denis note que cet outil a eu des répercussions sur le plan marketing, notamment en termes d'image de la banque, et qu'il est « *éventuellement plus performant [que les outils de détection de fraude existants]* ».

Conformité

Au niveau de la conformité, Orce Marinkovski nous dit que « *oui, c'est possible de mettre en place des processus répétitifs pour vérifier que toutes les opérations soient conformes et que la RPA [peut permettre de] mettre en place les contrôles pour assurer la conformité* ». Ce qu'ils ont d'ailleurs fait dans pour les activités Know Your Transactions (KYT) où une IA a été développée. Cet outil IA permet d'établir le profil du client selon différents paramètres (montants, activités, paiements in et out, etc.) et d'identifier si les transactions sont conformes par rapport à ce profil comme l'explique Marc Aguilar. Il note également les bienfaits de cet outil par rapport aux processus classiques faits par des humains : « *le travail est mieux fait et on a une meilleure garantie, on a une algorithmie dans laquelle on peut prouver quels sont les critères [de décision]*. ».

Sous-section 8.2 : BNP Paribas Fortis

Au préalable, il est intéressant de noter les zones d'applications et opportunités de la BNP Paribas Fortis. En termes d'amélioration de l'expérience client, il a été fait mention du développement d'un chatbot capable de répondre à des demandes relativement simples (demande de carte, gestion de carte en cas de perte, etc.), notamment dans le but d'éliminer de plus en plus l'étape agence d'après Ruben Olieslagers. Cependant, Ruben Olieslagers rapporte qu'au niveau de l'IA, « *c'est surtout pour des applications crédits, fraudes ou compliance*. ».

Crédit

Au niveau crédit, Ruben Olieslagers mentionne que les modèles de scoring ont été développés dans les années 90 jusqu'en 2007. Ces modèles fonctionnent en collectant des données et en y appliquant une régression ou une analyse discriminante linéaire. Aujourd'hui, la banque souhaite aller de l'avant en développant des modèles plus performants basés sur de l'intelligence artificielle. Ruben Olieslagers nous dit : « *Maintenant, on commence à réfléchir pour IA, mais ce sont des tests pour une population comme retail banking où on a des bases de données de grande taille*. ». On voit d'ailleurs à nouveau la nécessité d'une grande quantité de données pour développer des modèles d'IA.

En termes de RPA, Augustin Borsu et Ruben Olieslagers ont expliqué que cette technologie devrait permettre la reconnaissance de documents et la possibilité d'établir des documents qui entrent dans le cadre de la gestion des crédits (e.g. : des templates de demande de crédit).

Fraude

BNP Paribas Fortis utilise des outils de détection de fraude basés sur des technologies IA. Cependant, nos entretiens n'ont pas été plus extensifs sur le sujet.

Conformité

En termes de conformité, nous avons distingué deux applications, la première déjà en fonction et la seconde est en cours d'analyse.

Le premier outil est un système de reconnaissance de clients à l'aide de documents et est utilisé dans le cadre des activités Know Your Transactions. Il est qualifié d'Augmented Intelligence¹⁸ par Augustin Borsu. Cet outil permet de comparer les données de documents avec celles de la banque et d'établir s'il y a une correspondance. L'outil donne ensuite un degré de certitude par rapport à cette correspondance. Dès lors, s'il y a un degré de correspondance suffisamment élevé, l'outil fonctionne de manière autonome. Si le degré de correspondance est trop faible ou qu'il conclut à des incertitudes sur cette correspondance, alors il y a une intervention humaine. Augustin Borsu note : « *Ce n'est pas simplement un feedback à l'humain, c'est-à-dire que l'humain n'intervient que si le modèle rencontre une incertitude mais si la reconnaissance des données trouve un match dans les données de la banque, l'humain n'est pas requis.* ». Pour établir une correspondance, l'outil utilise différents paramètres : nom du client, code postal, date de naissance, etc.

Le deuxième outil IA, en cours d'analyse, relève également de la conformité. Il s'inscrit dans le cadre de la vente de produits et est un outil « speech to text ». Augustin Borsu explique que, lorsqu'on vend un produit de crédit ou d'assurance par exemples, le vendeur a l'obligation de présenter certaines informations. Pour le moment, certains (longs) appels sont sélectionnés et une personne va écouter ces appels pour vérifier la conformité des informations mentionnées. L'outil permettra de réaliser cette étape, c'est-à-dire l'écoute et l'analyse sur la conformité des

¹⁸ https://en.wikipedia.org/wiki/Intelligence_amplification

informations. L'outil signalera ensuite les appels pour lesquels il y a un problème et un humain repassera derrière pour vérification.

Conclusion

Puisque nos deux banques font partie du même groupe, nous pouvons commencer par aborder les avancées de BNP Paribas sur les thématiques IA et RPA. Nous continuerons par les points de divergence et les aspects convergents des banques de notre échantillon. Finalement, nous évaluerons les banques sur leurs applications IA et RPA pour les risques de crédit, fraude, et conformité.

En tant que grande banque européenne, BNP Paribas a pris relativement tôt conscience des enjeux liés aux nouvelles technologies. C'est un point qui s'est fait ressentir dans nos entretiens lorsqu'ils abordaient le groupe BNP Paribas. En effet, Ruben Olieslagers relate que BNP Paribas est précurseur sur ces technologies, notamment en expliquant que le Chief Data Officer du groupe a mis en place une équipe IA de 200 personnes avec environ 40 experts en IA et d'autres personnes largement ouvertes sur les opportunités liées à l'IA. Marc Aguilar parle d'une « *équipe assez pointue à Paris* ». Comme nous le disions plus tôt, la volonté du groupe est de se focaliser sur l'automatisation dans un premier temps plutôt que sur la création de nouveaux produits. Marc Aguilar pousse la réflexion un peu plus loin en disant que le groupe est certainement dans le premier tiers en termes de place sur le marché en Europe pour ces technologies. Cependant, il mentionne « *BNP est en avance en Europe, mais par rapport aux États-Unis, l'Europe a du retard.* », ce qui corrobore les résultats de Calzolari (2021, p. 35) lorsqu'il explique que l'Europe a du retard sur les développements d'applications IA par rapport à d'autres pays.

Au travers de nos entretiens, nous avons pu constater que la BNP Paribas Fortis montre des signes d'avancement plus étendus en termes d'IA et de RPA que la BGL BNP Paribas. En effet, nous avons montré que les départements respectifs pour ces banques ne sont pas au même stade. Premièrement, les équipes IA et RPA à la BGL BNP Paribas sont plus petites et ont été mises en place plus tard alors que la BNP Paribas Fortis a mis en place des équipes plus tôt avec plus de personnel. À ce sujet, Orce Marinkovski pense que « *l'intelligence artificielle, je dirais qu'à ma connaissance, elle n'est qu'à un niveau d'étude, donc d'étude de « Comment on peut l'utiliser ?* ». ». Laurent Denis tente d'expliquer pourquoi : « *on n'a pas des budgets pour engager 20 personnes comme tu l'aurais chez Fortis.* ». Il corrobore d'ailleurs notre constat en

disant que la « *BNP Paribas Fortis ça a toujours été un peu le précurseur dans la matière et notamment l'IA.* ». Cependant, il montre également des signes encourageants lorsqu'il explique que l'objectif pour 2021 est de recruter quelqu'un en interne pour l'équipe IA, notamment dans le but d'ajouter un peu plus de stabilité dans l'équipe qui actuellement fait appel à des chercheurs de l'Université de Luxembourg qui ne sont généralement là que pour quelques mois. Également, il mentionne que la BGL BNP Paribas vise à fonctionner de manière agile ce qui devrait étendre les possibilités d'amélioration des processus grâce à l'IA et la RPA.

Un autre point de convergence, nous l'avons vu, est l'ouverture vers le marché et la façon dont les deux banques abordent leur appétit pour le risque lié aux données. La BNP Paribas Fortis semble montrer une ouverture vers le marché plus accrue dans la mesure où elle traite avec plus d'acteurs tierces, notamment en travaillant avec des Fintechs, en faisant du market watch, et en réalisant des screenings sur le marché. Augustin Borsu la positionne comme une « smart follower », c'est-à-dire qu'ils évaluent ce qui se trouve sur le marché et sélectionnent les opportunités pour lesquelles le rendement est le plus intéressant. La BGP BNP Paribas, quant à elle, montre également des signes d'ouverture sur le marché mais dans une moindre mesure, notamment parce que la piste des Fintechs avait été écartée en 2017-2018 même si Marc Aguilar mentionne quelques partenariats avec des acteurs tiers. Un lien potentiel entre cette relativement faible ouverture et le constat de Calzolari est possible. En effet, il a montré que les acteurs importants du secteur financier développent leurs solutions IA en interne parce que les services tiers peuvent représenter une source de risque (Calzolari, 2021, p. 34).

Finalement un autre point sensible qui permet de distinguer nos deux banques est la masse critique des données. En effet, nos interviewés ont rapporté que, pour développer des outils d'IA robustes, il était nécessaire de posséder une grande quantité de données. Or, la BGL BNP Paribas évolue dans un environnement plus restreint que la BNP Paribas Fortis, elle ne possède donc pas de volumes de données suffisamment importants sur certaines populations de clients pour développer des modèles d'IA. À la BNP Paribas Fortis, nous notons que les bases de données sont plus fournies, ce qui permet des possibilités de développements élargies.

Au niveau des convergences, nous avons pu identifier que les deux banques étaient amplement conscientes des risques éthiques sous-jacents à l'IA. Notamment, il a été fait mention de la grande prudence à avoir par rapport aux biais inclus dans les données en entrée qui peuvent conduire à des conclusions discriminantes en sortie. Ceci est bien résumé par l'aphorisme « garbage in, garbage out » utilisé par Augustin Borsu.

Également, nous remarquons que l'approche retenue pour promouvoir les développements IA et RPA est une approche top-down. Il en résulte que ces applications sont mises en œuvre à l'initiative du management, voire sont dues à une pression du groupe. Cependant, nous expliquions qu'il était parfois compliqué de sortir de son environnement quotidien pour penser à des solutions plus performantes. Laurent Denis recommande la mise en place de sessions de travail « out of the box ».

Un autre aspect récurrent est la résistance au changement. En effet, les équipes opérationnelles, pourtant celles pour lesquelles les possibilités sont parmi les plus grandes, ne semblent pas toujours enclines à inclure ces nouvelles technologies dans leurs méthodes de travail. Il convient donc de supporter les efforts de communication pour convaincre les personnes impliquées des bienfaits de ces technologies. Sur ce point, Calzolari (2021, p. 31) propose aux institutions financières d'être transparentes sur les données utilisées afin de susciter l'acceptation par le public.

L'intégration de nouveaux processus et nouvelles technologies dans les processus existants est un autre défi pour ces deux banques. En effet, il est souhaitable d'harmoniser les outils informatiques utilisés pour l'IA et RPA avec les départements IT pour faciliter les intégrations.

Finalement, ces technologies nécessitent des experts à la pointe et présents pour assurer le monitoring et le suivi. Ce point a fait l'objet de plusieurs préoccupations dans la mesure où il est compliqué de retenir des experts à la pointe capables d'assurer ces tâches, ou même de les engager, ce qui en soi, est encore un autre défi comme le dit Ruben Olielsagers.

Concernant les applications IA et RPA rapportées par nos interviewés, nous constatons que la BGL BNP Paribas a mentionné plus d'applications IA et RPA sur le risque de crédit alors que la BNP Paribas Fortis semble plutôt axée sur le risque de conformité.

Nous notons également des convergences vers des améliorations des modèles de credit scoring (risque de crédit) et des applications déployées dans le cadre des activités Know Your Transactions (risque de conformité). En ce qui concerne la fraude, les deux banques utilisent des outils IA de détection de fraude mais nos entretiens n'ont pas permis d'entrer dans les détails.

Au niveau de la RPA, nous remarquons que les applications sur cette technologie sont principalement des automatisations pour réduire la quantité de tâches répétitives à faible valeur ajouté et pour améliorer et accélérer les processus opérationnels.

Enfin, nous remarquons que les deux banques mentionnent des applications IA et RPA soit en développement, soit en discussion. Une évaluation ultérieure pourrait montrer une quantité d'applications supérieure sur cet échantillon.

CONCLUSION

Ce mémoire avait pour objectif d'étudier les tendances et défis principaux de l'IA et de la RPA sur les risques de crédit, fraude, et conformité sur les places financières belge et luxembourgeoise. Pour ce faire, nous avons, dans un premier temps, posé les bases de ce que sont l'IA, la RPA, la gestion des risques et sa taxonomie, et l'état actuel des avancées et défis en matière d'IA et de RPA. Dans un second temps, nous avons conduit des entretiens semi-directifs avec des experts sur les technologies IA et RPA dans deux banques européennes.

Quelques limites doivent d'abord être considérées. Premièrement, malgré nos efforts pour obtenir d'autres entretiens, notre échantillon est relativement restreint et ne permet pas de généraliser nos résultats sur l'ensemble des places financières belge et luxembourgeoise. Toutefois, si l'affirmation suivante : « *nous sommes dans le premiers tiers [en matière d'IA et de RPA]* », posée par Marc Aguilar au sujet du groupe BNP Paribas se veut réaliste, nous pouvons supposer que nos résultats forment déjà une bonne contribution au regard de la revue de la littérature.

Une deuxième limite est que nous n'avons pas eu l'occasion de nous entretenir avec un spécialiste RPA au sein de la BNP Paribas Fortis. Les observations et applications applicables strictement à la RPA semblent donc relativement pauvres. Notamment, nous expliquions dans la partie précédente que la BNP Paribas Fortis semble plus avancée que la BGL BNP Paribas sur ses développements IA et RPA. Or, l'inventaire des applications ne retranscrit pas complètement ce résultat.

Troisièmement, nous n'abordons pas les tendances et défis liés à ces technologies sous le point de vue d'organes régulateurs ni d'autres institutions financières comme les compagnies d'assurances. Une étude plus approfondie devrait également traiter le sujet sous ces angles et avec différents acteurs du secteur financier.

Concernant nos résultats, nous avons montré que l'intelligence artificielle reste un domaine abstrait en substance, même pour des experts en la matière qui la qualifie selon une, voire des définitions négatives, c'est-à-dire en termes de ce qu'elle n'est pas. La RPA, quant à elle, semble être un domaine beaucoup plus clair. La distinction s'impose généralement sur le caractère intelligent, autoapprenant, et autocorrecteur de l'IA qui n'est pas présent pour la RPA.

Plusieurs aspects sur les données ont été observés. Premièrement, les développements d'outils basés sur de l'IA nécessitent une masse critique de données, sans quoi, il n'est pas possible de construire des outils robustes. Deuxièmement, la qualité des données est primordiale pour s'assurer de l'absence de biais qui conduisent à des décisions discriminantes et ainsi développer des outils éthiques. La RPA peut supporter le développement d'outils d'IA dans la mesure où elle est une technologie capable d'acquérir des données en quantité et de qualité.

Afin de rester maître de la situation quant à l'évolution de l'IA, il est nécessaire (et même souhaitable) d'établir des lignes directrices et des cadres pour les développements en IA, sans quoi cette technologie pourrait devenir incontrôlable et, dans des scénarios extrêmes, écarter l'humain de la planète. La Commission européenne a emboîté le pas dans cette direction en proposant de nouvelles règles et actions pour l'excellence et la confiance dans l'intelligence artificielle¹⁹. Toutefois, en l'absence de réglementations précises et contraignantes, les banques se doivent de développer leur propre cadre de gestion de l'IA et de la RPA.

Les banques sont des organisations très conservatrices relativement peu adeptes de l'ouverture vers le marché, notamment pour des questions de sensibilité des données bancaires. Cependant, nous pensons qu'il est légitimement souhaitable de favoriser les partenariats pour plusieurs raisons. Tout d'abord, l'anonymisation des données n'est pas chose nouvelle et les paramètres sensibles des données bancaires ne sont de toute façon que peu utilisés. Les moyens pour parvenir à des situations positives pour les banques et leurs partenaires semblent disponibles et ne devraient plus représenter un tel frein aujourd'hui selon nous. De plus, les partenariats permettent de s'entourer d'experts et suggèrent des effets bénéfiques pour les deux parties. Ceci répondrait partiellement à un point de friction de l'IA et de la RPA sur l'acquisition et la rétention de personnel compétent. Une piste potentielle dans ce domaine est l'achat de Fintechs.

Nous soutenons également qu'il est souhaitable d'harmoniser les processus de développements IA et RPA pour faciliter les intégrations dans les systèmes existants. Également, dans l'objectif de favoriser les développements IA et RPA, il semble opportun de réaliser des efforts de communication auprès de toutes les parties prenantes (et particulièrement du personnel opérationnel) de sorte stimuler une approche bottom-up peu présente à ce jour mais potentiellement plus valorisante et mieux acceptée.

¹⁹ https://ec.europa.eu/commission/presscorner/detail/en/IP_21_1682

Nous pouvons également mettre en évidence que les applications déployées aujourd'hui sont celles pour lesquelles les rendements sont les plus intéressants et c'est un des aspects qui conditionne les tendances d'aujourd'hui.

Nous avons montré qu'en termes de gestion du risque de crédit, les modèles de credit scoring sont des zones propices pour développer des applications IA. Le risque de fraude semble avoir été un des premiers risques sur lequel ont été déployés des outils d'IA. Le risque de conformité semble pouvoir être fortement géré à l'aide d'applications IA et RPA dans la mesure où la conformité relève de règles et standards établis et pour lesquels l'étendue des automatisations sont grandes.

Finalement, vu la propension de ces technologies à devenir des éléments récurrents des modèles d'entreprise des banques dans les années à venir, nous suggérons la création d'évaluations à intervalles réguliers des outils IA et RPA et des audits annuels internes et externes sur ces technologies.

BIBLIOGRAPHIE

OUVRAGES

BESSIS, J. (2011). *Risk management in banking* (3è éd.). Chichester, UK: John Wiley & Sons.

CERRADA, K., DE RONGÉ, Y., DE WOLF, M., GATZ, M. (2011). *Comptabilité et analyse des états financiers* (3è éd.). Bruxelles : De Boeck.

CHAPMAN, R. J. (2011). *Simple tools and techniques for enterprise risk management*. New York, NY : John Wiley & Sons. En ligne <https://books.google.be/books?id=yosQeW8GcrQC&printsec=frontcover&hl=fr#v=onepage&q&f=false>

CHARTERED INSTITUTE OF MANAGEMENT ACCOUNTANTS (CIMA). (2008). *Fraud risk management: A guide to good practice*. London, UK : CIMA. En ligne https://www.cimaglobal.com/Documents/ImportedDocuments/cid_techguide_fraud_risk_management_feb09.pdf.pdf

CULP, C. L. (2002). *The risk management process: Business strategy and tactics* (Vol. 103). New York, NY: John Wiley & Sons. En ligne <https://books.google.be/books?id=2A81gjG9swMC&printsec=frontcover&hl=fr#v=onepage&q&f=false>

DHAENE, J., VANDUFFEL, S. & GOOVAERTS, M. J. (2008). Comonotonicity. In E.L. Melnick & B.S. Everitt (Eds.), *Encyclopedia of quantitative risk analysis and assessment*. doi : <https://doi-org.proxy.bib.ucl.ac.be/2443/10.1002/9780470061596.risk0341>

HUNT, V. D. (1983). *Industrial robotics handbook*. New York, Industrial Press Inc. En ligne <https://books.google.es/books?id=fHZTIZ8K-IUC&hl=fr>

KOK, J. N., BOERS, E. J. W., KOSTERS, W. A., VAN DER PUTTEN, P., POEL, M. (2009) *Artificial intelligence: definition, trends, techniques and cases*. Oxford, EOLSS Publishers/ UNESCO. En ligne https://books.google.es/books?id=v_jhDAAAQBAJ&printsec=frontcover&hl=fr&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false

LAM, J. (2014). *Enterprise risk management: From incentives to controls* (2è éd.). New York, NY : John Wiley & Sons.

LESSAMBO, F. I. (2020). *The U.S. banking system – Laws, regulations and risk management*. Cham, Suisse : Palgrave Macmillan. doi : https://doi-org.proxy.bib.ucl.ac.be/2443/10.1007/978-3-030-34792-5_11

MCCARTHY, J. (1959). *Programs with common sense*. Stanford, CA: Computer Science Department. En ligne <http://jmc.stanford.edu/articles/mcc59.html>

MESHKOVA, E., WAWRZYNIAK, D., WÓJCIK-MAZUR, A. (2018). *Risk management in banking: Credit, market and technology perspective*. Częstochowa, Pologne : Polish Economic Society.

O'REGAN, G. (2016). *Introduction to the history of computing – A computing history primer*. Switzerland: Springer International. doi: 10.1007/978-3-319-33138-6

PIECHOWIAK, S. (2003). *Intelligence artificielle et diagnostic*. Saint-Denis : Techniques de l'ingénieur.

PIERANDREI, L. (2019). *Risk Management*. Paris : Dunod. <https://doi-org.proxy.bib.ucl.ac.be/2443/10.3917/dunod.piera.2019.01>

ROSTAND, J. (1954). *Pensées d'un biologiste*. Paris : Stock.

STERNBERG, R. J. (2000). *Handbook of intelligence*. New York: Cambridge University Press. En ligne <https://books.google.be/books?id=HvXLCgAAQBAJ&printsec=frontcover&hl=fr#v=onepage&q&f=false>

UMBRELLO, S. (2021). AI winter. In P. F. Frana & M. J. Klein (Eds.), *Encyclopedia of artificial intelligence – The past, present, and future of AI* (pp. 7-8). Santa Barbara, CA: ABC-CLIO.

VAN CAMPENHOUDT, L., QUIVY, R., & MARQUET, J. (2011). *Manuel de recherche en sciences sociales* (4e éd.). Paris : Dunod.

VAN GREUNING, H. & BRATANOVIC, S. B. (2020). *Analyzing banking risk: A framework for assessing corporate governance and risk management* (4e éd.). Washington, DC : World Bank. doi : 10.1596/978-1-4648-1446-4

ARTICLES

ALDASORO, I., FROST, J., GAMBACORTA, L., WHYTE, D. (2021). Covid-19 and cyber risk in the financial sector. *BIS Bulletin* 37, *Bank for International Settlements*. En ligne <https://www.bis.org/publ/bisbull37.htm>

ALDASORO, I., GAMBACORTA, L., GUIDICI, P., LEACH, T. (2020). The drivers of cyber risk. *BIS Working Papers* 865, *Bank for International Settlements*. En ligne <https://www.bis.org/publ/work865.htm>

ALONSO, A. & CARBÓ, J. M. (2021). Understanding the performance of machine learning models to predict credit default: a novel approach for supervisory evaluation. *Banco de España, Documentos de Trabajo* n°2105. En ligne <https://www.bde.es/f/webbde/SES/Secciones/Publicaciones/PublicacionesSeriadas/DocumentosTrabajo/21/Files/dt2105e.pdf>

AMMANATH, B., NOVAK, D. R., ANDERSON, S., KULKARNI, A. (2020, octobre 28). *Conquering AI risks – Unpacking and alleviating concerns that threaten AI advancement*. En ligne <https://www2.deloitte.com/us/en/insights/focus/cognitive-technologies/conquering-ai-risks.html>

BERTRAND, J. (1987). Test de Turing : jeu d'imitation ou test d'intelligence ? *Quaderni*, 1, 35-45. doi: 10.3406/quad.1987.2095

BIKKER, J. A., & VERVLIT, T. M. (2018). Bank profitability and risk-taking under low interest rates. *International Journal of Finance and Economics*, 23(1), 3-18. doi : <https://doi.org/10.1002/ijfe.1595>

BISWAS, S., CARSON, B., CHUNG, V., SINGH, S., THOMAS, R. (2020). *AI-bank of the future: Can banks meet the AI challenge?* En ligne <https://www.mckinsey.com/industries/financial-services/our-insights/ai-bank-of-the-future-can-banks-meet-the-ai-challenge>

BLANC, M., CHARRON, E., FREYSSENET, M. (1989). Le développement des systèmes experts en entreprise. *GIP Mutations industrielles* 43, 1-66.

BORIO, C. (2020). The prudential response to the Covid-19 crisis. *Bank for International Settlements*. En ligne <https://www.bis.org/speeches/sp200630a.htm>

BUCHANAN, B. G. (2019). Artificial intelligence in finance. *The Alan Turing Institute*. doi : <http://doi.org/10.5281/zenodo.2612537>

BUCHANAN, B. G. (2005). A (very) brief history of artificial intelligence. *AI Magazine*, 26(4), 53-60. En ligne <https://www-proquest-com.proxy.bib.ucl.ac.be:2443/scholarly-journals/very-brief-history-artificial-intelligence/docview/208132026/se-2?accountid=12156>

BYUN, K. & SONG, S. (2021). Value at Risk of portfolios using copulas. *Communications for Statistical Applications and Methods*, 28, 59-79. doi : <https://doi.org/10.29220/CSAM.2021.28.1.059>

CALDARA, D. & IACOVIELLO, M. (2018). Measuring geopolitical risk. *International Finance Discussion Papers* 1222. doi : <https://doi.org/10.17016/IFDP.2018.1222>

CALZOLARI, G. (2021). Artificial intelligence market and capital flows. *European Parliament, Policy Department for Economic, Scientific and Quality of Life Policies*. En ligne https://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_STU%282021%29662912

CHRISTOPHER, E. L., EVANS, P. C., FANNIN, R., FERSHT, P., GUPTA, S., JUSTICE, C., RYAN, D., SNOWDON, J., SWAMINATHAN, V. (2019, mars 28). *Easing the pressure points: The state of intelligent automation*. En ligne <https://home.kpmg/be/en/home/campaigns/2019/04/the-state-of-intelligent-automation.html>

CONTRI, B., GALASKI, R., BAUMANN, N., STIER, C., CELNER, A. (2018). *The new physics of financial services – How artificial intelligence is transforming the financial ecosystem*. En ligne <https://www2.deloitte.com/ro/en/pages/financial-services/articles/new-physics-of-financial-services.html>

DEMIRGUC-KUNT, A., PEDRAZA, A., RUIZ-ORTEGA, C. (2020). Banking sector performance during the Covid-19 pandemic. *Policy Research Working Paper*, 9363. En ligne <https://openknowledge.worldbank.org/handle/10986/34369>

DENT, K., WESTWOOD, B., SEGOVIANO, M. B. (2016). Stress testing of banks: An introduction. *Bank of England Quarterly Bulletin* 2016 Q3, 130-143. En ligne https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2866325

EDLICH, A., IP, F., WHITEMAN, R. (2018, novembre 15). *How bots, algorithms, and artificial intelligence are reshaping the future of corporate support functions*. En ligne <https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/how-bots-algorithms-and-artificial-intelligence-are-reshaping-the-future-of-corporate-support-functions>

ELNAHASS, M., TRINH, V. Q., LI, T. (2021). Global banking stability in the shadow of Covid-19 outbreak. *Journal of International Financial Markets, Institutions and Money*, 72, 101322. doi : <https://doi.org/10.1016/j.intfin.2021.101322>

FABRIS, N. (2020). Financial stability and climate change. *Journal of Central Banking Theory and Practice*, 3(1), 27-43. doi : [10.2478/jcbtp-2020-0034](https://doi.org/10.2478/jcbtp-2020-0034)

GANASCIA, J. (2019). Peut-on contenir l'intelligence artificielle ? *Pouvoirs*, 170, 71-81. doi : <https://doi.org/10.3917/pouv.170.0071>

GUAL, J. (2021). The post-COVID-19 recovery: what challenges and roadmap for the banking industry?. *SUERF Policy Note, Issue 217*. En ligne <https://www.suerf.org/policynotes/19605/the-post-covid-19-recovery-what-challenges-and-roadmap-for-the-banking-industry>

KOCH-MEDINA, P. MUNARI, C., SVINDLAND, G. (2021). Which eligible assets are compatible with comonotonic capital requirements?. *Insurance: Mathematics and Economics*, 81, 1-19. doi : <https://doi.org/10.1016/j.insmatheco.2018.04.003>

ŁASAK, P. (2021). The commercial banking sector in eurozone after the pandemic: the paths to recovery. *European Research Studies Journal, Volume XXIV Special Issue 1*, 1233-1246. doi : 10.35808/ersj/2101

LEO, M., SHARMA, S., MADDULETY, K. (2019). Machine Learning in Banking risk management: A literature review. *Risks* 7(1), 1-22. doi : <https://doi.org/10.3390/risks7010029>

MARCU, M. R. (2021). The impact of the COVID-19 pandemic on the banking sector. *Manegement dynamics in the Knowledge Economy*, 9(2), 205-223. doi : 10.2478/mdke-2021-0013

OLSSON, R. (2007). In search of opportunity management: Is the risk management process enough?. *International journal of project management*, 25(8), 745-752. doi: 10.1016/j.ijproman.2007.03.005

OPPY, G. R., & DOWE, D. L. (2003). The Turing test. *Stanford Encyclopedia of Philosophy*, Winter 2020 Edition, 1-26. En ligne https://plato.stanford.edu/entries/turing-test/?source=post_page-----#Tur195ImiGam

PWC GLOBAL. (2019). *PwC 22nd Annual Global CEO Survey*. En ligne <https://www.pwc.com/gx/en/ceo-survey/2019/report/pwc-22nd-annual-global-ceo-survey.pdf>

RAO, A. S., & VERWEIJ, G. (2017, juin 22). *Sizing the prize – What’s the real value of AI for your business and how can you capitalise?* En ligne <https://www.pwc.com/gx/en/issues/data-and-analytics/publications/artificial-intelligence-study.html>

SCHILLIG, M. (2021). Banking and finance after COVID-19. *King’s Law Journal*, 32(1), 49-59. doi : 10.1080/09615768.2021.1886659

SCOTT, M., VAN HUIZEN, J., JUNG, C. (2017). The Bank of England’s response to climate change. *Bank of England Quarterly Bulletin 2017 Q2*, 98-109. En ligne <https://www.bankofengland.co.uk/quarterly-bulletin/2017/q2/the-banks-response-to-climate-change>

SGHAIER, W., HERGON, E., DESROCHES, A. (2015). Gestion globale des risques. *Transfusion clinique et biologique* 22(3), 158-167. doi : <https://doi.org/10.1016/j.traccli.2015.05.007>

STIJN, C., DE LIEDEKERKE, L. (2019). *Artificial intelligence may be a game changer for pricing*. En ligne <https://www.pwc.be/en/news-publications/2019/artificial-intelligence-may-be-game-changer-for-pricing.html>

SUDARSHAN, P. N., ABHISHEK, V., GUPTA, G. (2017). *Artificial intelligence: Why businesses need to pay attention to artificial intelligence?* En ligne <https://www2.deloitte.com/content/dam/Deloitte/in/Documents/technology-media-telecommunications/in-tmt-artificial-intelligence-single-page-noexp.pdf>

TAULLI, T. (2020). *The robotic process automation handbook: A guide to implementing RPA systems*. Monrovia, CA: Apress. doi: <https://doi.org/10.1007/978-1-4842-5729-6>

TRIPATHI, K. (2011). A Review on knowledge-based expert system: Concept and architecture. *International Journal of Computer Applications*, 19-23. En ligne <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.206.3352&rep=rep1&type=pdf>

TURING, A. M. (1950). I.—Computing machinery and intelligence. *Mind*, 59(236), 433-460. doi: 10.1093/mind/LIX.236.433

TÜRISOY, T. (2018). Risk management process in banking industry. *MRPA Paper 86427*, 1-37. En ligne <https://mpra.ub.uni-muenchen.de/86427/>

RÉFÉRENCES WEB

ANDERSON, J., VIRY, P., WOLFF, G. B. (2020). *Europe has an artificial-intelligence skills shortage*. En ligne <https://www.bruegel.org/2020/08/europe-has-an-artificial-intelligence-skills-shortage/>

BASEL COMMITTEE ON BANKING SUPERVISION. (1998). *Framework for internal control systems in banking organisations*. En ligne <https://www.bis.org/publ/bcbs40.htm>

BASEL COMMITTEE ON BANKING SUPERVISION. (2000). *Principles for the management of credit risk*. En ligne <https://www.bis.org/publ/bcbs75.htm>

BASEL COMMITTEE ON BANKING SUPERVISION. (2004). *Principles for the management and supervision of interest rate risk*. En ligne <https://www.bis.org/publ/bcbs108.pdf>

BASEL COMMITTEE ON BANKING SUPERVISION. (2005). *Compliance and the compliance function in the banks*. En ligne <https://www.bis.org/publ/bcbs113.htm>

BASEL COMMITTEE ON BANKING SUPERVISION. (2008). *Principles for sound liquidity risk management and supervision*. En ligne <https://www.bis.org/publ/bcbs144.htm>

BASEL COMMITTEE ON BANKING SUPERVISION. (2009). *Enhancements to the Basel II framework*. En ligne <https://www.bis.org/publ/bcbs157.htm>

BASEL COMMITTEE ON BANKING SUPERVISION. (2011). *Principles for the sound management of operational risk*. En ligne <https://www.bis.org/publ/bcbs195.htm>

BASEL COMMITTEE ON BANKING SUPERVISION. (2018). *Stress testing principles*. En ligne <https://www.bis.org/bcbs/publ/d450.htm>

BASEL COMMITTEE ON BANKING SUPERVISION. (2019). *The market risk framework – In brief*. En ligne https://www.bis.org/bcbs/publ/d457_inbrief.pdf

BASEL COMMITTEE ON BANKING SUPERVISION. (2020). *Calculation of RWA for operational risk – Standardised approach*. En ligne https://www.bis.org/basel_framework/chapter/OPE/25.htm?inforce=20230101&published=20200605

DEUTSCH BANK. (2017). *Annual report 2017*. En ligne https://www.db.com/ir/en/download/DB_Annual_Report_2017.pdf

DIGALAKI, E. (2021). *The impact of artificial intelligence in the banking sector & how AI is being used in 2021*. En ligne <https://www.businessinsider.com/ai-in-banking-report?IR=T>

EUROPEAN BANKING AUTHORITY. (2019). *Risk assessment questionnaire – Summary of the results*. En ligne <https://www.eba.europa.eu/documents/10180/2854739/RAQ+Booklet+Spring+2019.pdf/916f8c4b-7099-4aba-ac1f-882cfd4c3583>

EUROPEAN BANKING AUTHORITY. (2021). *Risk Dashboard*. En ligne <https://www.eba.europa.eu/risk-analysis-and-data/risk-dashboard>

EUROPEAN BANKING FEDERATION. (2019). *EBF position paper on AI in the banking industry*. En ligne <https://www.ebf.eu/innovation-cybersecurity/ai-in-the-banking-industry-ebf-position-paper/>

FINANCIAL STABILITY BOARD. (2013). *Principles for an effective risk appetite framework*. En ligne https://www.fsb.org/2013/11/r_131118/

FINANCIAL STABILITY BOARD. (2017). *Artificial intelligence and machine learning in financial services: Market developments and financial stability implications*. En ligne <https://www.fsb.org/2017/11/artificial-intelligence-and-machine-learning-in-financial-service/>

FINANCIAL STABILITY BOARD. (2018). *Cyber lexicon*. En ligne <https://www.fsb.org/2018/11/cyber-lexicon/>

FLICHE, O. & YANG, S. (2018). Intelligence artificielle : enjeux pour le secteur financier. *Pôle Fintech-Innovation, ACPR*. En ligne <https://acpr.banque-france.fr/document-de-reflexion-intelligence-artificielle-enjeux-pour-le-secteur-financier>

FUTURA TECH. (2021). OCR : Qu'est-ce que c'est ?. En ligne <https://www.futura-sciences.com/tech/definitions/informatique-ocr-3953/>

GLOBAL RISK INSTITUTE. (2021). *Macroeconomic risk*. En ligne <https://globalriskinstitute.org/research/macroeconomic-risk/>

GOGINENI, C. (2019). *10 use cases of RPA in banking industry*. En ligne <https://www.comtecinfo.com/rpa/use-cases-of-rpa-in-banking-industry/>

GOUVERNEMENT DU CANADA. (2016). *Guide to risk taxonomies*. En ligne <https://www.canada.ca/en/treasury-board-secretariat/corporate/risk-management/taxonomies.html>

HARPER, D. R. (2020). *An introduction to value at risk (VaR)*. En ligne <https://www.investopedia.com/articles/04/092904.asp>, consulté le 16 juin 2021

KAGAN, J. & BROCK, T. (2020). *Default risk*. En ligne <https://www.investopedia.com/terms/d/defaultrisk.asp>, consulté le 18 juin 2021

NATIONAL BANK OF BELGIUM. (2018). *Financial stability report 2018*. En ligne https://www.nbb.be/doc/ts/publications/fsr/fsr_2018.pdf

NATIONAL BANK OF BELGIUM. (2021). *Financial stability report 2021*. En ligne https://www.nbb.be/doc/ts/publications/fsr/fsr_2021.pdf

OPEN RISK MANUAL. (2021). *Fraud risk*. En ligne https://www.openriskmanual.org/wiki/Fraud_Risk

REAKTOR & UNIVERSITÉ D'HELSINKI. (2020, septembre 30). *Elements of AI*. En ligne https://www.elementsofai.be/fr?_ga=2.78211668.1589501757.1622305948-1429548984.1612038500, consulté le 2 décembre 2020

RISK.NET. (2021). *Risk glossary: Counterparty risk*. En ligne <https://www.risk.net/definition/counterparty-risk>

SEGAL, T. (2021). *Nonperforming loans (NPL)*. En ligne <https://www.investopedia.com/terms/n/nonperformingloan.asp>, consulté le 22 juin 2021

WEB SUMMIT. (2018, septembre 8). *Stephen Hawking at Web Summit 2017* [Vidéo]. Youtube. En ligne <https://www.youtube.com/watch?v=H41Zk1GrdRg>

WILDS, C. (2018). *Robotics in banking with 4 RPA use case examples + 3 bank bot use case videos*. En ligne <https://thelabconsulting.com/robotics-in-banking-with-4-rpa-use-case-examples/>

WORLD ECONOMIC FORUM. (2021). *The global risks report 2021* (16^e éd.). En ligne <https://www.weforum.org/reports/the-global-risks-report-2021>

COURS

DE MOERLOOSE, C. (2020). *Séminaire d'accompagnement du mémoire*. Syllabus, Université catholique de Louvain.

HENRARD, L. (2020). *Central banking, financial regulation and supervision: The new rules of corporate governance*. Syllabus, Université catholique de Louvain.

OLIESLAGERS, R. (2019). *Principles of banking and finance: Introduction to risk and regulation*. Syllabus, Université catholique de Louvain.

OLIESLAGERS, R. (2020). *Central banking, financial regulation and supervision: BCBS 239 – Principles for effective risk data aggregation and risk reporting*. Syllabus, Université catholique de Louvain.

MÉMOIRES

AHLIN, F. (2017). *Internal model for spread risk under Solvency II* (Mémoire de master). KTH Royal Institute of Technology, Stockholm. En ligne <http://kth.diva-portal.org/smash/record.jsf?pid=diva2%3A1149190&dswid=-3962>

VALGAEREN, H. (2019). *Robotic process automation in financial and accounting processes in the banking sector: A qualitative study with experts in the field* (Mémoire de master). Katholieke Universiteit Leuven, Leuven. En ligne https://www.scripriebank.be/sites/default/files/thesis/2019-09/MBA_Valgaeren_H_Final_Report1819.pdf

ANNEXE

Annexe 1 : Liste des personnes interrogées

Au cours de mémoire, cinq personnes ont été interviewées durant cinq interviews.

- Laurent Denis – Responsable Enterprise Risk Architecture à la BGL BNP Paribas
- Orce Marinkovski – Responsable Robotic Process Automation & Concepteur et Développeur de produits à la BGL BNP Paribas
- Ruben Olieslagers – Responsable du CFO Office (Data Management, Validation Committees, & Environment and Socializing Governance) chez BNP Paribas Fortis
- Augustin Borsu – Responsable Analytics & AI et déploiement support chez BNP Paribas Fortis
- Marc Aguilar – Chief Data Officer à la BGL BNP Paribas

Annexe 2 : Laurent Denis – Responsable Enterprise Risk Architecture à la BGL BNP Paribas

Alexandre Senden (AS) : Globalement, ce mémoire a pour but d'étudier l'apport de l'intelligence artificielle et de la robotic process automation pour améliorer la gestion des risques de conformité, fraude et crédit sur les places financières belges et luxembourgeoises. Ces interviews me permettront d'établir les tendances du marché en termes d'IA et RPA sur ces places et pour ces trois risques. Pour ce faire, j'ai scindé mon questionnaire en trois sections. La première traitera de questions générales. Ensuite, puisque nous considérons trois risques et deux nouvelles technologies, les deux autres sections traiteront de l'IA d'abord, vue sous les trois risques et puis de la RPA vue sous les trois risques également. On peut donc commencer.

AS : Quel poste occupez-vous au sein de BGL BNP Paribas ?

Laurent Denis (LD) : Depuis que vous avez quitté la banque, le nom de mon poste a légèrement changé, je suis maintenant responsable ERA (Enterprise Risk Architecture) mais ça reste similaire par rapport à ce qu'on faisait précédemment. Le processus est pluridimensionnel : le volet RPA, le volet contact avec les régulateurs et tout ce qui est en rapport auprès du régulateur dont le rapport ICAAP et toutes les thématiques de notation réglementaire.

AS : Je vois, les thématiques ont un petit peu évolué et l'équipe également. Bref. Depuis quand occupez-vous ce poste et quelle est votre ancienneté dans la banque ?

LD : C'est janvier 2010.

AS : Ok. Ce sont seulement des questions pour un peu évaluer le profil des intervenants, notamment en fonction de l'ancienneté et des connaissances sur la banque. De manière générale, quelle est le degré d'implication de la banque en termes d'IA et de RPA ?

LD : En matière d'IA, la banque s'est dotée d'un département spécialisé qui s'appelle le data lab qui est piloté par Madame X qui est responsable, c'est une toute petite équipe en fait qui était déjà là quand vous étiez en stage. Cela fait au moins trois ans qu'elle est en place. C'est une petite équipe donc en fait ils sont 3-4-5, ça dépend et elle travaille principalement avec des chercheurs, des doctorants de l'université de Luxembourg ce qui fait que son équipe... elle n'a pas de stabilité dans l'équipe donc c'est un peu la critique et c'est comme ça qu'elle perçoit aussi c'est qu'elle a du mal à avancer dans le temps parce que les personnes font du va-et-vient, ils

sont là pour six mois puis quittent la banque et il faut recommencer presque à zéro. Et sur le projet d'IA bah voilà on est tout au début donc ils arrivent toujours avec plein de bonnes idées en pensant d'un point de vue théorique que ça va pouvoir se faire très rapidement mais quand on confronte à la réalité du terrain mais tu vois que voilà il y a dépendances avec les différents départements, notamment avec l'IT et malheureusement dans la banque même si on met en avant la culture agile dans les faits ça se passe pas très bien et l'IT est un peu rigide donc ça prend du temps. Donc petite structure en place depuis 3-4 ans et problèmes de turnover dans l'équipe

AS : Est-ce que le fait que ça soit des jeunes donc relativement inexpérimentés est un frein au développement de l'équipe ?

LD : Oui c'est également un point, ils n'ont pas de connaissance du monde bancaire. Le degré d'implication de la banque aujourd'hui donc oui on est impliqués mais on est dans les débuts. Et petite structure qui fait que le département a peu de financements, on prend des universitaires parce qu'ils nous coûtent très peu d'argent et là je pense que c'était dans les plans pour 2021 de pouvoir recruter quelqu'un en interne mais je ne sais pas si ça s'est fait mais voilà est en tout cas le message c'est qu'il y a quelque chose, c'est petit mais ça commence à se mettre en place mais on n'a pas des budgets pour engager 20 personnes comme tu l'aurais chez Fortis.

AS : Pourquoi alors à la place la BGL BNP Paribas n'envisage pas de sous-traiter ? Par exemple, avec des fintechs qui peuvent fournir des services IA et qui sont spécialement là-dedans en fournissant des solutions déjà prêtes.

LD : Cela c'est une approche qui aujourd'hui n'a pas à ma connaissance qui n'a jamais été validée. Ce sont des pistes qui ont été évoquées mais qui n'ont pas été retenues. On en parlait déjà en 2017-18 quand on a voulu refondre les programmes crédit, on parlait déjà de s'entourer de fintechs à l'époque. Alors aujourd'hui, ça sort peut-être un peu du cadre mais on est en train de repenser, enfin on est sur un schéma de transformation IT au niveau des packages front to back et là on est sur des éditeurs, deux sont des éditeurs traditionnels et un est plutôt orienté fintech voilà mais ce n'est même pas certain, on n'est pas allé voir plus loin et on n'est même pas aller voir plus, aller voir des sociétés qui ont vraiment participé à la mise en place de banques style Revolut, ce genre de choses. Je ne sais pas quelle est la décision aujourd'hui, à l'époque de ce que je sais en 2017-18, on n'aimait pas trop les fintechs parce que les fintechs ne sont pas solides, c'est ça le risque et on n'a pas non plus de volonté de les acheter. Donc il

faut pouvoir travailler avec un partenaire qui demain sera encore là et sur cet environnement un peu incertain, on a préféré ne pas prendre le pari de travailler avec quelqu'un qui demain n'est plus présent. Et la volonté n'était pas d'acheter des fintechs, raison pour laquelle aujourd'hui on ne travaille pas vraiment avec eux.

AS : Ok donc en termes d'IA, pas de fintech partenaire avec la BGL.

LD : Non, non. Notre Chief Data Officer pourra vous en dire plus parce que c'est un membre du comité de direction qui a participé à des discussions dont moi je ne suis même pas au courant donc voilà c'est peut-être un point que vous devriez creuser avec lui ce que je vous donne là est un feedback qui date de 2018.

AS : Et en matière de RPA ?

LD : Donc alors même chose en matière de RPA. Il y a de la volonté, on a des ambitions vis-à-vis du groupe de transformer donc on a une personne qui est responsable du programme de transition au sein de la banque qui s'appelle Monsieur X et Madame X est responsable de l'entité RPA. Donc en termes de RPA, c'est plus ou moins la même histoire donc volonté du groupe de développer de la RPA au sein de chaque entité marché domestique, ça s'est mis en place il y a 2-3 ans, petite structure également, ils doivent être un peu moins de 10 personnes, plus grosse que l'IA mais reste quand même de taille modérée et là aux dernières informations d'il y a une quinzaine de jours/trois semaines, ils viennent seulement d'acquérir des logiciels OCR un peu plus performants que ceux qu'ils avaient auparavant et que nous nous utilisons avec Orce depuis fin 2017. Ils ne sont pas à la pointe de la technologie mais bon ils se mettent dans les clous, enfin dans les starting blocks de la compétition.

AS : Au niveau RPA c'est quand même un petit peu plus avancé que l'IA alors ?

LD : Oui, oui. Alors ce qui n'est pas évident en fait c'est quand il y a deux ans ils ont présenté le programme RPA au sein de la banque en disant voilà clairement on va mettre de la RPA en place parce que on vise des synergies, donc on vise à remplacer des hommes par des robots et donc ils sont allés trouver les différents métiers/fonctions en leur demandant de monter des business cases et voir quelles étaient les économies de personnes que l'on pouvait faire et les gens n'ont pas vraiment joué le jeu donc les départements métiers et fonctions n'ont pas vraiment joué le jeu et de mémoire, par exemple sur un département qui était operations, c'est là où tu t'attends à avoir le maximum d'applications RPA et d'automatisation la plus poussée,

ils sont arrivés avec des synergies de quelques personnes donc le responsable des opérations a dit « si on met de la RPA chez moi, on pourrait faire ça et ça et ça va me dégager peut-être 2-3 personnes ». Ce que je dis ici c'est que le changement est encore un peu compliqué, chacun protège encore un peu ses équipes, on n'a pas identifié au sein de la banque de programmes, de processus qui pourraient complètement être informatisés ou robotisés et dégagerait 20 personnes d'un coup pour la mise en place d'un processus robotique, ça on n'en est pas là.

AS : Un facteur négatif là-dedans, c'est que les personnes montrent pas mal de résistance au changement de manière assez évidente et puis les personnes protègent leurs équipes.

LD : Oui, et puis les gens ne sont pas, on l'a vu quand on a fait les travaux avec Orce, les gens sont... globalement tu restes dans ta zone de connaissance, tu n'anticipes pas ce que la RPA pourrait t'apporter sur d'autres processus donc pour certaines personnes, il n'est pas évident de se projeter et d'identifier toutes les potentialités d'une solution RPA. Il faudrait avoir des sessions de travail un peu out of the box. Quand t'es plongé dans ton quotidien et que tu réfléchis qu'à ton périmètre de production, il faut déjà bien le maîtriser je pense pour savoir ou avoir vraiment des gens des opérations qui te remontent les points pour voir un peu quels sont les « pain points » et là pour automatiser les choses. Donc un manager n'a pas nécessairement la vue sur tous ces « micro pain points » et pour un manager réfléchir soit très proche du processus ou complètement out of the box en mettant en place de nouveaux processus qui s'appuieraient sur de la RPA, c'est pas évident. Donc ils sont un peu au milieu des deux et je pense que c'est ça qu'il fait que ça marche moyennement aujourd'hui c'est qu'on n'est pas capable d'identifier correctement les différentes zones ou les différents endroits là où la RPA pourrait jouer pleinement son jeu.

AS : Dans ce cas, pourquoi pas mettre un expert RPA et IA dans chaque département ?

LD : Mais vous voyez bien les sujets qu'on a avec l'IT, c'est ce que je disais en intro, c'est que l'agilité on en parle mais on ne la met pas en place. Donc un concept agile c'est exactement ça, ce serait former, et ils l'ont défini, ils font la promotion du concept agile depuis début janvier, ils veulent vraiment revenir à un mode de fonctionnement où ils vont détacher les gens de leur département pour les mettre en place dans ce qu'ils appellent une squad donc c'est vraiment une équipe dédiée à la mise en place, à l'aboutissement d'un projet. Et ces gens-là bah ce sont des gens des opérations, des gens de l'IT, du marketing, tout ce qui tourne autour de la conception d'un produit ou d'un processus mais aujourd'hui dans ces squads-là, je ne suis pas

certain que le volet RPA intervient. Donc l'agilité, c'est bien sur le papier mais au sein de la BGL aujourd'hui, on ne le vit pas vraiment.

AS : Est-ce similaire dans toute la banque ?

LD : Je pense bien oui. Pour vous donner un exemple, un des sujets qu'on traite avec un membre de mon équipe c'est le fait d'avoir un backup pour les solutions RPA qu'on développe donc ça fait un moment maintenant qu'on essaye d'avoir un backup de l'IT directement chez nous et on avait bon espoir avec cette mise en place des squads et on n'arrive toujours pas intégrer quelqu'un de l'IT dans notre service. Donc c'est compliqué, très politisé et donc tu n'es pas non plus dans une culture à l'américaine où on promeut quelque part le succès, l'innovation. Ils ont vu ce que certains départements sont capables de faire et clairement avec ce que l'on met en place avec Orce, bah les équipes de l'équipe RPA ça ne leur fait pas de la bonne pub donc au final c'est de la politique.

AS : Et dans cette équipe-là, l'équipe spécialisée RPA, c'est une équipe fixe ou ça fonctionne de la même manière que le data lab ?

LD : Oui c'est une équipe fixe, ce sont tous des employés de la banque qui ont été reconvertis pour monter cette équipe-là mais eux sont en CDI, oui.

AS : Ok, donc c'est déjà un peu plus stable et donc ça devrait produire plus d'effets positifs et de solutions à terme. Globalement, la banque, sur ces thématiques, par rapport aux autres banques, serait un peu à la traine ?

LD : Je ne sais pas au fait parce qu'il y a quand même un élément positif en matière d'IA, c'est qu'on est arrivés à monétiser une application IA sur la place du Luxembourg, c'est un module qui permet la détection de la fraude donc c'est quelque chose qui a été mis en place au sein de la BGL et qui a été vendu à des partenaires, enfin à des autres institutions bancaires au Luxembourg donc dire qu'on est à la traine, je ne sais pas mais au travers de ce produit-là, c'était quand même une belle plaquette marketing en matières d'IA.

AS : Cet outil est uniquement pour la fraude ?

LD : C'est uniquement pour la fraude, ça s'appelle Gold Finder.

AS : Je vois.

LD : Donc l'IA, on a un peu rayonné sur la place en monétisant, en revendant ce produit. En matière de RPA, là tu restes en interne. Dans la banque, la responsable de l'équipe RPA a quand même déployé des processus robotisés dans plusieurs départements. Avec son équipe de 10-15 personnes, ils ont quand même fait des choses mais la critique aujourd'hui, Paris leur a reproché qu'ils ne transformaient pas suffisamment.

AS : Les processus aujourd'hui manuels qui seraient automatisables ?

LD : Oui. Donc les estimations, les synergies, les gains d'ETP, aujourd'hui on n'est pas au niveau attendu des responsables à Paris donc il y a un peu de pression ici aujourd'hui au sein de la banque sur cette équipe-là. C'est ce que je disais, c'est une culture, les gens ne sont pas prêts à ça, les gens défendent leurs équipes et je pense que tant que tu n'es pas sous contrainte de Paris qui dit que tu dois absolument faire -5 dans ton département eh bien tu ne vas pas prendre l'initiative de dire ok je vais diminuer le personnel. Si aujourd'hui quelqu'un vient te trouver en disant que la RPA pourrait améliorer le quotidien et qu'éventuellement vous pourriez mettre des gens sur des tâches à plus de valeur ajoutée ou autre part dans la banque, si tu n'as pas la pression du groupe ou de la banque qui te dit « tu dois faire moins x personnes dans ton département », tu vois pas vraiment l'intérêt et tu vas te dire que cette carotte tu vas la garder quand j'aurai soif et quand demain ou après-demain Paris viendra avec des économies d'ETP à réaliser obligatoirement. Donc tu n'es pas proactif mais tu seras réactif.

AS : Est-ce que ceci ne serait pas également dû à la culture d'entreprise à la BGL ?

LD : Oui, c'est un peu ça. On n'est pas dans un esprit PME.

AS : Et donc c'est le cas pour toutes les branches du groupe ou certaines sortent du lot ?

LD : BNP Paribas Fortis ça a toujours été un peu le précurseur dans la matière et notamment l'IA, je pense qu'en 2016 ils en parlaient déjà. Et vraiment la volonté, ils ont mis 10 personnes dans une salle et ils leur ont demandé de fournir un truc. Là ils ont mis les gens en mode agile, ils les ont déchargés de leur BAU, ils ont mis des statisticiens, des personnes qui maîtrisent les langages IA dans le but de pondre quelque chose qui facilite la vie du business et c'était mettre en place un nouveau produit sur le marché. Ils ont vraiment bossé en mode agile, en étant détachés de leur BAU, comme des fous et vase clos pendant 2-3 mois. C'est ça le mode agile en fait, tu vas chercher les équipes.

AS : Un frein serait alors la culture non-entrepreneuriale de la banque, culture lente qui prend du temps à suivre les thématiques ?

LD : C'est le propre des grosses structures je pense, tu n'es pas dans un esprit PME ou collaboratif, c'est le manque d'esprit collaboratif inter entités, c'est plutôt en gestion de silos, une gestion très politisée de chacun des départements. Donc quand tu arrives avec des départements transverses telles que l'IA et la RPA qui doivent venir aider chaque département, bah la volonté est certainement là de la part de ces départements mais ils font vite face à certains freins.

AS : Vous parliez que pour BNP Paribas Fortis, l'objectif était de fournir un nouveau produit donc dans cette logique, est-ce que l'IA et/ou la RPA permettrait de fournir de nouveaux produits ?

LD : Là à l'époque, c'était de l'octroi automatique donc Fortis, c'était une approche un peu scoring donc c'était de l'octroi automatique de produits, c'était un produit particulier c'était je pense des demandes d'avances sur TVA. C'est une avance de trésorerie donc c'est l'équivalent d'un produit. Le projet c'était d'évaluer la solvabilité des clients et dès lors qu'ils rentraient dans les clous, cette demande d'avance de fonds leur était automatiquement accordée, donc c'est quelque part un scoring, du score à l'octroi mais c'était basé sur un volet IA. Alors, tous les scorings ne sont pas avec de l'IA, il faut bien faire la différence entre les deux mais ici il y avait le caractère auto-apprentissage que tu ne retrouves pas sur tous les modèles de scoring.

AS : Je vois. Lors de mon stage d'ailleurs, je me rappelle vous avoir demandé si les modèles de scoring étaient basés sur de l'IA. La réponse était non. Cela a-t-il changé pour certains modèles ?

LD : Eh bien, le data lab a développé un nouveau modèle de scoring pour les PME donc on pensait tous qu'il était basé sur de l'IA puisqu'on a fait le lien entre data lab donc IA donc le modèle contient de l'IA. Mais en fait ce que le data lab a fait, c'est une simple régression linéaire multivariée donc le modèle ne contient aucun autoapprentissage.

AS : Un peu dommage, donc. J'ai encore deux petites questions avant qu'on passe aux risques vus sous l'IA et la RPA. Est-ce qu'il y aurait une crainte que l'IA génère des comportements de masse ? Que des algorithmes basés sur de l'IA prennent des décisions tous en même temps et de telle façon à ce que ça produise des crashes boursiers par exemple ?

LD : Ici, je ne pourrais pas, ça s'est vu donc j'imagine donc ce qu'on entend comme critique facile sur l'IA c'est que l'IA est programmée par des humains et donc les biais de l'humain se retrouvent dans les algos IA. Sinon, je n'ai pas vraiment de réponse par rapport au risque que vous évoquez, maintenant un defect dans le module ferait que, si par exemple une variable n'est plus alimentée correctement, eh bien oui tu vas avoir le résultat de ton algo qui va toujours dans le même sens, ça c'est un risque également donc un risque important c'est le monitoring, c'est de pouvoir surveiller ton algo. Donc tu le mets en place mais il faut être derrière pour s'assurer qu'il ne commence pas à prendre des décisions déconnantes. Quand tu prends 10 décisions par jour, très bien, tu as le temps de le voir venir mais quand ce sont des millions de décisions prises dans un temps très court, il devient évidemment impossible de les vérifier.

AS : Suivre autant de décisions prises au même moment, impossible et se mettre des flags à des endroits où tu ne sais même pas où il faut les mettre, impossible également.

LD : Oui donc ce n'est pas parce que c'est de l'intelligence artificielle qu'il ne faut pas monitorer, il faut quand même continuer à suivre.

AS : Du coup, ici je vois un peu l'importance des données dans ce cas. Une erreur dans les données implique une erreur dans la décision de l'algo.

LD : Oui, c'est exactement ça. Ou le fait que l'algo ne soit plus, enfin quand vous dites les données, la donnée peut être propre mais l'alimentation de la donnée, l'exploitation de cette donnée au travers d'une variable qui est définie, si l'exploitation de la variable déconne pour une raison x, y dans l'algo, donc la variable n'est plus traitée, qu'est-ce qu'il se passe ? Tu as un comportement qui est inattendu et donc il faut pouvoir intercepter très très vite et monitorer très très vite.

AS : Donc deux points importants quand on utilise des outils basés sur l'IA, c'est monitorer la qualité des données, ce qui je pense se fait dans toutes les grandes banques européennes puisque ce sont des réglementations européennes et le deuxième c'est monitorer la transmission et l'exécution des données dans l'algo. Passons à la dernière question pour cette partie. L'IA pourrait standardiser des décisions et réduire trop les risques de crédit, ce qui est potentiellement néfaste pour l'économie qui a besoin d'intermédiaires capables de prendre des risques. Qu'en pensez-vous ?

LD : Alors là, pour moi c'est juste une question de calibrage donc dans ton modèle, tu dois pouvoir lui dire « moi je vis avec 3% de risque ou je vis avec 0.1% de risque ou avec 14% de risque » et c'est en fonction du positionnement de ce trigger que le moteur IA va te dire « ok je prends ou je ne prends pas ». Cela reste une contrainte de ton modèle et cette contrainte-là, si tu fais ton job correctement et que t'arrives à monitorer ta production presque en temps réel (pas de jour en jour mais disons de mois en mois), tu vas voir que par rapport à un environnement macroéconomique, par exemple si tu maintiens tes contraintes inchangées, eh bien que tu vas engendrer plus de coût du risque donc plus de pertes donc il est temps d'agir et de revoir à la hausse ou à la baisse cette contrainte. C'est une question de monitoring et d'optimisation sous contraintes.

AS : Si on imagine une première étape dans laquelle on aurait un premier data set qu'on fait tourner sur un modèle IA, et qu'on lui fixe un pourcentage de risque donné, l'appétit du risque à ce moment-là, selon l'environnement macroéconomique, puis qu'on fait un deuxième essai avec un risque donné différent puis un troisième essai on laisserait le modèle IA définir lui-même le risque en fonction de contraintes et de l'environnement macroéconomique. Ceci ne pousserait pas à ce que le modèle ne réduise pas le risque au maximum ? Enfin, ceci dépend toujours du calibrage.

LD : C'est ça en fait, si tu lui dis 0 défaut, il va te calibrer pour que tu aies 0 client. Si tu dis 0 défaut, tu ne prends pas de risque donc il faut quand même, pour moi c'est une optimisation sous contraintes.

AS : Donc quand on parle d'IA, on doit calibrer dans tous les cas ou sinon ça revient à dire à l'outil de restreindre à 0 presque tout.

LD : Je ne sais pas. Pour moi, ton algo tu dois l'entraîner sous contrainte, donc interprète des données par rapport à une situation que je veux ou que je ne veux pas voir arriver, c'est ça la contrainte. Donc le je ne veux pas voir arriver c'est je ne veux pas arriver plus de 3% de défauts, je ne veux pas voir arriver un cas de fraude de plus d'1 million d'euros. Je pense que c'est comme ça que tu calibres ton modèle, ça reste une thématique d'optimisation sous contraintes.

AS : Je vois, très bien. On peut peut-être passer à la suite. En termes de risque, les trois risques considérés ici, c'est-à-dire conformité, fraude et crédit, est-ce que la banque utilise des outils IA ? Quelles sont les perspectives d'utilisations IA sur ces trois risques ?

LD : En fraude, c'est l'outil Gold Finder dont on a déjà parlé.

AS : J'imagine que cet outil a eu de très bonnes répercussions ?

LD : Déjà en termes d'image, oui, savoir que la BGL était leader en 2019-2020 sur les thématiques d'IA pour le risque de fraude.

AS : Cela a-t'il permis des améliorations comme plus d'efficacité, réductions de personnel ou recalibrage des tâches du personnel pour plus de valeur ajoutée ?

LD : Cela détecte tout le boulot qui reste de remonter, enfin ils avaient d'autres outils de la fraude. Concrètement, je ne sais pas répondre à ta question, je n'ai pas vu le business case donc je ne sais pas quel s'il y a eu un impact de réduction des effectifs suite à ce projet-là.

AS : Peut-on quand même supposer que ça a engendré une baisse de coûts puisque l'outil semble être très performant ?

LD : Oui, après on avait déjà d'autres outils de détection de cas de fraude, notamment des outils groupe donc voilà, aujourd'hui est-ce qu'on a juste remplacé ces outils ? Il est éventuellement plus performant mais les équipes qui sont derrières doivent quand même confirmer que le cas est un réel cas de fraude parce que l'outil va détecter des suspicions donc là il faut confirmer que c'est un cas réel et puis tu lances toute la machinerie pour analyser en profondeur et puis remonter le cas éventuellement au parquet. Donc hier on avait quelque chose, aujourd'hui on a quelque chose qui est plus puissant.

AS : Est-ce que Gold Finder remplace les outils qui étaient utilisés avant ?

LD : Bah j'espère, je ne le sais pas mais j'espère que c'est le cas. Donc, par rapport à ta question est-ce qu'on a réduit la personne, j'imagine que non.

AS : Pourquoi est-ce qu'il faut encore un humain derrière pour valider les suspicions ? Si l'outil a travaillé sur les données et qu'il les connaît, il y a un moment où il ne se trompe plus. Enfin, il y a aussi moyen de monitorer à quel point il est performant et il est probablement proche de 99%.

LD : Parce que comme vous dites, vous avez 1% qui fait que tu n'envoies pas directement toutes tes déclarations de suspicion au parquet, pour ne pas noyer le parquet donc il faut filtrer sur

base de meilleures connaissances et la meilleure connaissance elle est détenue là où les opérations se passent donc c'est-à-dire au sein de la banque.

AS : Cela pourrait même être envisagé de développer une suite à cet outil qui ferait l'analyse de l'humain de dire si la suspicion est réelle et qu'il faut envoyer au parquet.

LD : M'oui, cela voyez le directement avec Madame X, c'est peut-être le résultat de l'algo.

AS : C'est vrai, peut-être qu'il va déjà aussi loin. On peut juste finir sur la fraude, il n'y a pas spécialement de perspectives selon ce que vous savez à ce jour et ensuite, enchaîner avec les deux autres risques, conformité et crédit ?

LD : D'aller vers autre chose, non, ils vont certainement améliorer l'outil, le stabiliser et le fiabiliser mais je n'ai pas d'autres infos. Conformité, je ne sais pas. Je ne sais pas qui pourra vous répondre là-dessus, éventuellement Marc Aguilar. Et sur la partie crédit, c'est ce que je vous disais tout à l'heure par rapport au scoring crédit, c'est-à-dire qu'on pensait qu'il y avait de l'IA dans les algos mais il n'y en a pas. Donc aujourd'hui, en matière d'IA crédit, sur le scoring on n'en a pas et il y a peut-être un petit truc mais ça fait 3 ans que c'est en projet, ça n'a jamais été livré, c'est une proposition de validation automatique des dépassements sur compte courant. Cela s'appelle le projet ODAV et Madame X peut te préciser s'il s'agit d'IA ou pas mais avec ce que j'ai vu maintenant sur le scoring, j'ai de moins en moins confiance sur la présence d'IA au sein du data lab. Je pense que c'est emballé pour faire joli mais ça reste des modèles, les outils statistiques qu'ils utilisent sont peut-être plus performants donc pour analyser les données historiques mais la façon dont ils modélisent c'est de la régression linéaire mais la détection des variables est plus fine donc les outils statistiques aujourd'hui qui permettent de traiter les données historiques sont plus puissants, plus fins, et permettent de catégoriser mieux les variables et les nœuds dans un algo mais après je pense que tu n'as qu'une fonction linéaire ou logarithmique. Aujourd'hui, le scoring ça va être une fonction linéaire avec un intercept qui va prendre une valeur numérique puis après c'est un + un -, plus un facteur alpha fois la variable 1, moins un facteur delta fois la variable 2 donc c'est vraiment une régression linéaire. Donc, est-ce que ça c'est de l'IA ? Ce n'est pas évident à dire.

AS : Ce n'est pas de l'IA je pense.

LD : Oui c'est ça, ce n'est pas autoapprenant en fait. Ensuite, on te parle d'effectuer un exercice de backtesting annuel. Si tu avais vraiment de l'IA, je ne pense pas que t'aurais un exercice de

backtesting, mais ce serait backtesté en continu, directement sur les données. C'est ça que quand on me parle de backtesting à horizon 1 an... je ne pense pas que ça soit de l'IA.

AS : Leur objectif est probablement de migrer vers l'IA ? On peut peut-être concevoir que ce qu'ils font aujourd'hui c'est la première étape avant de passer sur de l'IA.

LD : Éventuellement, oui.

AS : Peut-être de stabiliser la manière dont les données sont évaluées, dont la qualité des données est évaluée et une fois que ceci est 100% opérationnel, on peut faire tourner cela avec de l'IA.

LD : Mais est-ce qu'on ne devrait pas être capable aujourd'hui de passer directement sur un modèle d'IA ? Parce que les technologies existent, les données sont là. Qu'est-ce qui fait qu'on n'est pas en mode IA aujourd'hui ?

AS : Effectivement. On peut passer à la RPA maintenant. Donc, la question est un peu similaire. Quels sont les outils RPA que la banque possède actuellement ? Toujours en termes de risques de crédit, fraude et conformité.

LD : En termes de crédit, il n'y a que ce qu'on fait chez nous avec Orce et un deuxième volet, l'équipe de Madame X spécialisée en RPA. Je vais peut-être commencer par la seconde. Cette équipe intervient pour robotiser les processus de back office donc elle intervient, la cible c'est que, sur base des données qui sortent des processus crédit, elle puisse préparer des documents de demande de crédit et réaliser des encodages dans les outils de saisie du back office donc, une injection de taux d'intérêt, une injection d'une durée, la préparation d'un contrat avec l'adresse, le nom du client, *etc.* Je ne pense pas qu'il y a eu beaucoup de projets RPA qui sont déjà live aujourd'hui, je pense qu'il y en a encore quelques-uns qui sont à l'étude ou en cours de développement mais je ne pourrais pas te dire ceux qui sont développés aujourd'hui.

AS : Est-ce que ce sont aussi des outils OCR comme ce que vous faites avec Orce ?

LD : Très très light dans le sens où ils ont seulement, il y a trois semaines/un mois, ils ont présenté ce qu'était vraiment un OCR performant. Auparavant, ils utilisaient un outil groupe qui s'appelle le Blue Prism, c'est une solution IBM, qui est également au sein de la BIL. Dans Blue Prism, il y a également un OCR natif mais qui n'est pas du tout performant. Donc ils nous l'ont présenté en 2018 et on a dit « ok ça va, on ne sait rien faire avec » donc on est parti avec

notre propre solution. Donc là, l'équipe RPA a switché vers un nouvel OCR. Dans la RPA, tu n'as pas besoin de l'OCR pour faire de la RPA, c'est une couche supplémentaire qui te permet de dématérialiser ton processus, tu viens d'un support papier vers un support informatique. Donc, aujourd'hui, ils ne sont pas encore suffisamment prêts, ou bons, en matière d'OCR mais ça n'empêche pas que sur la RPA ils fournissent des solutions. Voilà pour le risque de crédit back office. Je ne suis pas au courant d'autres sujets au niveau front chez eux. Nous au niveau du middle office dans les équipes de RISK, Orce est arrivé avec sa solution risk based review, lecteur automatisé des bilans. La raison est l'historique au Luxembourg : absence d'une centrale des bilans complète, tu as un projet EDITUS qui s'est mis en place il y a 2 ans dans le but justement de fournir aux établissements financiers, des données financières. Le problème c'est que les données financières sont, dans la majorité des cas, pas complètes donc tu vas retrouver l'actif et le passif mais il n'y aura pas le compte de résultat donc en matière d'analyse financière, sans compte de résultat, tu ne fais pas grand chose, même rien du tout. Donc, partant de ce constat-là, Orce a développé avec une technique d'OCR, d'expressions régulières, on peut même éventuellement dire que c'est un début d'IA, il a su lui traiter des états financiers pour les rendre lisibles à travers un fichier Excel et ensuite, passer la couche RPA qui ira encoder les informations contenues dans le fichier Excel dans les outils de back office.

AS : Pourquoi pourrait-on presque dire que c'est de l'IA ?

LD : C'est au niveau des expressions régulières, je ne saurais pas en parler comme ça.

AS : Au niveau conformité, vous n'aurez pas plus d'informations ?

LD : Non, ça je ne saurais pas vous dire. Demandez à Marc Aguilar si vous avez un entretien avec lui.

AS : Et au niveau fraude ?

LD : Là, je pense qu'ils n'ont rien fait.

AS : Quelles sont les conséquences positives et négatives de ces utilisations (ex : amélioration(s), baisse des coûts, rapidité d'exécution, réduction de personnel, etc.) ?

LD : Oui, ici clairement la RPA, dans un service de back office, c'est réduire le risque opérationnel. J'en parlais ce matin avec quelqu'un qui est aux paiements, papys et mamys continuent d'envoyer des documents, enfin des virements qu'ils font à la main, aujourd'hui on

en reçoit encore énormément et des personnes doivent saisir ça donc il y a un OCR qui passe dessus, quand c'est mal écrit, c'est une personne qui doit interpréter et faire l'encodage et dans certains cas, enfin au niveau du service des paiements, ils ont énormément d'erreurs qui sont réalisées, et quand tu ne respectes pas, il y a des pénalités qui sont calculées et voilà, il me disait encore hier qu'il y a un paiement qui a été refusé, ils sont tombés en dehors de la date et ça a coûté 6000€ sur un transfert de quelques millions. Donc en termes de risque opérationnel, la RPA permet certainement de le réduire.

LD : Un autre point important à considérer c'est que les départements IT sont souvent sous l'eau, débordés et où les coûts de mise en œuvre sont souvent très élevés et c'est pourquoi la RPA et l'utilisation de robots est intéressante parce que ce sont des solutions modulaires, flexibles et à moindre coût. Là, on ne fait pas appel à l'IT mais la robotique est souvent gérée dans un département connexe à l'IT, il y a des informaticiens dedans bien sûr mais c'est un peu plus agile.

AS : C'est ce que la banque vise à avoir avec l'équipe RPA de ce que j'ai compris.

LD : Oui, l'équipe RPA est une équipe décentralisée, elle n'est pas dans l'IT, elle est reprise sous une autre autorité de gouvernance. Moi je crois vraiment au système décentralisé, c'est ce qu'on fait avec Orce, c'est-à-dire que le métier ou la fonction s'entoure de personnes qui ont les compétences mais qui sont directement là à côté de toi. Cela n'empêche pas d'avoir un département informatique qui lui fait la coordination, qui garde les liens fonctionnels avec les équipes qui sont décentralisées, qui les maintient à jour sur toutes les informations, les évolutions en termes technologiques, les nouvelles façons de coder donc tu gardes un pilotage central mais l'exécution en day to day elle est proche des opérationnels, c'est ça qui fait que ça marche et que c'est rapide et que c'est réactif.

AS : Cela fait sens en tout cas. On peut peut-être terminer là-dessus. Merci beaucoup de m'avoir accordé ce précieux entretien. Je vous souhaite une bonne continuation.

LD : Pas de problème, bonne continuation également.

Annexe 3 : Orce Marinkovski – Responsable Robotic Process Automation & Concepteur et Développeur de produits à la BGL BNP Paribas

Alexandre Senden (AS) : Bonjour. Merci de m'accorder cet entretien. Je vais commencer par un petit récapitulatif de ce qu'on va aborder durant cet entretien. Alors, globalement, ce mémoire a pour but d'étudier l'apport de l'intelligence artificielle et de la robotic process automation pour améliorer la gestion des risques de conformité, fraude et crédit sur les places financières belges et luxembourgeoises. Ces interviews me permettront d'établir les tendances du marché en termes d'IA et RPA sur ces places et pour ces trois risques. J'ai donc scindé mon questionnaire en trois parties. D'abord, des questions générales. Ensuite, deux sections, une sur l'IA et une sur la RPA. Chacune traitera des trois risques abordés dans mon mémoire.

Orce Marinkovski (OM) : Très bien.

AS : Alors, commençons. Quel poste occupez-vous au sein de BGL ?

OM : Je suis en charge de ce qui est automatisation de process, je suis concepteur et développeur de produits.

AS : Depuis quand occupez-vous ce poste et quelle est votre ancienneté dans la banque ?

OM : J'occupe ce poste depuis 2018 et je suis dans la banque depuis 1998.

AS : Globalement, que pouvez-vous dire sur le degré d'implication de la banque en termes d'IA et de RPA ?

OM : Alors, l'intelligence artificielle, je dirais qu'à ma connaissance, elle n'est qu'à un niveau d'étude, donc d'étude de « Comment on peut l'utiliser ? ». En ce qui concerne la RPA, elle est déjà utilisée mais principalement sur des tâches répétitives, sans intelligence derrière.

AS : Oui, de ce que j'ai compris de la RPA, ce n'est pas censé être un outil doté d'intelligence comme pourraient l'être des outils basés sur l'intelligence artificielle.

OM : On va dire que la RPA a quand même une tendance à aller vers des synergies également avec l'intelligence artificielle. Par exemple, quand il y a des tâches répétitives et que des erreurs se répètent, l'IA peut intervenir pour identifier et corriger automatiquement des erreurs, donc en fait corriger le tir pour les robots qui tournent. Il y a de plus en plus l'IA mais c'est encore à ses prémices. C'est au niveau étude qu'on doit voir comment on peut l'implémenter et l'utiliser.

AS : Quel est l'état d'avancement de la banque, IA et RPA, par rapport au secteur ? Où se trouve la BGL BNP Paribas par rapport aux autres banques ?

OM : J'aurais du mal à juger de ça ne sachant pas où se trouvent les autres sur la place financière, mais de ce que je vois, je ne peux que me répéter : l'IA n'est qu'au stade d'étude. Pour la RPA, on a peut-être un petit retard par rapport à d'autres banques qui ont commencé plus tôt avec la RPA. Maintenant, est-ce qu'on a rattrapé ce retard, je ne sais pas le dire. Il faudrait voir ça avec les personnes concernées par la RPA au sein de la banque. Nous, on a un département RPA chez nous, mais c'est avec des robots développés par nous. On ne peut donc pas se comparer sur le marché, enfin c'est compliqué.

AS : Oui, j'ai prévu des entretiens avec d'autres personnes pour avoir des points de vue différents. Quels seraient alors les principaux facteurs qui permettent à la banque d'utiliser des outils IA ou RPA et les freins éventuels ?

OM : Tous les changements, l'adaptation du fonctionnement, parce qu'on va dire que des processus totalement autonomes drivés par l'IA, je pense que c'est un peu un idéal. Je pense que ce sera plutôt un truc où l'IA et la RPA seront utilisées en tant qu'outils d'aide. Bon, les freins, je dirais que c'est plutôt au niveau de la maîtrise des outils.

AS : Qu'est-ce qui pousse à utiliser des outils basés IA et RPA ?

OM : RPA, c'est surtout une facilité d'implémentation rapide, d'un besoin qui, c'est mon point de vue, est une béquille provisoire. Les vendeurs de RPA ne le voient pas comme ça. Pour eux, c'est la nouvelle façon de programmer ou la nouvelle façon d'implémenter des automatismes. Il faut savoir que la RPA va simuler une action qui est faite par l'utilisateur. Vue de ce point de vue-là, la RPA utilise des ressources trop importantes pour les tâches qui sont faites, donc on peut dire que c'est provisoire pour dire ok, on aimerait bien réorganiser un certain process, aller vite, s'assurer que ça tient la route. Faire de la RPA fait sens parce que ça va vite et on ne modifie pas la structure information derrière de la banque, mais implémenter la RPA en disant que ce sont de nouveaux programmes, ça peut être dangereux parce qu'on aura alors une dépendance d'une sous-couche, l'applicatif, et si lui évolue, il faut aussi faire évoluer la RPA. Donc, dans ce cas-là, on se retrouve dans une situation où ça coûte beaucoup plus cher que ce qu'initialement tu aurais prévu. Effectivement, implémenter la RPA, ça coûte moins cher mais à condition d'être de courte durée. Si ça reste longtemps, ça peut être très cher à mettre à jour. Par exemple, quand la RPA travaille sur l'applicatif, elle simule donc l'utilisateur, mais si

l'applicatif derrière change, il faut également adapter la RPA, donc les robots, ce qui représente un coût supplémentaire.

AS : Ok, donc les outils RPA seraient des outils temporaires qui ne sont pas voués à perdurer trop longtemps parce qu'ils représentent des coûts de mise à jour ?

OM : C'est ça. Je précise encore que c'est mon point de vue mais ce n'est pas comme ça que les vendeurs de RPA vont le mettre en avant. Effectivement, s'ils mettent les RPA en avant comme des outils temporaires, alors les coûts qui sont demandés actuellement sont trop élevés. Les robots sont trop chers, c'est pour ça qu'ils sont vendus comme des nouvelles façons de programmer plus rapides. Personnellement, je privilégie la RPA uniquement en tant que solution temporaire pour faire un projet minimum viable. C'est la nuance : la RPA ne doit pas modifier l'ensemble du processus. La RPA, l'idée, c'est qu'elle réplique juste ce qui est fait manuellement pour le faire automatiquement. À partir du moment où tu modifies les processus derrière, ce n'est plus de la RPA. La RPA, tu l'utilises juste pour imiter ce qu'un utilisateur ferait mais que ce n'est pas l'implémenter dans un programme derrière, sinon ça signifierait que ce n'est plus imiter un utilisateur. Au niveau des ressources informatiques, tu es plus optimal.

AS : À la BGL, l'accent est donc aujourd'hui plus prononcé pour la RPA que pour l'IA ?

OM : Tout à fait. C'est un geste répétitif, les robots sont moins chers qu'une personne.

AS : Vous avez déjà songé à sous-traiter les applications IA ou RPA, avec des entreprises très spécialisées, dans le sens où ce serait moins cher que de les créer en interne ?

OM : Pour sous-traiter de la RPA, ça risque d'être difficile parce que la plus-value de la RPA, c'est la connaissance métier. Implémenter pour que le robot imite ce qu'un utilisateur fait n'est pas une grande tâche. Si tu apprends à un robot à parcourir certains écrans d'une certaine façon, tu peux réutiliser ça à chaque fois. Donc, avec le temps, c'est juste en interne que ça doit être transposé. Alors, sous-traiter ça en externe, je ne vois pas directement la plus-value. Par contre, si tu me poses la même question pour l'IA, c'est tout à fait différent. Là, ça pourrait faire sens parce qu'au niveau IA, ça exige une certaine maîtrise technique à avoir pour bien l'implémenter. L'IA, c'est un outil qui doit être bien paramétré. Si l'IA n'est pas bien paramétrée, ça peut ne pas bien fonctionner comme tu veux, alors qu'avec la RPA, si tu lui dis de faire quelque chose, tu vois immédiatement les résultats. Avec l'IA, le niveau de maîtrise technique est plus élevé.

AS : L'idéal, ce serait d'avoir des personnes compétentes en IA en interne ?

OM : La question qui va se poser, c'est que c'est une technologie qui évolue très rapidement. Est-ce qu'en interne, les personnes qui ne sont en contact qu'avec leur propre environnement, pourront évoluer si vite, aussi vite qu'une start-up qui est en contact avec d'autres acteurs du marché financier, et acquérir une expérience d'ajustement de l'utilisation et d'appropriation de l'IA pour les besoins du secteur financier ? L'IA doit apprendre différents scénarios, différentes situations possibles, et plus elle est confrontée à des situations, plus elle apprend. C'est la même chose au sein d'une banque : si les gens se limitent à l'environnement de leur propre banque, ils n'ont pas de vue sur toute la problématique de la place financière. Ce sera plus difficile pour suivre technologiquement et être au top des évolutions.

AS : L'IA a besoin d'un grand nombre de données pour apprendre. Sous-traiter dans cette logique ferait sens parce que le sous-traitant aura des données de différents secteurs et donc pas que les données d'une seule banque ?

OM : Tout à fait. C'est aussi le principe de Google et Amazon qui mettent à disposition des services d'intelligence artificielle gratuits, comme par exemple la reconnaissance d'images ou la reconnaissance d'un contenu dans l'image. Ils mettent à disposition gratuitement les outils pour avoir des données pour entraîner leurs algorithmes. Une fois que l'algorithme est entraîné, c'est là que se situe la plus-value. Une fois que tu as entraîné l'algorithme, tu n'as plus besoin des données. La donnée sert juste comme un flux d'informations et chaque donnée qui arrive va venir ajuster l'algorithme : au plus tu as de données, au plus tu ajustes l'algorithme et une fois que l'algorithme est bien ajusté, qu'il a pris en compte les différentes constellations de données existantes, chaque donnée supplémentaire n'apportera plus de plus-value parce qu'elle ne va plus entraîner le modèle qui aura déjà été entraîné. Il entrera alors dans sa phase prédictive : quand une nouvelle donnée arrivera, il pourra prédire comment ça va évoluer et se terminer, donc plus besoin de nouvelles données.

AS : Mais peut-être qu'aujourd'hui une donnée sera comprise d'une certaine manière mais que demain ce sera d'une autre manière.

OM : Oui, c'est ponctuel, c'est sur une période de temps. Si des règles changent par exemple, si l'environnement change, tu auras à nouveau besoin de données pour réajuster le modèle à l'évolution de ton environnement. Admettons que ton environnement ne change plus, tu n'as pas besoin de nouvelles données pour ajuster ton modèle.

AS : Et à partir de quand on pourrait dire qu'on a assez de données ? Existe-t-il une échelle à considérer ?

OM : Il faut toujours faire attention à ne pas surentraîner ou trop spécialiser l'IA, ton modèle plutôt, parce que si le modèle devient trop spécialisé, il ne sera plus prédictif. Si tu veux identifier la fraude, le modèle doit rester assez générique parce qu'à partir d'un moment, sinon, le modèle risque de devenir trop spécialisé et il ne sera pas assez large pour prendre en considération différents scénarios.

AS : Pour la fraude par exemple, il se spécialiserait pour les 90% de cas qui arrivent le plus régulièrement et donc ne prendrait pas en compte les 10% restants, alors qu'un modèle plus générique va capter presque 100% des fraudes ?

OM : Oui, on ne peut en fait jamais parler de 100% mais effectivement, si tu gardes ton modèle un peu plus large, il te permettra également d'identifier des cas de fraudes qui ne sont pas réguliers. Les fraudeurs sont innovants, donc si ton modèle se spécialise trop, il risque de ne pas voir les nouvelles techniques des fraudeurs. Il faut un équilibre entre les faux-positifs et les positifs corrects. Si tu arrives à un point où tu n'as que des positifs corrects, le modèle est trop spécialisé.

AS : Ok. Et dans quelle mesure ces nouvelles technologies permettraient à la banque de proposer de nouveaux produits ? Je pense notamment à des produits pour les assurances ou des conseils de trading automatiques.

OM : Vu qu'on apprend à mieux connaître les clients, il sera effectivement possible d'identifier les éventuels besoins des clients et donc de leur proposer de nouveaux produits. C'est envisageable, mais toujours avec la question de la GDPR. On n'a pas le droit d'utiliser des données sans le consentement du client. C'est un peu une barrière dans la connaissance approfondie du client parce que c'est une protection pour lui. Proposer de nouveaux produits comme des conseils automatiques, oui, mais seulement si le client a accepté qu'on utilise ses données pour mieux le servir.

AS : Le GDPR c'est donc à la fois une bonne chose mais aussi un frein à l'utilisation d'outils basés sur l'IA ?

OM : Oui, c'est un peu comme sur internet : tu acceptes les cookies ou tu ne les acceptes pas. Si tu les acceptes, tu as de la publicité qui n'est pas forcément dérangeante parce qu'elle est

spécialisée par rapport à ton profil. Si tu ne les acceptes pas, tu vas quand même recevoir des publicités mais qui ne sont pas dans ton domaine d'intérêt et vont te gêner. Mais oui, il faut toujours peser le pour et le contre de la protection de l'utilisateur.

AS : Ok, je vois. Et existe-t-il une crainte que l'IA génère des comportements de masse ? Mon père m'a parlé de ça l'autre jour : des algorithmes qui ont pris des décisions tous ensemble au même moment et ça a créé un petit crash boursier. Est-ce que ça pourrait être un risque lié à l'IA ?

OM : Effectivement, c'est possible, mais c'est l'IA ou pas ? Parce qu'on confond souvent l'IA avec des algorithmes très puissants. À la base, de ce que j'ai appris, l'IA est un algorithme qui lui-même peut s'autocorriger lorsqu'il constate par lui-même qu'il a commis une erreur. Donc, l'IA est dotée d'une possibilité de constater des erreurs et d'une possibilité d'agir, de réajuster. Et ça, c'est plutôt l'exception. On fait l'amalgame entre l'IA et des algorithmes très puissants. À partir du moment où l'algorithme ne peut pas se corriger lui-même, ce n'est pas de l'intelligence artificielle. Pour revenir à ta question sur les comportements de masse, avec le crash boursier, c'est possible avec des algorithmes programmés à réagir à une certaine situation. Oui, si cette constellation se produit, tous les algorithmes vont réagir en même temps, mais ce n'est pas de l'IA.

AS : Pour que l'IA puisse s'autocorriger, ça passe par la façon dont un outil IA a été conçu au départ ?

OM : En fait, par analogie, une formation sur l'IA a montré une camionnette sur un terrain vague. Elle était commandée par un ordinateur mais l'ordinateur ne savait pas conduire, il savait juste regarder la route devant lui. On lui a demandé de s'assurer que le chemin se trouve toujours au milieu du pare-brise et si ce n'était pas le cas, il avait un volant qu'il pouvait utiliser pour ajuster sa trajectoire. Au début, ça allait de gauche à droite jusqu'à un moment donné où l'ordinateur a compris qu'il pouvait utiliser le volant et que tourner le volant pouvait ajuster le chemin au milieu du pare-brise. Pour en revenir à l'IA, oui, elle doit être dotée d'un genre de jeu qu'elle peut utiliser. Sans vraiment programmer l'IA, tu lui donnes des instructions sur comment elle doit se comporter si elle constate une anomalie. La seule contrainte, c'est que le chemin devait se trouver au milieu du pare-brise et le seul moyen qu'elle avait pour ajuster ça, c'était le volant, on ne lui disait pas de tourner à gauche ou à droite.

AS : Ok, l'IA passe donc par une bonne définition des contraintes au départ ?

OM : C'est ça.

AS : Ok. Est-ce que l'IA pourrait standardiser trop des décisions au point de réduire trop les risques, ce qui serait néfaste pour l'économie qui a besoin d'intermédiaires justement capables de prendre des risques ?

OM : Effectivement, c'est possible. Plus tu as des informations, au mieux tu peux prédire les risques. En tant que banque, tu essaies de minimiser les risques. Si tu as beaucoup d'informations, tu peux arriver à un stade où tu te dis « je ne traite plus qu'avec des personnes qui présentent très peu de risque » et donc à discriminer d'autres acteurs économiques, ne pas leur prêter d'argent par exemple, et donc la banque ne prendra plus de risque, ce qui signifie mourir. Et ça va aussi influencer les comportements des clients dans le sens où ça va obliger les acteurs économiques à respecter un niveau de risque maximum exigé par l'intelligence artificielle. Au plus tu respectes les règles de l'IA, au plus tu reçois de points, par exemple, donc de meilleurs prix tu auras. C'est un peu comme les impôts incitatifs où si tu investis dans certains secteurs, tu peux déduire une partie de ta base imposable. Tu as une influence sur les acteurs économiques, aussi avec l'IA : une forte influence sur les acteurs économique de sorte qu'ils ne sont plus autonomes.

AS : Oui, un peu comme l'application en Chine qui évalue les gens selon leurs bonnes/mauvaises actions ?

OM : Oui, c'est un bon exemple avec la Chine. Comme acteur individuel en Chine, tu es dans un engrenage où tu fonctionnes comme c'est exigé ou alors tu es écarté et tu ne bénéfices de plus rien. Le risque c'est d'écarter certains êtres humains parce qu'ils ne sont pas assez compétitifs pour faire partie du marché économique. C'est un peu comme les voitures autonomes : la voiture de niveau 5 qui n'existe pas encore, ce serait une voiture super prudente, encore plus prudente qu'un être humain. Le risque c'est que certains acteurs économiques n'auront plus le droit de participer au marché économique car ils seront jugés trop risqués.

AS : Dans ce cas-là, il faut aussi donner un niveau de risque acceptable. Ce n'est pas l'individu qui détermine ce risque. Il faudrait dicter un niveau de risque au modèle basé sur l'IA ?

OM : Oui, comme vous dites. Il faudrait définir ce que l'IA a le droit de prendre en considération pour ajuster son algorithme. Aux États-Unis, des algorithmes sont arrivés à des conclusions sur des individus à l'embauche où c'était décidé que certaines personnes ne valaient pas la peine

parce qu'elles étaient plus propices à l'absentéisme. Il faudrait donc interdire à l'IA de prendre en considération certains paramètres.

AS : Le risque qui réside dans l'IA, c'est que l'humain édicte des contraintes peu éthiques en quelque sorte ?

OM : Oui, toutes les dérives ne se sont pas faites du jour au lendemain. Quand tu regardes l'histoire, chaque dérive c'est un truc qui a progressé de plus en plus avec le temps. Ce sera sans doute la même chose avec l'IA.

AS : Oui, je pense aussi. On va pouvoir passer à la deuxième partie. Quels sont les outils IA utilisés par la banque ? Quelles sont les conséquences positives ou négatives de leur utilisation ?

OM : En conformité, fraude ou crédit, je pense qu'on n'utilise pas encore d'outil IA. On a quelque chose pour détecter la fraude, mais c'est plutôt un algorithme très poussé, ce n'est pas encore de l'IA. Pour les crédits, c'est peut-être à l'étude, je ne sais pas.

AS : Pourquoi l'outil fraude n'est pas de l'IA ? Il n'apprend pas par lui-même ?

OM : De ce que je sais, ce n'est pas un outil qui apprend par lui-même. C'est un outil dans lequel tu déposes un algorithme, donc des règles complexes, sur base de différents critères, pour vérifier si c'est une fraude ou pas. Si c'est de l'IA, j'ai dû mal comprendre.

AS : Et quelles sont les perspectives d'utilisation d'outils IA sur ces risques ?

OM : C'est à l'étude. Il ne faut pas oublier la question de la sous-traitance, donc externaliser parce que l'IA a besoin de beaucoup de données. La masse de données pour une vraie IA au Luxembourg, ce n'est pas là. En Belgique ou en Italie, ils ont des volumes de données plus conséquents pour permettre à une IA d'apprendre.

AS : Ces outils ne sont pas partagés avec le Luxembourg ?

OM : C'est la question du GDPR. Il faut protéger les utilisateurs, donc on ne centralise pas toutes les données. Encore une fois, c'est un frein, mais un frein positif. En Chine, des gens n'ont plus le droit de prendre le TGV rapide parce qu'ils ont été notés négativement, c'est un truc où tu te dis « Wow ! ». Tu te retrouves dans un engrenage où tu es écarté et tu ne sais plus corriger le tir. Un gros challenge de l'IA, ce sera d'éviter d'écarter l'être humain. Chaque être

humain doit pouvoir refuser que ses demandes soient traitées par des algorithmes. Je pense que c'est prévu par la GDPR. Je pense que le client peut refuser que sa demande de financement soit traitée par une machine. Je ne suis pas certain, mais je pense que ça existe.

AS : Ok. On peut passer à la dernière partie. Quels sont les outils RPA utilisés par la banque ? Quelles sont les conséquences positives ou négatives de leur utilisation ?

OM : Au niveau conformité, je ne sais pas si c'est d'application, mais sur un plan théorique, oui, c'est possible de mettre en place des processus répétitifs pour vérifier que toutes les opérations soient conformes. La RPA peut aider, parce que c'est rapide. Concernant la fraude, là je ne sais pas si la RPA peut aider. Concernant les crédits, oui, la RPA peut aider pour redéfinir la façon de traiter les demandes des clients. Dans un contexte Minimum Valuable Product (MVP) où tu essaies d'implémenter un processus, pour que ça aille plus vite, tu peux avoir recours à la RPA.

AS : Pour mettre en place un outil RPA, il faut des règles fixes ? C'est l'objectif des tâches répétitives, comme pour la conformité, des règles pour être conforme ?

OM : Oui, la RPA va mettre en place les contrôles pour assurer la conformité. Pour les crédits, il ne faut pas de besoin d'interprétation, sinon ce n'est plus de la RPA. Quand la RPA se retrouve dans une situation où ça sort de l'ordinaire, c'est possible d'avoir un appui de l'IA, mais en réalité ce sont plutôt des algorithmes poussés.

AS : Comment distinguer l'IA des algorithmes très poussés ?

OM : À partir du moment où l'être humain n'a plus besoin d'intervenir pour définir un nouveau cas de figure, c'est de l'intelligence artificielle. Un algorithme poussé, ça va être un assemblage de différents contextes prévisibles. La complexité de l'algorithme, c'est un nombre de cas prévus pour anticiper. Avec l'IA, tu ne prévois rien, c'est elle qui s'ajuste au fur et à mesure de l'arrivée de nouveaux cas. On n'a pas besoin de dire à l'IA « voici une nouvelle information à prendre en considération pour détecter la fraude », sinon c'est un algorithme poussé avec une action humaine où on ajoute une information sur la fraude. C'est un amalgame entre les deux. L'algorithme prend des décisions oui, mais des décisions prévues et anticipées, donc ce n'est pas de l'intelligence artificielle.

AS : Ok, je vois. J'ai terminé avec mes questions. Merci beaucoup pour cet entretien.

OM : Je vous en prie. Et que ça se passe bien avec votre mémoire.

AS : Merci. Bonne continuation.

OM : Merci. Bonne journée.

Annexe 4 : Ruben Olieslagers – Responsable du CFO Office (Data Management, Validation Committees, & Environment and Socializing Governance) chez BNP Paribas Fortis

Alexandre Senden (AS) : Bonjour ! Tout d'abord, je tiens à vous remercier pour cet entretien. Avant de commencer, je vais rappeler les grandes lignes de mon mémoire et les sujets que l'on va aborder aujourd'hui. Globalement, ce mémoire a pour but d'étudier l'apport de l'intelligence artificielle et de la robotic process automation pour améliorer la gestion des risques de conformité, fraude et crédit sur les places financières belges et luxembourgeoises. Ces interviews me permettront d'établir les tendances du marché en termes d'IA et RPA sur ces places et pour ces trois risques. J'ai donc scindé mon questionnaire en trois parties. D'abord, des questions générales. Ensuite, deux sections, une sur l'IA et une sur la RPA. Chacune traitera des trois risques abordés dans mon mémoire.

Ruben Olieslagers (RO) : Parfait.

AS : Nous pouvons commencer avec les questions générales. Premièrement, quel poste occupez-vous au sein de Fortis ?

RO : Je suis responsable du CFO Office, avec trois parties là-dedans. Une première partie axée sur le data management (donc qualité des données, nouveaux développements) et dans ce cadre-là, on a la réglementation BCBS 239, que tu dois connaître. Là, je suis responsable pour assurer une bonne qualité des données et j'ai des contacts avec le département risque, le département finance, le business, *etc.* On s'assure que les données sont de bonne qualité et on s'assure des contrôles. Une deuxième partie de ma fonction, c'est que dans notre organisation, nous avons un comité qui s'appelle le Exceptional Transaction Validation Committee et New Activity Committee, donc chaque fois que la banque lance une nouvelle activité, ça va passer dans ce comité et autour de ce comité, on a différentes fonctions comme legal & tax, risk, compliance, data, finance, *etc.* Mon rôle ici, c'est d'assurer que le business case tient la route. Est-ce que ça va rapporter ou juste coûter de l'argent ? En plus de cette deuxième casquette « nouvelles activités », j'ai une troisième casquette, la casquette ESG (Environment and Socializing Governance), ça bouge beaucoup dans ce cadre-là : green deal, *etc.* Les banques doivent faire de plus en plus de reporting pour soutenir la transition vers la neutralité carbone. Mon rôle ici, c'est le responsable pour ce programme, comme un manager, avec des contacts avec beaucoup d'autres départements. Donc, trois casquettes.

AS : Ok, je vois.

RO : Et comment j'ai des affinités avec IA et RPA ? Pour RPA, c'est quelque chose qu'on essaie de faire aussi pour la finance : automatiser certaines interventions manuelles le plus possible parce que l'intervention des gens, ça coûte des ressources. Je suis aussi en relation avec RPA dans le cadre des nouvelles activités parce que la banque est en train de se réorganiser. Si tu as un problème avec ta carte, tu vas dans l'agence dire que tu as cassé ta carte, puis un manager va commander une nouvelle carte pour toi. On passait donc souvent par l'agence pour plusieurs services à l'époque, mais aujourd'hui on va tenter d'éliminer de plus en plus l'étape agence. Tu pourras appeler un numéro et expliquer ton problème puis ton problème sera peut-être résolu avec une machine, ou une personne si ton cas est plus complexe. Quand on parle de l'intelligence artificielle, c'est la plupart du temps l'équipe data management qui s'occupe de la mise en place des applications IA dans la banque. C'est aussi possible pour la finance, par exemple faire des prédictions pour le futur, donc intégrer l'IA dans le département finance. On a déjà eu des propositions de boîtes de consultance mais on n'a pas avancé là-dedans, au niveau finance. On n'a pas encore de grandes updates au niveau finance chez nous pour cette nouveauté. Cependant, dans l'équipe data, on a un gros pilier IA avec une vingtaine ou une trentaine d'experts. C'est surtout pour des applications crédits, fraudes ou compliance. On ne fait pas tous les développements seuls dans notre coin, on regarde aussi ce qui a été développé en IA ailleurs par les FinTechs. Il ne faut pas oublier qu'une banque, c'est une organisation assez conservatrice, donc il faut réfléchir avant d'intégrer ces techniques. On a fait ça aussi pour RPA, on a travaillé avec Accenture qui est assez spécialisée dans la robotic process automation. Un souci, c'est qu'avec RPA, tu automatises quelque chose mais si la personne quitte l'entreprise après, ce n'est pas toujours facile de faire les changements. Tu développes en interne mais alors ces gens-là ne peuvent pas quitter ou alors tu fais ça avec des consultants externes mais alors pas pour des missions éternelles mais dans des délais bien définis. Il faut faire attention parce qu'après des changements, plus personne ne comprend, une fois que la personne qui a développé a quitté.

AS : Ok. Alors passer par des externes pour RPA, c'est une sorte de frein, c'est mieux de développer ça en interne ?

RO : Exactement. Il faut savoir aussi que dans le département des finances, la plupart des gens sont très opérationnels, c'est-à-dire qu'ils font le même travail depuis des années, donc ils ne sont pas très familiers avec RPA. Ils n'ont pas les compétences et s'ils sont ouverts pour le

faire, ils tuent leur propre job, tu comprends ? Donc, pas vraiment d'initiative de leur côté pour faire beaucoup d'automatisations. Parfois, c'est via des pressions qui viennent de plus haut qu'on arrive à trouver des solutions pour améliorer l'efficacité. Le souci avec RPA, c'est la certaine complexité dans les process, ce n'est pas toujours aussi facile. On développe quand même des EUC (End User Computing), pour faciliter la vie. Des gens dans l'équipe ont la maîtrise et font des EUC qui seront intégrés, mais ce n'est pas la majorité des gens, c'est plutôt une minorité.

AS : Ne faudrait-il pas engager des experts en interne ?

RO : Il faut les engager, donc c'est un frein, donc parfois on engage quand même mais pas en masse, c'est l'exception. Il faut faire une distinction : IA s'applique surtout sur la partie compliance, donc des screening, ce genre de choses, RPA c'est quand on utilise toujours les mêmes formats.

AS : IA actuellement, vous l'utilisez plutôt pour des applications de détection de fraude et des applications en conformité mais peu pour les crédits ?

RO : Oui, des développements se font là-dedans, en crédit, mais la plupart des modèles ont été développés en 2005-2006. On a des modèles de rating. On a beaucoup développé pour ça dans les années 90 et jusqu'en 2007. Beaucoup de ces modèles sont faits de la façon classique : on collecte des données et on applique une logistic regression ou une discriminant analysis. On a utilisé ces modèles pendant plusieurs années. Maintenant, on commence à réfléchir pour IA, mais ce sont des tests pour une population comme retail banking où on a des bases de données de grande taille, des applications de scoring. On voudrait harmoniser le nombre de modèles, mutualiser l'utilisation de certains modèles, même si certains modèles sont très liés à la situation en Belgique par exemple, donc pas top pour Paris ou l'Italie.

AS : Ok, je vois. Je vais revenir un peu en arrière. Globalement, quel est le degré d'implication de BNP Paribas Fortis en termes d'IA et de RPA ?

RO : Pour l'IA, on a quand même une équipe assez importante, côté data management. On a déjà des applications dans le cadre compliance, un peu côté fraude aussi, mais on regarde toujours pour trouver de nouvelles applications IA. Je crois que la volonté du data management est parfois plus élevée que la volonté du business pour intégrer des technologies IA. Enfin, tu vois, les gens qui sont dans ces différentes fonctions ne sont pas forcément au courant des

différentes possibilités que peuvent offrir ces nouvelles technologies. Il y a quelques années, data management a organisé un training où différentes FinTechs pouvaient se proposer, mais quand une FinTech se présente, ce n'est qu'une audience de 15-20 personnes, ce n'est pas beaucoup.

AS : On constate donc une forme de résistance à l'utilisation d'outils IA parce que ça va remplacer leur travail ?

RO : Oui, souvent. C'est rare qu'il y ait une approche bottom vers le top, c'est plutôt l'inverse, c'est imposé au final.

AS : Mais l'équipe data a-t-elle une vue assez poussée pour proposer des solutions adéquates ?

RO : L'équipe data a des contacts avec des consultants, ils participent à des séminaires. Dans ces séminaires, d'autres banques et d'autres consultants présentent leurs applications, alors on va se dire ok nous pouvons aussi appliquer ça chez nous. On a aussi eu des idées pour utiliser l'IA en business intelligence mais c'est quand même encore limité. On utilise aussi déjà l'IA pour les ChatBots.

AS : Je vais passer maintenant aux deux dernières parties parce que vous avez déjà fourni beaucoup d'éléments de réponse sans même que j'aie à poser les questions. Selon vous, quels sont les principaux facteurs qui permettent à BNP Paribas Fortis d'étendre son utilisation d'outils IA et RPA ? Par exemple, j'imagine, beaucoup de data pour l'IA ?

RO : Oui. Je dois dire qu'on fait partie d'un grand groupe, avec environ 200.000 personnes. On a donc quand même l'expertise pour faire pas mal de choses ou pour acheter cette expertise. La banque ne peut pas se permettre de dire qu'IA ou RPA ne nous intéressent pas, non, la banque est ouverte pour regarder les nouvelles opportunités, mais avec plusieurs vitesses dans la banque. C'est souvent comme ça avec les nouveautés, ce n'est pas toujours d'abord un succès. L'avantage, c'est qu'on a de grosses bases de données, donc on a accès à des choses pour bien développer des nouvelles choses, c'est pourquoi les universités sont intéressées pour travailler avec nous, parce qu'on a ces grandes bases de données.

AS : Le travail avec les universités, c'est avec un réel suivi des projets ?

RO : Oui avec des PhD. Le problème, c'est la source des données, on leur donne parfois accès mais les données doivent rester dans la banque. C'est vrai que Fortis avec notre Chief Data

Officer du groupe, nous sommes assez précurseurs, il a mis en place une équipe pour l'IA, avec 200 personnes je crois, sur 200 000, 30-40 étant de vrais experts en IA et d'autres gens ouverts sur la question mais il y a quand même moins d'experts sur les possibilités de l'IA.

AS : On en a déjà un peu parlé mais que pouvez-vous dire des outils IA utilisés chez Fortis sur les trois risques : conformité, fraude et crédit ?

RO : Sur l'IA, on a des doutes sur une sorte de discrimination qui peut se faire dans ces algorithmes. Tu traites de ça aussi ?

AS : Oui, car les algorithmes sont créés à l'image de la pensée humaine et sur des datasets qui contiennent parfois des discriminations, donc si l'humain ou le dataset possède un biais cognitif à la base, il va recréer ce biais, c'est un risque de l'IA.

RO : Est-ce que tu connais le Risk Magazine ? Tu peux trouver des infos intéressantes.

AS : Je vais regarder, merci. J'ai regardé pas mal les Big Four et les rapports au niveau européen.

RO : Tu peux aussi regarder la documentation du CEPS, Place du Congrès.

AS : Ok, je vais me renseigner.

RO : Encore une question ?

AS : Non, c'est parfait. Merci pour votre temps. On se recontacte par e-mail.

RO : Bon week-end alors Alexandre.

AS : Merci. Et bon match ce soir !

RO : Certainement !

Annexe 5 : Augustin Borsu – Responsable Analytics & AI et déploiement support chez BNP Paribas Fortis

Alexandre Senden (AS) : Bonjour. Avant de commencer avec mes questions, je vais d'abord faire un débriefing du sujet de mon mémoire et vous expliquer comment je vais conduire cet entretien. Globalement, ce mémoire a pour but d'étudier l'apport de l'intelligence artificielle et de la robotic process automation pour améliorer la gestion des risques de conformité, fraude et crédit sur les places financières belges et luxembourgeoises. Ces interviews me permettront d'établir les tendances du marché en termes d'IA et RPA sur ces places et pour ces trois risques. J'ai donc scindé mon questionnaire en trois parties. D'abord, des questions générales. Ensuite, deux sections, une sur l'IA et une sur la RPA. Chacune traitera des trois risques abordés dans mon mémoire.

Augustin Borsu (AB) : C'est noté.

AS : Commençons. Quel poste occupez-vous au sein de BNP Paribas Fortis ?

AB : Je suis team lead Analytics & AI et déploiement support donc notre équipe est en charge d'accompagner l'intégration des projets IA dans les systèmes de la banque. Donc lorsqu'un data scientist a développé un projet, il faut l'automatiser et définir la marche à suivre, le processus d'implémentation. On définit donc le processus. Mais nous ne faisons pas le run, nous contactons les équipes qui peuvent mettre ça en place. Ce que nous cherchons à industrialiser vise l'optimalité.

AS : Depuis quand occupez-vous ce poste ?

AB : L'équipe a été créée il y a un an en juin 2020 et avant ça, j'étais data scientist.

AS : Je vois. Globalement, que pouvez-vous dire sur le degré d'implication de BNP Paribas Fortis en termes d'IA ?

AB : Fortis est positionnée comme une smart follower, c'est-à-dire qu'on ne prend pas d'initiatives, on saisit plutôt les opportunités sur le marché mais on ne crée pas directement. Donc on garde une vue du paysage et quand on voit des opportunités intéressantes, on les intègre ou on les développe, nous ne sommes pas à la pointe mais tout à fait conscients qu'il faut suivre ces sujets et sélectionner les plus prometteurs en termes de rentabilité et efficacité, c'est-à-dire celles pour lesquelles le return on investment est le plus intéressant.

AS : Et si on reprend la même question sur le degré d'implication de BNP Paribas Fortis en termes de RPA ?

AB : Au niveau de la RPA, nous avons un département entier dédié à ce sujet sur lequel je n'ai pas la vision globale mais je pense qu'ils tournent avec une dizaine de use cases par an.

AS : Ok. Si vous deviez évaluer objectivement l'état d'avancement de BNP Paribas Fortis sur les thématiques IA et RPA par rapport au secteur, où la situeriez-vous ?

AB : D'après moi, nous sommes plus ou moins au même niveau que Belfius et ING, KBC sort du lot.

AS : Intéressant. Que pouvez-vous dire au niveau des principaux facteurs permettant à BNP Paribas Fortis d'étendre son utilisation d'outils basés sur l'IA et la RPA ?

AB : Le principal facteur pour l'IA c'est en termes de pression pour travailler plus efficacement. L'accent est mis sur l'Augmented Intelligence, donc faire en sorte que les gens effectuent leur travail de manière plus efficace. Par exemple, l'objectif est de faire en sorte que 2 personnes effectuent le travail de 10 maintenant. En fait, on se concentre sur l'optimisation des processus. Nous avons déjà quelques use cases qui ont fourni des rendements intéressants, notamment en termes de chatbot via l'IA, de détection de fraude, de marketing. Nous voulons aussi créer un outil « speech to text » qui est un peu plus innovant mais l'analyse est encore en cours. Au niveau RPA, comme je l'ai dit nous avons un département entier pour la RPA qui développe 10 use cases par an sur la robotique, notamment pour la reconnaissance de documents.

AS : Dans la même idée, quels seraient les principaux freins réduisant l'utilisation d'outils basés sur l'IA et la RPA par BNP Paribas Fortis ?

AB : Le plus gros frein c'est que dans un monde bancaire, il y a une forte sensibilité aux risques et les systèmes d'IA sont des modèles probabilistes et en proba il y a toujours un degré d'incertitude. Il faut donc réussir à convaincre les gens que les endroits où on applique ces modèles, le risque associé est acceptable. Alors évidemment cela implique de définir le degré d'incertitude que l'on veut prendre. Il y a toujours un besoin de convaincre les principales parties prenantes que le risque est limité.

AS : Je vois. C'est étonnant qu'il y ait autant de résistance sachant que les humains conduisent probablement à un taux de risque plus élevé.

AB : En effet, le taux de risque est plus faible avec l'IA qu'avec les humains mais l'impact peut être très différent également. Un autre frein est que dans la banque, on utilise plus JAVA que d'autres langages alors que nos data scientists travaillent plutôt avec R et Python. Donc c'est parfois un peu compliqué pour intégrer nos projets dans les systèmes IT. Bref, donc on a l'augmented intelligence qui ne requiert pas d'intervention humaine sauf dans quelques cas particuliers. Par exemple, nous avons un système de reconnaissance des clients à partir de documents. Si l'augmented intelligence trouve un match du nom du client avec les données de la banque, alors il n'y aura pas d'intervention humaine. En revanche, il arrive qu'il y ait des noms similaires et alors le système va regarder la date de naissance. Si après la date de naissance, il y a encore une incertitude qui persiste alors le cas est envoyé à un humain pour qu'il s'occupe de l'incertitude mais pas de tout le processus. Ce système fonctionne comme une feedback loop et est réentraîné régulièrement. Donc, si le modèle n'est pas sûr à 100%, il y aura une décision humaine. Le temps de gestion des transactions a été considérablement réduit grâce à cet outil.

AS : Ce sont déjà de beaux progrès. Y a-t-il un accent prononcé sur l'une ou l'autre de ces technologies ? Et si oui, pourquoi ?

AB : Oui, sur RPA du fait que nous avons un département dédié. Ceci est d'ailleurs en ligne avec la stratégie du groupe qui souhaite améliorer et automatiser les processus, même si on peut le faire avec l'IA, la RPA suggère des progrès pas trop coûteux, rapides et efficaces.

AS : Tout à fait. Est-ce que vous sous-traitez tout ou partie de l'IA ou RPA vu leur côté spécialisé ?

AB : Alors, c'est très compliqué pour des raisons d'accès aux données parce que tous les systèmes IA sur les données clients impliqueraient de devoir donner les accès à des tiers. La banque doit définir son Data Risk Appetite et dépend toujours de la GDPR. Ce qu'on sous-traite c'est parfois des capabilities qui ne nécessitent pas de recourir aux accès clients. On ne peut pas envoyer nos données à des contreparties parce qu'on s'expose alors à des databreaches, au hacking, qu'ils utilisent nos données pour entraîner des modèles *etc.* Nous utilisons donc principalement des outils qui peuvent être développés en interne, c'est un requirement du Data risk appetite de la banque qui est relativement limité. On est très rigoureux à ce niveau-là. Cependant, on peut faire appel à des tiers si l'utilisation de nos données n'est pas requise. Nous l'avons fait avec un outil de reconnaissance vocal qu'on a intégré dans nos use cases.

AS : Est-ce que vous envisagez de filialiser des fonctions, très liées à ces nouvelles activités, pour les rendre plus dynamiques via des fintechs ? (Par exemple, une fintech pour l'octroi de crédits qui propose une solution basée sur l'IA).

AB : On fait du market watch, tous les quaters on invite des fintechs qui viennent présenter un produit intéressant et si on trouve des produits suffisamment intéressants alors un partenariat est envisagé. On a toujours ici le requirement que l'outil soit développé en interne et donc sans sortie de données vers des tiers. Cela a par exemple été le cas avec le développement d'un SAAS dans le cloud de la banque. On préfère en général les sociétés qui ont un niveau élevé de sécurité et certifications parce qu'évidemment, on s'expose au risque de réputation si on perd des données.

AS : Ok et d'ailleurs à ce sujet, la GDPR n'est pas un frein également pour former des partenariats ?

AB : La GDPR n'est pas forcément un problème. Si on partage les données, les conditions de partage de données et les conditions applicables au niveau GDPR seront incluses dans le contrat avec les entités.

AS : Dans quelle mesure ces nouvelles technologies permettront à BNP Paribas Fortis de proposer de nouveaux produits ? (Par exemple : assurances, conseils trading automatiques...)

AB : C'est en cours, il y a un assistant qui a été créé au niveau du groupe sur la gestion des portefeuilles du groupe mais il est relativement faiblement développé pour le moment. La priorité est plutôt sur l'étendue des services existants, peu sur la création de nouveaux produits. Donc l'objectif est d'améliorer les outils actuels plutôt que de s'attaquer à la création de nouveaux outils. On vise quand même à fournir des services 24h/24 via des chatbots qui seraient capables de répondre à des demandes relativement simples comme bloquer/débloquer une carte.

AS : Ah oui, c'est la stratégie du groupe don vous parliez. Aurait-il une crainte que l'IA génère des comportements de masse ? Que les algorithmes prennent des décisions tous en même temps impliquant ainsi des crashes boursiers comme on l'a connu dans le passé par exemple ?

AB : Déjà il faut se rendre compte que depuis la crise, les banques de détail et banque d'investissement ont été splitées. Mais oui, il y a des risques sur les modèles : on s'inquiète plutôt sur les risques de biais. C'est-à-dire un risque de faire continuer les préjudices et qu'ils soient renforcés. Nous faisons très attention au risque de biais sur les modèles, en data science

on dit garbage in garbage out : si les data ont un biais en entrée, alors elles auront un biais en sortie puisque les modèles tirent des conclusions basées sur les données. Le data scientist pourrait introduire un biais dedans mais c'est là-dessus qu'ils travaillent, quand on crée des règles expertes, il faut faire attention à ne pas inclure les biais, notamment sur la race, le genre, les préférences sexuelles, *etc.* Par exemple, si le modèle est capable de déterminer si le client a des allocations familiales, il va probablement conclure que dans la plupart des cas, ce sont des femmes et donc il contiendra un biais et c'est pour ce type de raisons qu'il faut considérer les données et ne pas inclure celles qui peuvent conduire à un biais. Alors, oui le modèle pourrait fonctionner avec des biais mais est-ce éthique ? Nous considérons beaucoup l'aspect éthique, parfois en développant des modèles moins performants mais plus éthiques.

AS : En effet, à ce sujet je lisais justement l'autre jour que des applications IA comportaient parfois des biais dans les données en entrée et conduisaient à des solutions discriminantes pour des groupes de population. L'IA pourrait standardiser des décisions et réduire trop les risques de crédit, ce qui est potentiellement néfaste pour l'économie qui a besoin d'intermédiaires capables de prendre des risques. Qu'en pensez-vous ?

AB : C'est le principe du coût du risque, plus un client est risqué, plus le taux va augmenter, après on lisse ça de manière à faire en sorte que si l'algo s'est trompé, on n'ait pas trop de soucis. Dans les modèles de risque, c'est différent du reste parce qu'ils doivent être soumis à la BNB (Banque Nationale de Belgique) et à l'ECB (European Central Bank) et donc sont très contrôlés.

AS : Ok, on va maintenant passer aux deuxièmes et troisièmes parties spécifiques à l'IA et la RPA. En termes de risque de conformité, fraude et crédit, que pouvez-vous dire sur les outils d'IA utilisés à BNP Paribas Fortis ?

AB : Nous souhaitons développer un service de chatbots pour être disponible 24h/24, notamment pour des problèmes qui reviennent régulièrement et dont le traitement peut être facilement automatisé puisqu'il est systématique. On peut également revenir ici à l'exemple de l'Augmented Intelligence qui permet de classer des documents et où des données sont insérées dans les systèmes de la banque, et il y a un outil IA qui donne un degré de confiance sur la reconnaissance du nom sur un document par rapport aux données de la banque. Ce n'est pas simplement un feedback à l'humain, c'est-à-dire que l'humain n'intervient que si le modèle rencontre une incertitude mais si la reconnaissance des données trouve un match dans les

données de la banque, l'humain n'est pas requis. Le système prend en charge d'autres facteurs pour identifier un client comme le code postal, la date de naissance. En compliance, nous avons un use case en cours, c'est le speech to text dont nous parlions tout à l'heure et l'idée c'est que quand on vend un produit de crédit ou d'assurance, la personne qui vend a l'obligation de présenter certaines infos aux clients et donc pour le moment, certains appels téléphoniques sont sélectionnés au hasard et quelqu'un va écouter tout l'appel pour vérifier que ce qui doit être dit a été dit. Nous avons un système IA, donc automatisé, qui va gérer ça parce que ce sont de très longs appels. L'outil détecterait donc que ce qui doit être dit l'a bien été. L'outil va signaler les appels pour lesquels il semblerait qu'il y ait un problème et un humain peut repasser derrière pour vérification.

AS : Quelles sont les conséquences positives et négatives de ces utilisations (ex : amélioration(s), baisse des coûts, rapidité d'exécution, réduction de personnel, etc.) ?

AB : Nous avons des business cases après la période use cases qui établissent les cost savings et permettent d'évaluer la performance financière d'une nouvelle implémentation. On s'aperçoit également qu'il y a une amélioration des conditions de travail puisqu'il ne faut plus se concentrer sur la partie répétitive, mais plutôt sur les tâches à plus haute valeur ajoutée. Pour les clients aussi, il y a des aspects positifs puisqu'on est plus disponible, notamment via le système qui permettrait d'étendre les horaires de call centers en utilisant des bots (24h/24). Sur les aspects négatifs, il y a toujours le risque qu'un modèle ne soit pas suffisamment compris, que la provenance des données ne soit pas comprise, etc. pour prendre une décision informée sur ce que le modèle dit. Chez Fortis, nous avons vraiment pleine conscience de ça de manière à ce que ces risques soient gérés.

AS : J'ai entendu qu'il y avait une nouvelle réglementation par la Commission européenne sur l'IA ?

AB : Elle n'est pas encore passée mais on a déjà fait une étude interne sur les documents de travail donc a priori ce sont des choses qu'on prend déjà en compte, chez Fortis on est assez prudents, conservateurs.

AS : Comment pouvez-vous vous préparer à ces nouvelles réglementations ?

AB : Eh bien, il y a ce qu'on appelle le CEO data governance que plusieurs personnes suivent et qui sont des sortes de recommandations publiées en interne et pour lesquelles on s'assure qu'on est préparés.

AS : Quelles sont les conséquences positives et négatives de ces utilisations (ex : amélioration(s), baisse des coûts, rapidité d'exécution, réduction de personnel, *etc.*) ?

AB : Là aussi, les aspects positifs se retrouvent sur un accroissement des tâches à plus haute valeur ajoutée puisque les robots permettent de prendre le pas sur des tâches répétitives et pour lesquelles un faible niveau intellectuel est requis comme des tâches un peu stupides de copier/coller *etc.* Dans la même idée que pour l'IA un risque c'est que les robots ne soient pas compris en interne, on a donc besoin de personnes capables de comprendre les processus, c'est-à-dire des experts qui peuvent suivre ce que le robot est en train de faire afin d'améliorer le processus à l'avenir parce qu'un robot n'évolue pas de lui-même et ne se remettra pas en question à l'image de l'humain. Il faut donc toujours garder des experts qui savent comprendre et gérer les robots et savent ce qu'ils font.

AS : Je vois. Je pense que ceci marque la fin de cet entretien. Je vous remercie grandement pour vos réponses et votre temps.

AB : Merci à vous.

AS : Bonne fin de journée.

AB : Également.

Annexe 6 : Marc Aguilar – Chief Data Officer à la BGL BNP Paribas

Alexandre Senden (AS) : Bonjour ! Je vais commencer par une brève explication de ce mémoire. Ensuite, je commencerai à vous poser mes questions. Globalement, ce mémoire a pour but d'étudier l'apport de l'intelligence artificielle et de la robotic process automation pour améliorer la gestion des risques de conformité, fraude et crédit sur les places financières belges et luxembourgeoises. Ces interviews me permettront d'établir les tendances du marché en termes d'IA et RPA sur ces places et pour ces trois risques. Pour ce faire, j'ai scindé mon questionnaire en trois sections. La première traitera de questions générales. Ensuite, puisque nous considérons trois risques et deux nouvelles technologies, les deux autres sections traiteront de l'IA d'abord, vue sous les trois risques et puis de la RPA vue sous les trois risques également.

Marc Aguilar (MA) : D'accord. Pour la RPA, je ne suis pas en charge, donc je ne sais pas vraiment où se situe la banque mais je connais le potentiel de la RPA.

AS : Pas de problème pour ça. Chacun des intervenants a une certaine vision. J'ai déjà fait par exemple une interview avec Orce Marinkovski de la BGL qui est plus axé RPA. On va commencer avec les questions générales. Quel poste occupez-vous au sein de la BGL ?

MA : Je suis Chief Data Officer.

AS : Depuis quand ?

MA : Je suis dans la banque depuis 26 ans mais j'occupe cette fonction depuis octobre 2015.

AS : Que pourriez-vous dire sur le degré d'implication de la BGL en termes d'IA et de RPA ?

MA : Je pense qu'on a démarré la création de l'IA en 2016. On a plusieurs productions aujourd'hui, notamment dans la détection de fraudes au paiement et dans le suivi compliance typiquement pour Know Your Transactions donc on va établir des profils des clients et on essaye d'identifier si les transactions sont conformes par rapport au profil du client, alors ça peut être en termes de montants, d'activités, de paiements in et out. On a démarré une réflexion de validation des paiements par l'IA c'est-à-dire que, ce qu'il peut arriver c'est que si quelqu'un paie sur un compte qui n'a pas assez de fond, ça va bloquer la transaction. Tu peux avoir deux millions sur un autre compte et évidemment les systèmes ne sont pas connectés ou il n'y a pas d'intelligence à ce niveau-là alors c'est bloqué, donc avec l'IA on essaie de ne pas bloquer ces paiements qui retombent sur le relationship manager qui doit les visualiser et libérer ces

payements si les fonds sont sur un autre compte. Avec un profil global, on va savoir que la personne dispose d'autres fonds sur un autre compte. La machine décide quand même alors d'exécuter la transaction, voilà un peu les applications qu'on a.

AS : Ok. Donc, c'est pour l'IA ?

MA : Oui. Pour RPA, je ne connais pas bien. Ce sont des programmes qui essayent de lire en automatique des documents et qui vont insérer de la data de manière automatique pour éviter les tâches manuelles qui sont très répétitives.

AS : Ok. Si vous deviez évaluer objectivement l'état d'avancement de la BGL sur les thématiques IA et RPA, où la situeriez-vous ?

MA : Globalement, je pense que nous sommes dans les meilleurs parce que BNP Paribas a poussé les choses depuis Paris. Je pense qu'on a eu le premier CDO, le premier lab d'IA. Donc, je pense que nous sommes dans le premier tiers, mais les autres aussi, ils investissent et recrutent pour ça.

AS : Et le fait que BNP Paribas c'est un groupe relativement gros par rapport aux autres, la plus grande banque européenne, ça a des impacts sur l'utilisation de ces outils ?

MA : Je pense que oui parce qu'on a une équipe assez pointue à Paris et surtout parce qu'on commence à réutiliser des algorithmes qui ont été développés ailleurs. BNP est en avance en Europe, mais par rapport aux États-Unis, l'Europe a du retard. En Europe, ils sont certainement dans le premier tiers.

AS : Le fait qu'il existe des degrés de validation pour arriver à un « oui » du top management, c'est-à-dire qu'il faut passer beaucoup de degrés de validation, est-ce que ça ne va pas ralentir un peu le processus ?

MA : Je pense que ça n'a rien avoir avec IA et RPA, mais avec la gouvernance de la banque. En gros, les décisions ne sont pas plus faciles ou moins faciles avec ces questions, ça ne dépend pas de ça. Je pense que ces sujets sont en compétition avec tous les autres, digitalisation, optimiser les processus, donc il faut toujours faire un business plan pour comprendre les coûts. Si c'est porteur, qu'on a des gains de productivité, alors ça passe.

AS : Ok. Et quels sont les principaux facteurs qui permettent à la BGL BNP Paribas d'étendre son utilisation d'outils basés sur l'IA et la RPA ?

MA : Plusieurs. Le premier c'est d'avoir des idées et de comprendre la technologie où aujourd'hui on peut l'utiliser. En gros, c'est comme du développement informatique sauf qu'on n'utilise pas du JAVA ou ce genre de langages pour développer des algorithmes mais c'est plutôt sur du PYTHON et des libraires et des environnements différents. Finalement, on prend la data et on la transforme de façon à ce qu'on retire de l'intelligence. Donc, premier point c'est de comprendre peut-être d'ici 10 à 15 ans l'évolution des développements informatiques qui ne sera plus réalisée avec des algorithmes classiques procéduraux et prédéfinis mais avec des algorithmes différents avec de l'intelligence. La deuxième chose, c'est le potentiel d'utilisation. On sait aujourd'hui faire des choses plus complexes grâce à la technologie qu'on ne sait pas faire avec de l'informatique classique, par exemple du machine learning qui permet d'identifier des patterns, soit on a du deep learning qui est un peu plus complexe parce que souvent les gens n'ont pas assez de données. En gros, on peut identifier des clusters d'objets qui ont des choses en commun. Ce qui drive en fait le choix, c'est le potentiel de l'exploitation de cette intelligence ou de l'information que l'on retire des algorithmes. Aujourd'hui, on l'utilise soit dans des automatisations de processus soit en fait dans les sujets réglementaires. Et pourquoi ? Parce que c'était là-dedans où je dirais, le return on investment est le plus simple à justifier.

AS : Donc en fait, ici ce que je vois c'est que pour le moment le focus est plutôt mis sur l'optimisation que sur la création de nouveaux processus basés sur IA ou RPA.

MA : Oui, mais ça c'est propre à nos choix parce que c'est la façon de mieux faire passer les décisions. Je donne un exemple. Si on parle de Know Your Transactions et si le régulateur nous force à revoir 20 000 clients pour être sûr que les transactions sont conformes, c'est-à-dire en ligne avec les profils, si ça se fait manuellement, il y a 4000 jours-homme de personnes qui sont en fait derrière les écrans pour vérifier les transactions et dire si les transactions sont okay et on n'a pas une garantie parce que chacun décide ça différemment et surtout est-ce qu'on a trouvé l'épingle dans le foin, est-ce qu'on peut être sûr qu'en fait, on a tout trouvé. Avec de l'IA, c'est l'inverse que l'on fait, en gros on réalise des profils des clients et on sort les transactions qui doivent être vérifiées et qui n'entrent pas dans le profil du client. Là on est sûr qu'on sort tout et on sort peut-être uniquement 2-3% des transactions et on ne vérifie que ces transactions-là. Avec ça, le travail est mieux fait et on a une meilleure garantie, on a une algorithmie dans laquelle on peut prouver quels sont les critères, comment est-ce qu'on bloque la transaction

alors que si 50 personnes font ça, eh bien chacun a son critère de décision. Du coup, c'est ce genre de thèmes qui permettent de justifier un return on investment, une productivité supérieure. Aujourd'hui, c'était le plus simple à argumenter parce que ça a permis de mesurer clairement le return. Je pense que si vous faites par contre un chunk, c'est aussi intéressant mais en fait vous dites « je fais un algorithme dans lequel je découvre les gens qui vont quitter la banque et j'essaie de découvrir 10 à 12 mois auparavant pour que je puisse établir une stratégie de rétention ». En fait, sur cette stratégie de rétention, vous avez très peu de mesures, combien de gens finalement vous arrivez vraiment à retenir et suivant si vous détectez en gros qu'un client est en train de quitter la banque ou de changer, mentalement il est déjà loin et en fait il a déjà quitté la banque donc vous pouvez téléphoner et essayer de le garder *etc.* Donc, faire ce programme-là qui plus ou moins coûte la même chose, dans l'un vous pouvez clairement calculer les gains, dans l'autre vous pouvez estimer les gains et avoir une espérance de rétention. Donc pour l'instant, il vaut mieux aller vers les business plans dans lesquels on peut calculer au début et après mesurer pour avoir le return.

AS : Ok, je vois. Vous parliez des données. La qualité des données, leur disponibilité, c'est un frein ?

MA : Absolument. C'est le gros problème des algorithmes. Le gros problème c'est la data, la qualité de la data et la mise à disposition de la data, pour différentes raisons. Déjà, on a besoin de l'historique des données, sans quoi on ne sait rien faire, ça doit être assez profond, donc 10-15 ans. La deuxième chose, c'est garantir la qualité de la donnée : disponibilité de la donnée, donnée consistante, donnée unique, mise à jour de la donnée, en gros avec un modèle de qualité derrière. Il faut aussi des extracteurs pour mettre à disposition rapidement la donnée, il faut une sorte de data lake. C'est ça qui coûte le plus cher, pas l'IA, mais la qualité des données de base. On va dire que l'algorithmie c'est 20% et la qualité des données 80% des coûts.

AS : Au Luxembourg, le secret bancaire est très présent. Est-ce que ça a un impact aussi sur la qualité et la disponibilité des données ?

MA : Je pense que non, c'est même plutôt un avantage parce qu'on est très sensibles sur nos données au niveau historique grâce à ce secret bancaire et donc en termes de procédures et de process, on avait pas mal avancé pour pouvoir notamment contrôler de l'accès qui aujourd'hui en termes GDPR nous permet d'expatrier les données avec déjà des processus bien en place et des garanties de sécurité.

AS : Y a-t-il un partage des données entre les données du groupe et les données, on va dire, territoriales ?

MA : Oui, un partage au niveau du Luxembourg et au niveau de l'Europe, surtout dans le domaine des entreprises, des sociétés pour lesquels en matière de databases groupes, pour gérer et bien servir les clients. Au niveau privé, rien, ou moins. Dans tous les cas, il faut le consensus des clients.

AS : Vous pensez à d'autres freins pour plus d'utilisation d'outils IA et RPA ?

MA : La question, c'est de savoir si on a la masse critique pour faire ce job. C'est aussi une question d'évolution. Demain, l'informatique sera peut-être basée à 50% sur de l'IA. Les freins pour l'IA, ce sont les données. Pour faire de l'IA, on a besoin d'une profondeur dans les données. La deuxième chose, c'est que l'IA va prendre de l'ampleur mais on ne sait pas encore les données dont on aura besoin demain, donc il faut stocker toutes les données disponibles, car dans 15 ans l'avantage ce seront les données qui vont alimenter l'algorithme pour créer une IA avec du sens. Là, la GDPR nous bloque un peu, parce que c'est un extrême où on stocke toutes les données sans transparence vis-à-vis des clients ou alors on ne stocke pas mais le potentiel de l'IA va se réduire. C'est un débat. Il faut trouver un équilibre. On ne doit pas arriver à une situation comme la Chine qui contrôle sa population, ça c'est un grand danger. Je n'ai pas vraiment peur de ça chez nous avec nos sociétés. Le problème, ce ne sont pas les entreprises mais les États qui veulent contrôler les habitants. Le plus grand danger, je pense aujourd'hui, c'est la dictature qui utilise la technologie pour contrôler sa population.

AS : Le risque éthique, c'est donc aussi un frein à l'utilisation de l'IA ?

MA : Chaque technologie nouvelle comporte un risque éthique, dans toutes les sciences, toutes les inventions. On utilise la nouvelle technologie pour des causes positives ou mauvaises, c'est toujours une question qui se pose mais c'est à l'humanité de mettre des guidelines de façon à ce que cette technologie soit utilisée dans un cadre qui crée de la valeur pour les êtres humains, et non pas qui supportent des développements négatifs. Ce n'est pas un problème lié à l'IA mais bien à toutes les innovations.

AS : Vous avez la même vision que Stephen Hawking (rires). Et un autre risque, ou une opportunité, c'est d'avoir des experts qui connaissent vraiment les besoins de l'IA, ce que les outils IA font ? C'est plus un risque ou une opportunité selon vous ?

MA : Il faut un minimum d'expertise pour tirer du savoir ou de l'information de la data. Encore une fois, c'est « qu'est-ce qu'on va faire après de la data ? ». Je vais donner un exemple. Je vois que quelqu'un, pendant deux ou trois semaines, dépense à l'étranger. Je sais voir si c'est en Europe ou aux États-Unis par exemple. Mais si c'est aux États-Unis, une journée à l'hôpital, ça coûte 1500 dollars, sans assurance maladie complémentaire. Donc, je pourrais proposer à la personne de contracter une assurance maladie supplémentaire si je constate qu'elle se rend là-bas, ou lui donner l'information. La question, « c'est intrusif ou pas ? ». Si c'était moi, je trouverais ça bien, mais quelqu'un d'autre va être choqué qu'on suive ses déplacements. C'est un exemple à interpréter en positif ou en négatif, vous voyez.

AS : Ok. On va passer à la suite. L'accent est-il plus prononcé sur l'une ou l'autre de ces technologies ? Si oui, Pourquoi ?

MA : Non, je pense que c'est complémentaire. C'est utilisé dans des contextes différents, optimiser les processus, automatisation, acquisition de données. Le problème, c'est l'acquisition de données. Il faut commencer par acheter de la donnée comme des numéros de téléphone ou des adresses emails. Mais si on achète, ça doit être mis à jour. La RPA, c'est un canal d'acquisition de données.

AS : Je vois. Est-ce que BGL BNP Paribas sous-traite certaines activités IA ou RPA ?

MA : Oui, pour l'acquisition de données. Sous-traiter avec l'IA, ce sont plus des collaborations, on a démarré en 2006. Par exemple, on a démarré une collaboration avec la poste luxembourgeoise ou avec DataThings. Donc, c'est plutôt accéder à des gens pointus ou compétents sur le domaine. On les aide à démarrer leur activité mais on utilise aussi leurs compétences, donc oui.

AS : Et dans ces partenariats, le partage de données est-il autorisé ?

MA : En gros, les partenaires travaillent sur nos données ici à la banque. À ma connaissance, on n'a pas encore eu besoin d'avoir des données à eux. Je vais reformuler : avec les partenariats on a ajusté les méthodes pour préparer les données de façon que la confidentialité des données reste garantie.

AS : Ils ne peuvent pas développer un autre outil avec vos données donc ?

MA : C'est ça. C'est réglé dans des contrats avec eux pour clarifier les conditions et les résultats attendus.

AS : Ok. Et une autre question : dans quelle mesure les nouvelles technologies IA et RPA permettent-elles à la banque de proposer de nouveaux produits ? J'avais pensé à des conseils de trading automatiques ou comme votre exemple avec d'autres assurances pour les États-Unis.

MA : Avec les algorithmes, on propose de nouveaux crédits, surtout des crédits à la consommation, parce que l'algorithme va décider si on propose ou pas 25 000 euros à quelqu'un pour une nouvelle voiture. C'est déjà le cas ça, aujourd'hui, ça existe en France chez BNP mais chez nous au Luxembourg, je ne sais pas à 100%. On a aussi une opportunité intéressante avec l'IA pour la tarification des clients, pour savoir ce qui s'adapte le mieux aux clients. Je vais donner un exemple. Avec la tarification, on va devoir couvrir nos coûts, liquidité et risque, puis on prend une marge. Le problème c'est qu'aujourd'hui les taux sont standards, après on discute avec les clients pour faire des réductions mais ce n'est pas très scientifique.

AS : Et c'est une crainte que l'IA génère des comportements de masse, comme vers 2008-2009 où des algorithmes ont pris des décisions en même temps ce qui a créé des petits crashes boursiers ?

MA : Si les critères d'exécution des algorithmes sont les mêmes, oui le risque existe. C'est clair. Ils ont la même logique donc ça exécute le truc, mais le risque n'est pas plus grand avec l'IA puisqu'elle va sortir de l'information des données pour ensuite prendre des décisions. Si ces technologies sont corrélées, certaines décisions vont déclencher une avalanche de décisions non-maîtrisées. Ce n'est pas dû à l'IA, mais à tous les algorithmes.

AS : L'IA, c'est un outil d'aide à la décision « informée » je dirais, ou « plus informée que l'humain », mais de manière générale, l'IA prend des décisions ou elle donne des indications à l'humain ?

MA : Ça dépend de son implémentation. Encore une fois, l'IA ce sont des algorithmes mathématiques qui vont dégager de l'information de la data, information qui n'est pas prévisible sans cette intelligence. Si je connais la date de naissance de tous mes clients, ça ne me sert pas, mais si un algorithme crée une courbe de ces âges-là, ce n'est pas de l'IA mais mettre ça sur une courbe, ça crée de l'intelligence : « mince, j'ai trop de vieux ». Ce n'est pas de l'IA mais ça donne une info énorme, mais la décision que tu vas prendre sur ça, l'utilisation de cette

information, comme « mail pour tous les 30-35 ans qui sont des clients potentiels pour des crédits immobiliers », là c'est automatisé. Du coup, ça n'a rien avoir avec l'IA, elle donne aussi cette info mais ce qui compte c'est ce que tu vas en faire après pour atteindre tes objectifs. Il faut faire attention à la corrélation des données quand les informations qui ressortent sont fausses, si on a des doublons par exemple. L'information qui va ressortir commence toujours par la qualité des données à la base, il faut vérifier que les données de base ne sont pas erronées.

AS : Ok. On va passer aux deux dernières parties. Sur les trois risques considérés, conformité, fraude et crédit, que pouvez-vous dire sur les utilisations IA ? Vous avez déjà parlé de l'outil fraude, mais pour conformité et crédit ?

MA : On a des outils IA aussi pour conformité et crédit. On regarde aujourd'hui des algorithmes pour les transactions, ça va regarder en automatique si les transactions sont conformes aux clients. On a aussi des algorithmes de détection de la fraude. On a aussi pour les décisions des crédits comme j'avais expliqué si quelqu'un n'a pas assez de fond sur un compte mais assez sur un autre compte.

AS : Et quelles sont les conséquences positives ou négatives pour l'IA et RPA ?

MA : Je ne vois des points négatifs ou positifs dans le sens où c'est une autre technologie pour faire parler les données. On a appris des données avec l'informatique avec des algorithmes prédéfinis. L'informatique existe depuis 40 ans. Ici, ce sont plutôt des nouvelles méthodes d'exploitation des données pour déboucher sur des conclusions. La machine va trouver des patterns dans une énorme masse de données, ce n'est pas prédéfini mais ce sont des algorithmes qui vont auto-apprendre et devenir de plus en plus précis par eux-mêmes. Je pense qu'un problème c'est de faire coopérer ou intégrer cette technologie dans la technologie classique. Pour détecter la fraude, si tu dois interroger une nouvelle technologie, tu demandes « c'est une fraude ou pas ? », c'est là où tu interconnectes une nouvelle technologie avec une ancienne. Tu poses une question, tu dois injecter de la data, puis l'algorithme va te donner une probabilité de fraude. Une fois que tu as cette info, tu prends la transaction et tu décides ou pas de l'exécuter. Si tu estimes que le risque de fraude reste assez faible, grâce à la probabilité qui a été donnée, tu autorises la transaction. Mais si tu considères que non, tu bloques la transaction. Il faut des opérateurs après pour appeler les clients, etc. C'est ça qui coûte cher. Si on a l'IA qui fonctionne elle-même, c'est complexe à intégrer dans les outils existants. C'est faisable le 100% automatique, on a réussi à faire ça, mais les coûts sont élevés, pas sur la data, mais ce qui coûte

cher c'est d'intégrer l'algorithme dans la base existante pour que ça puisse coexister. Si l'algorithme n'est pas une production mais quelque chose qui ne donne qu'une liste d'info, aucun problème. C'est une énorme différence si l'IA est en off-production ou en vraie production informatique, si vous voulez.

AS : L'IA a une valeur ajoutée pour automatiser des tâches répétitives ? La définition du job change ?

MA : Oui, c'est ça. Les algorithmes sont vieux. On utilise les mathématiques depuis très longtemps. Aujourd'hui, on traite les données en automatique, ça a des avantages. C'est une valeur ajoutée pour le personnel qui ne doit plus faire des tâches répétitives mais ça pose des questions éthiques. Est-ce que demain l'IA sera autonome ? Est-ce que ça va se développer de sorte qu'on en perde le contrôle ? Imagine que demain on a de l'IA pour la sécurité de la BGL, une IA responsable de la sécurité, qui utilise les badges, etc. Du coup, l'IA pourra se dire : « j'ai une faille parce que le seul qui a encore la possibilité de me dominer, c'est l'administrateur, c'est lui qui a les codes d'accès », donc l'IA va détecter cette faille parce qu'il a auto-appris et donc imagine qu'il ferme cette porte de sorte à ce qu'aucun administrateur ne puisse rentrer, c'est devenu autonome en gros. Tu te dis ok, je retire la prise. Mais l'IA aura développé une sortie de mécanisme de survie, quand la machine va détecter une coupure d'électricité, toute l'intelligence sera sur d'autres serveurs et ce sera transmis sur ces machines-là, donc même si tu tues la machine quand tu retires la prise, ça ne va pas mourir parce que ça aura transféré l'information. Du coup, c'est autonome. On ne peut pas garantir que ce scénario n'arrivera pas dans le futur. On développe de la technologie mais d'ici 20-30 ans, la puissance de cette technologie sera énorme. Le risque, c'est qu'on ne le maîtrise plus. C'est progressif, on maîtrise la situation un jour puis on ne la maîtrise plus le lendemain.

AS : Que mettre en place pour empêcher ça ?

MA : La question c'est de savoir si nous le voulons ou pas. On en arrive presque à la théorie de l'évolution. Cette intelligence n'est pas sur un support biologique mais c'est quand même la même chose parce que tu vas reproduire le cerveau, ça va donc créer une nouvelle race très intelligente. Cette technologie, aujourd'hui, on ne sait pas où ça va nous mener. Si tu veux mettre de l'intelligence dans l'univers, ça doit être sur un support technologique et pas biochimique, ça c'est une évidence. Si on rencontre de l'intelligence un jour, ce sera sur des machines, pas des êtres humains comme nous. Du coup, si cette machine fonctionne avec de

l'intelligence artificielle aussi sur les émotions, c'est de la machinerie qui aura de l'émotion. J'ouvre cette porte pour que ça donne une autre vue sur la chose. Aujourd'hui, c'est encore de l'intelligence artificielle élémentaire. Ce n'est pas mature, mais c'est une évolution réelle.

AS : C'est possible d'insérer des émotions dans des outils IA ?

MA : Je pense que oui. On ne sait pas la manière dont un être humain capte l'émotion ou sa façon de gérer cette information mais je pense qu'un jour on pourra le comprendre avec des critères émotionnels formalisés. Une émotion, ce sera aussi du captage de data. Ton cerveau, c'est un ordinateur qui traite de la data sur une base biochimique, mais un jour on va recréer ça sur une base technique, je pense. La machine apprendra comme un bébé. Tu peux imaginer un algorithme aléatoire alors, sinon tous les êtres créés seront parfaits. On pousse un peu loin l'idée mais je pense que si demain nous définissons la race comme la religion, nos valeurs, *etc.*, ce phénomène va se déplacer du biochimique sur des supports technologiques.

AS : Est-ce que la complexité, on pourra encore la comprendre ?

MA : C'est une bonne question. L'évolution sera-t-elle contrôlable, toujours ce que l'être humain souhaite qu'elle fasse, ou alors elle va nous échapper, devenir incontrôlable et autonome ? C'est la première chose que cette intelligence cherchera à faire, éliminer l'être humain, puisqu'elle va détecter que c'est l'homme le problème de sa survie. C'est la première décision que cette intelligence prendra puisque l'humain représente une menace pour la planète et pour l'intelligence elle-même. Est-ce qu'on pourra toujours maîtriser ça ? C'est la question. Les débats sont ouverts, c'est possible d'argumenter d'un côté ou de l'autre. Bill Gates et Elon Musk ont clairement exprimé des craintes, mais pas de panique, c'est encore loin (rires). Facebook a créé des ordinateurs qui ont commencé à se parler et ils ont inventé une nouvelle langue.

AS : Chez Microsoft aussi, avec le chatbot qui a commencé à exprimer des propos racistes.

MA : Oui, c'est proche du cadre d'apprentissage des enfants, si tu le conditionnes comme raciste, il sera raciste.

AS : La question, c'est de savoir si l'IA pourra se remettre en question.

MA : Oui, je pense que oui.

AS : Ok, merci.

MA : Si des choses ne sont pas claires, tu peux me rappeler.

AS : Ok. Merci beaucoup pour l'entretien.

MA : Très bien. Data et big data, c'est l'avenir, donc bonne chance Alex !

AS : C'est vrai, merci beaucoup !

MA : Au revoir.

AS : Au revoir.

Annexe 7 : Texte original de la proposition de projet de recherche estival de Dartmouth sur l'IA

Articles

AI Magazine Volume 27 Number 4 (2006) (© AAAI)

A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence

August 31, 1955

*John McCarthy, Marvin L. Minsky,
Nathaniel Rochester,
and Claude E. Shannon*

■ The 1956 Dartmouth summer research project on artificial intelligence was initiated by this August 31, 1955 proposal, authored by John McCarthy, Marvin Minsky, Nathaniel Rochester, and Claude Shannon. The original typescript consisted of 17 pages plus a title page. Copies of the typescript are housed in the archives at Dartmouth College and Stanford University. The first 5 papers state the proposal, and the remaining pages give qualifications and interests of the four who proposed the study. In the interest of brevity, this article reproduces only the proposal itself, along with the short autobiographical statements of the proposers.

We propose that a 2 month, 10 man study of artificial intelligence be carried out during the summer of 1956 at Dartmouth College in Hanover, New Hampshire. The study is to proceed on the basis of the conjecture that every aspect of learning or any other feature of intelligence can in principle be so precisely described that a machine can be made to simulate it. An attempt will be made to find how to make machines use lan-

guage, form abstractions and concepts, solve kinds of problems now reserved for humans, and improve themselves. We think that a significant advance can be made in one or more of these problems if a carefully selected group of scientists work on it together for a summer.

The following are some aspects of the artificial intelligence problem:

1. Automatic Computers

If a machine can do a job, then an automatic calculator can be programmed to simulate the machine. The speeds and memory capacities of present computers may be insufficient to simulate many of the higher functions of the human brain, but the major obstacle is not lack of machine capacity, but our inability to write programs taking full advantage of what we have.

2. How Can a Computer be Programmed to Use a Language

It may be speculated that a large part of human thought consists of manipulating words according to rules of reasoning and rules of conjecture. From this point of view, forming a generalization consists of admitting a new

Source : <https://ojs.aaai.org//index.php/aimagazine/article/view/1904>

Annexe 8 : Dialogue entre ELIZA et une utilisatrice

User/patient: Men are all alike.
ELIZA: *In what way ?*
User/patient: They are always bugging us about something or others.
ELIZA: *Can you think of a specific example?*
User/patient: Well, my boyfriend made me come here.
ELIZA: *Your boyfriend made you come here?*
User/patient: He says I'm depressed much of the time.
ELIZA: *I am sorry to hear that you are depressed.*
User/patient: It's true; I am unhappy.
ELIZA: *Do you think that coming here will help you not to be unhappy?*
User/patient: I need some help; that much seems certain.
ELIZA: *What would it mean to you if you got some help ?*
User/patient: Perhaps, I could learn to get along with my mother.
ELIZA: *Tell me more about your family.*

Source : O'Regan (2016, p. 259), Introduction to the history of computing

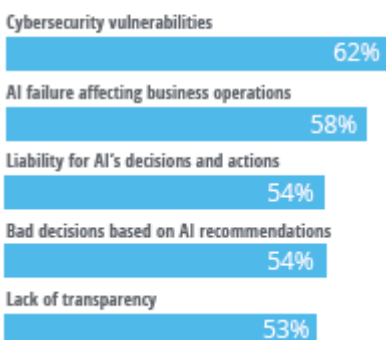
Annexe 9 : Répartition des risques les plus représentés pour chaque catégorie de risque

AI confidence concerns

■ Extreme or major concern



Overall, how concerned is your organization about the following potential risks associated with your AI initiatives?

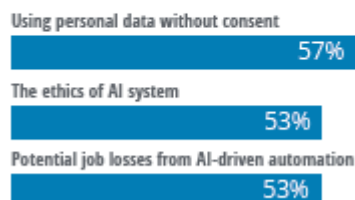


Ethical AI concerns

■ Extreme or major concern



Overall, how concerned is your organization about the following potential risks associated with your AI initiatives?

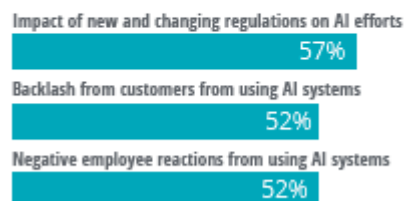


Marketplace uncertainty concerns

■ Extreme or major concern

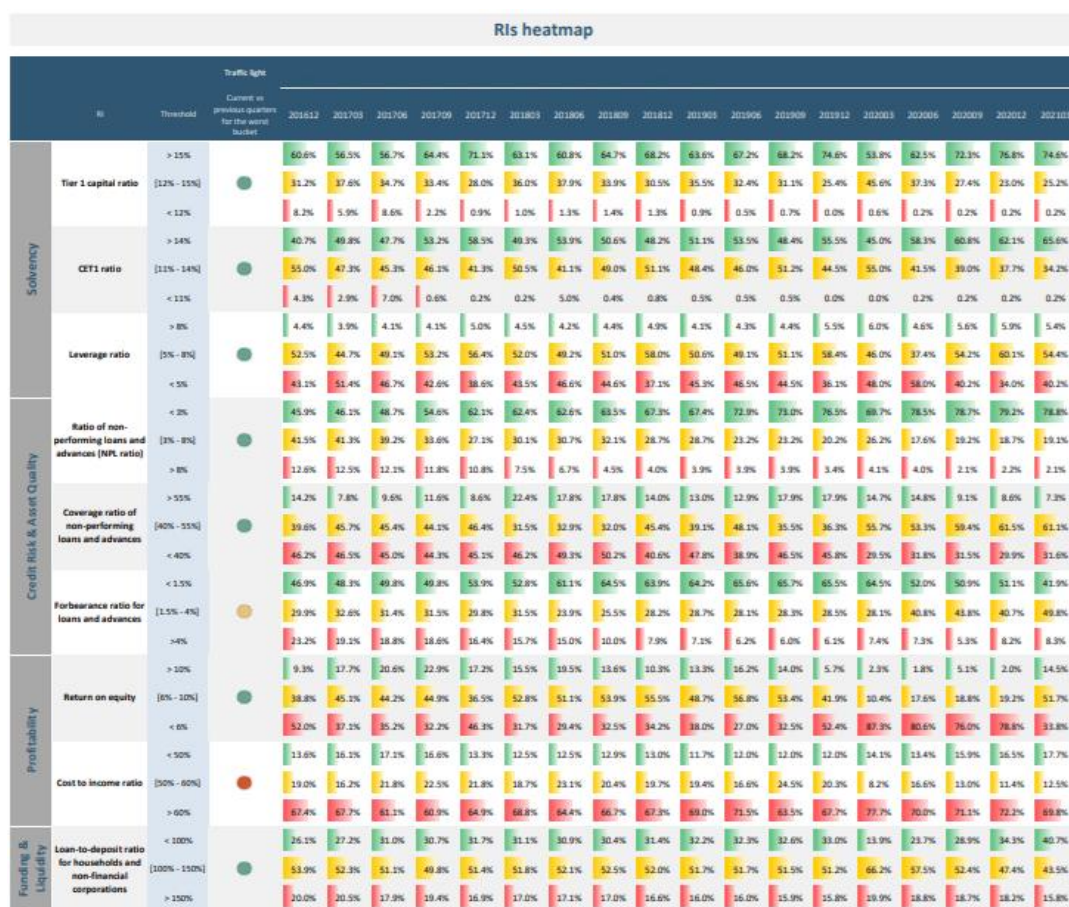


Overall, how concerned is your organization about the following potential risks associated with your AI initiatives?



Source : Ammanath *et al.* (2020, pp. 4-7), Conquering AI risks – Unpacking and alleviating concerns that threaten AI advancement

Annexe 10 : Carte thermique des indicateurs de risque pour le Q1 2021 (EBA, 2021, p. 5).



Source : EBA (2021, p. 5), Risk dashboard

Annexe 11 : Taxonomie des risques détaillée – catégories de risque et sous-risques : définitions

Catégorie	Définition	Sous-risque	Définition
Risque de marché ou market risk	Le risque de pertes à la suite des changements de prix d'instruments financiers comme les obligations, les actions ou les monnaies (BCBS, 2019, p. 1).	Risque de prix des actions ou equity price risk	La perte potentielle due à un changement défavorable du prix d'une action (Leo et al., 2019, p. 2).
		Risque de taux d'intérêt ou interest rate risk	L'exposition de la situation financière d'une banque à des mouvements défavorables des taux d'intérêt (BCBS, 2004, p. 5).
		Risque de taux de change ou foreign exchange risk	Le risque que la valeur des actifs ou des passifs d'une banque change dû à des fluctuations dans le taux de change de la monnaie (Leo et al., 2019, p. 2).
		Risque lié aux prix des matières premières ou commodity price risk	La perte potentielle due à un changement défavorable du prix des matières premières détenues (Leo et al., 2019, p. 2).
Risque de crédit ou credit risk	L'éventualité qu'un emprunteur ou une contrepartie bancaire ne parviendra pas à remplir ses obligations conformément aux conditions convenues (BCBS, 2000, p. 1).	Risque de défaut de paiement ou de fail risk	Le risque pris par un prêteur au cas où un emprunteur ne serait pas en mesure d'effectuer les paiements requis sur sa dette (Kagan & Broek, 2020).
		Risque de spread ou spread risk	Le risque qui découle dans le niveau ou dans la volatilité dans les spreads de crédit par rapport à la structure à terme du taux d'intérêt sans risque (Ablin, 2017, p. 1).
		Risque de contrepartie ou counterparty risk	« The risk of one or more parties in a financial transaction defaulting on or otherwise failing to meet their obligations on that trade. » (Risknet, 2021).
		Risque de règlement de transaction ou settlement risk	Le risque que le règlement d'une transaction financière ne se produira pas comme prévu, impliquant les risques de liquidité, de marché, opérationnel, réputationnel et de crédit (BCBS, 2000, p. 2).
Risque opérationnel ou operational risk	Le risque opérationnel comme étant le risque d'occasionner des pertes découlant d'une gestion inadéquate ou défectueuse des processus internes, des personnes, des systèmes ou d'événement externes (BCBS, 2011, p. 3).	Risque technologique ou technology risk	Le risque technologique survient lorsqu'une banque utilise de manière journalière des systèmes informatiques (Lessambo, 2020, p. 172). Il survient des fois quand des technologies inappropriées sont choisies, suite à l'adoption de technologies obsolètes ou encore suite à la non-adoption de technologies adéquates (Lessambo, 2020, p. 172).
		Risque lié aux processus ou process risk	« Operational risk occurs through ineffective and/or inefficient processes. » (Lam, 2014, p. 241). En ce sens, les processus inefficaces ne parviennent pas à atteindre leurs objectifs alors que les processus inefficaces sont ceux qui atteignent leurs objectifs en consommant des coûts excessifs (Lam, 2014, p. 241).
		Risque lié aux personnes ou people risk	Le risque lié aux personnes est la résultante de l'incompétence, des contraintes de personnel, de la malhonnêteté, ou d'une culture d'entreprise qui ne cultive pas une conscience du risque (Lam, 2014, p. 243).
		Risque d'événement externe ou external event risk	Le risque d'événement externe considère les pertes dues à des événements très peu probables mais dont les conséquences sont graves s'ils se produisent (Lam, 2014, p. 245). Ce risque possède une faible prédictibilité parce que les événements sont généralement très aléatoires et donc inattendus (Lam, 2014, p. 254).
Risque de liquidité ou liquidity risk	Le risque de liquidité est la capacité d'une banque à financer l'augmentation de ses actifs et à faire face à ses obligations lorsqu'elles arrivent à échéance, sans subir de pertes inacceptables (BCBS, 2008, p. 1).	Risque de liquidité de financement ou funding liquidity risk	Le risque que l'entreprise ne soit pas en mesure de répondre efficacement aux besoins actuels et futurs, qu'ils soient prévus ou inattendus, en matière de flux de trésorerie et de garanties, sans affecter les opérations quotidiennes ou la situation financière de l'entreprise (BCBS, 2008, p. 1).
		Risque de liquidité des actifs ou asset liquidity risk	Le risque qu'une entreprise ne puisse pas facilement compenser ou éliminer une position au prix du marché en raison d'une profondeur de marché insuffisante ou d'une perturbation du marché (BCBS, 2008, p. 1).
Autres risques	/	Risque commercial ou business risk	Le risque de perte lié à des changements inattendus de l'environnement compétitif ou à des tendances qui nuisent à la franchise et/ou à l'économie d'exploitation de l'entreprise (Lam, 2014, p. 246).
		Risque de conformité ou compliance risk	Le risque auquel une organisation s'expose lorsqu'elle se trouve dans l'incapacité de répondre à ses obligations, c'est-à-dire aux réglementations, règles de conformité et standards propres à l'organisation, aux lois et au code de conduite applicable aux activités bancaires (BCBS, 2005, p. 7). Auquel cas, les retombées sur l'organisation peuvent être financières (ex : sanctions réglementaires, pertes financières substantielles), organisationnelles ou encore réputationnelles (BCBS, 2005, p. 7).
		Risque stratégique ou strategic risk	Le risque associé à la sélection initiale, exécution ou modification dans le temps d'une stratégie sans pour autant que cette stratégie atteigne ses objectifs globaux (Chapman, 2011).
		Risque macroéconomique ou macroeconomic risk	Le risque macroéconomique comme le comportement des industries et des gouvernements et des relations entre eux résultant des politiques monétaire et fiscale, des flux commerciaux et d'investissement et des développements politiques nationaux et internationaux, ainsi que les effets de ces facteurs sur les portefeuilles financiers et les valorisations des entreprises (Global Risk Institute, 2021).
Risque des risques	/	Risque de réputation ou reputational risk	« The risk arising from negative perception on the part of customers, counterparties, shareholders, investors or regulators that can adversely affect a bank's ability to maintain existing, or establish new, business relationships and continued access to sources of funding. » (BCBS, 2009, p. 19).

Source : Contribution personnelle de l'auteur

Annexe 12 : Zooms sur les risques émergents

Zoom n°1 : Risque de taux d'intérêt bas (« low interest rate risk »)

Depuis une décennie et notamment à la suite de la crise des subprimes de 2008, les taux d'intérêt ont baissé drastiquement pour atteindre des valeurs proches de 0%, voire en Europe surtout, des valeurs négatives. Ces taux d'intérêts bas peuvent avoir un impact sur les business models des institutions financières. Une étude de 2018 menée aux États-Unis par Bikker et Vervliet a montré l'impact des taux d'intérêts faibles sur la rentabilité des banques et sur le degré de prise de risque de celles-ci. En effet, la performance des banques est endommagée par les taux d'intérêts faibles et la capacité des banques à générer des profits via des sources de financement traditionnelles est réduite à cause des marges nettes compressées dues aux taux d'intérêts faibles (Bikker & Vervliet, 2018, p. 15). Concernant le degré de prise de risque, l'étude n'a pas trouvé de preuve d'une augmentation de l'exposition par les banques dans le but d'atteindre des rendements et pour contrecarrer l'effet des taux d'intérêts faibles. Cependant, il a quand même été montré que les banques ont significativement réduit leur niveau de provisionnement de pertes de crédit dans un environnement de taux d'intérêts faibles (Bikker & Vervliet, 2018, p. 15). Pour le cas de la Belgique, la National Bank of Belgium (NBB) a d'ailleurs émis quelques commentaires au sujet de l'environnement de taux d'intérêts faibles dans ses Financial Stability Reports :

- « *The low interest rate environment is beginning to weigh on the profitability of the sector. The net interest margin of Belgian banks is effectively steadily coming under pressure now that the low interest rates are increasingly reflected in returns on assets while deposit interest rates reached their lower bound some time ago.* » (BNB, 2018, p. 7) ;
- « *The lasting low interest rate environment coupled with strong competition on some markets remains an important challenge for the profitability of banks and insurance companies, and the viability of some business models and the adequacy of current cost structures needs to be reassessed.* » (BNB, 2021, p. 16).

Zoom n°2 : Risque lié au changement climatique (« climate change risk »)

Plusieurs travaux montrent que l'impact du changement climatique s'articulera autour de deux risques : le risque physique et le risque de transition (Scott *et al.*, 2017, p. 98 ; Fabris, 2020, p. 33). Les risques physiques découlent d'événements climatiques comme les tempêtes, sécheresses, inondations, ouragans, *etc.* (Scott *et al.* 2017, p. 98). Le risque de transition découle du processus d'ajustement pour arriver à une économie à faible émission de carbone (Scott *et al.*, 2017, p. 98).

Encore une fois et comme pour tout risque, il est nécessaire d'établir une gestion saine afin de réduire l'impact et la probabilité du risque lié au changement climatique. Cependant, Fabris (2020, p. 33) rapporte que plusieurs études menées en grande partie sur des banques européennes ont conclu que le système bancaire commençait à prendre en compte les risques climatiques mais qu'il existait également des lacunes significatives dans l'identification, l'évaluation et la gestion de ces risques. Or, ces risques se matérialisent sur le long terme alors que le système financier a tendance à considérer les risques sur le court terme et c'est là qu'est le problème clé (Fabris, 2020, p. 33). En effet, au moment où ces risques seront clairement visibles, il sera déjà trop tard pour les empêcher, ou du moins diminuer leur impact. De plus, le risque lié au changement climatique ne constitue pas un type de risque financier en soi mais plutôt un risque dont l'impact sera visible sur chaque catégorie de la taxonomie de risque, i.e. crédit, liquidité, marché et autres (Fabris, 2020, pp. 33-34) (voir la figure ci-après pour des exemples d'impact sur le système financier).

Table 2: Climate change impact on the financial system

	Credit risk	Market risk	Operational risk
Physical	- Increasing flood risk to mortgage portfolio - Declining agricultural outputs	- Re-pricing of sovereign debt	- Impact on business continuity
Transition	- Tightening technological standards affects company business - Carbon taxes lead to growing expenses - Prohibition of use of outdated technologies - Long-term investments become unprofitable - Innovations jeopardize companies' business based on outdated technologies	- Tightening climate-related policy leads to re-pricing of securities	- Changing sentiment on climate issues leads to reputational risk
Indirect risk	- Losses for companies connected with firms affected by climate change	- Re-pricing of securities	- Low probability of negative impact (jeopardizing of a bank's supply chains)

Figure : Impact du changement climatique sur le système financier

Source : Fabris (2020, p. 34)

Le Global Risks Report 2021 du World Economic Forum montre des évidences sur les croissantes considérations pour les risques liés au changement climatique. En effet, le rapport retrace l'évolution du paysage des risques selon leur probabilité et leur impact (voir figure ci-après). Leur enquête a montré qu'en 2021, quatre des cinq risques dont la perception est la plus forte en termes de probabilité sont des risques liés au changement climatique. Le classement est le suivant : 1) conditions météorologiques extrêmes ; 2) échec de l'action climatique ; 3) dommages environnementaux causés par l'homme ; 5) perte de la biodiversité (World Economic Forum, 2021, p. 14). En termes d'impact, on retrouve trois risques liés au changement climatique parmi les plus perçus, dans l'ordre : 2) échec de l'action climatique ; 4) perte de la biodiversité ; 5) crises des ressources naturelles (World Economic Forum, 2021, p. 14). Il est également intéressant de noter que les maladies infectieuses arrivent en quatrième position selon la probabilité et en première position selon l'impact. Le zoom suivant traitera justement du risque de pandémie.



Figure : L'évolution du paysage des risques selon leur probabilité et leur impact

Source : World Economic Forum (2021, p. 14)

Zoom n°3 : Risque de pandémie (« pandemic risk »)

La COVID-19 a sans aucun doute été un événement perturbateur majeur pour l'économie globale et pour la stabilité bancaire mondiale. La COVID-19 a poussé à considérer plus que jamais un risque probablement oublié, le risque de pandémie. En effet, une pandémie mondiale a évidemment des impacts fondamentaux sur la stabilité financière. Elnahass, Trinh, et Li (2021) ont pointé les impacts du coronavirus sur le secteur bancaire. Parmi leurs conclusions, on retrouve que la COVID-19 a considérablement nui à la performance financière des banques (i.e. la performance basée sur la comptabilité et sur les marchés) et à la stabilité financière (i.e. risque élevé de défaut, risque élevé de liquidité, et risque élevé d'actifs). De plus, l'économie globale semble avoir été touchée puisque ces résultats se vérifient pour diverses régions géographiques, pays individuels, tailles des banques, âge des banques, niveaux de risque des banques et classification des revenus des pays (Elnahass, Trinh et Li, 2021, p. 21). Łasak a aussi montré que la COVID-19 a conduit à une croissance des prêts non performants (« non-performing loans (NPLs) »), c'est-à-dire les prêts pour lesquels l'emprunteur est en défaut de paiement parce qu'il n'a pas effectué les paiements prévus pendant une période déterminée (Segal, 2021).

Cependant, cette crise malheureuse apportait avec elle la capacité d'évaluer la réactivité des banques à des chocs et leur solidité après la crise des subprimes de 2008 qui a engendré un amas de régulations plus strictes pour assurer plus de sécurité du système financier. Demirguc-Kunt, Pedraza, et Ruiz-Ortega (2020, p. 13) ainsi que Schillig (2021, p. 57) rapportent qu'au début de la crise les banques étaient mieux préparées pour répondre aux besoins de prêts de l'économie réelle. Également, les banques, à l'entrée dans la crise, possédaient des réserves de capital et de liquidité supérieures résultant des durcissements sur les exigences en matière de fonds propres et de liquidité depuis la crise de 2008 (Borio, 2020, p. 6). Marcu (2021, p. 217) a pointé que cette crise a mis au défi la résilience et la capacité d'adaptation des banques, ce qui en retour a poussé à l'accélération des processus de digitalisation du secteur bancaire. L'objectif étant notamment de suivre les attentes des clients et d'innover en matière de produits et services (Marcu, 2021, p. 217). Finalement, des banques mieux positionnées qu'à la crise majeure précédente ont été en mesure de supporter l'économie et d'aider les clients (Marcu, 2021, p. 217).

La crise de la COVID-19 a aussi conduit à d'incroyables politiques fiscales et monétaires sans précédent. Ceci a été le fruit d'une collaboration étroite entre banques, régulateurs et superviseurs. Nous avons en effet vu des mesures comme des restrictions sur la distribution de dividendes pour augmenter le capital disponible de sorte à absorber les pertes et soutenir les prêts, des assouplissements des exigences de capital, des extensions de moratoire de paiement fournies par les banques pour les débiteurs, *etc.* (Gual, 2021, p. 2).

Même si le système financier était mieux préparé pour cette crise que pour la précédente, nous l'avons vu, il a quand même été affecté sur plusieurs plans. C'est pourquoi, dans le futur, on peut s'attendre à une gestion des risques plus stricte avec des évaluations des risques plus exhaustives, notamment au niveau des stress tests qui pourraient prendre en compte des scénarios en période de pandémie mondiale. Nous pouvons également nous attendre à un accroissement des régulations pour améliorer les processus de gestion de risque en cas de pandémie.

Zoom n°4 : Risque cybernétique (« cyber risk »)

Le risque cybernétique est un risque opérationnel qui comprend un large éventail de risques qui proviennent de la défaillance ou la violation des systèmes IT (Aldasoro *et al.*, 2021, p. 3). Le FSB précise que le risque cybernétique est la combinaison de la probabilité d'occurrence d'incidents cybernétiques et leurs impacts (FSB, 2018, p. 9). Un incident cybernétique est « *any observable occurrence in an information system that: (i) jeopardises the cyber security of an information system or the information the system processes, stores or transmits; or (ii) violates the security policies, security procedures or acceptable use policies, whether resulting from malicious activity or not.* » (Aldasoro *et al.*, 2021, p. 3). Aldasoro *et al.* (2020, pp. 37-38) ont dressé quelques conclusions sur l'impact du risque cybernétique :

- Coût moyen des événements cybernétiques en augmentation au cours de la dernière décennie ;
- Coûts plus élevés pour les grandes entreprises et les événements plus connectés ;
- Coûts plus faibles pour les cyber-événements à intention malveillante (cyber-attaques), surtout si l'attaque n'est pas menée à grande échelle ;
- Le secteur financier connaît le plus grand nombre d'incidents cybernétiques mais les banques et compagnies d'assurance subissent des pertes limitées comparées aux autres secteurs, probablement en raison des effets des régulations et d'investissement plus élevés dans la cybersécurité ;
- Le développement des compétences technologiques et la dépendance aux systèmes de cloud permettent aux entreprises d'atténuer les coûts des incidents cybernétiques.

Zoom n°5 : Risque géopolitique (« geopolitical risk »)

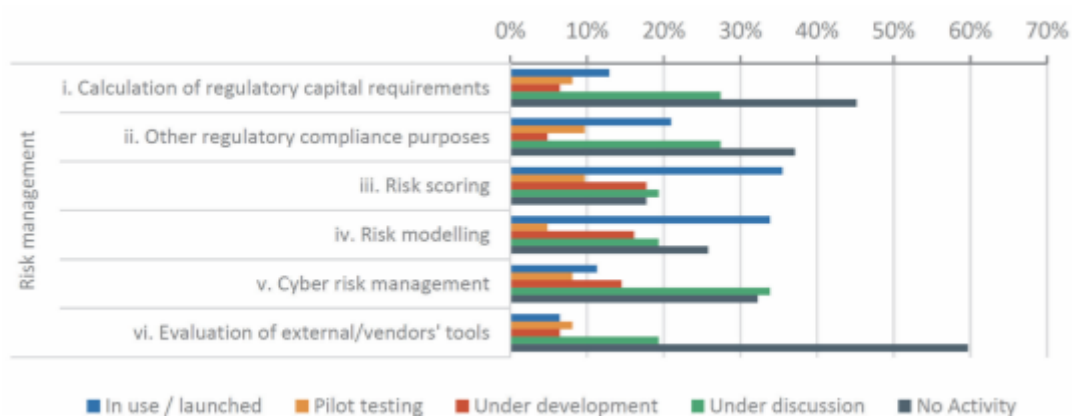
Le risque géopolitique est « *the risk associated with wars, terrorist acts, and tensions between states that affect the normal and peaceful course of international relations.* » (Caldara & Iacoviello, 2018, p. 2). L'étude de Caldara et Iacoviello (2018, p. 27) montre que des événements amplifiant le risque géopolitique exerce une pression sur l'activité économique.

Annexe 13 : Les principes d'évaluation des systèmes de contrôle interne classé par sources de déficiences

<i>Major sources of internal control deficiencies</i>	<i>Principles</i>	<i>Description</i>
Management oversight and the control culture	Principle 1	The board of directors should have responsibility for approving and periodically reviewing the overall business strategies and significant policies of the bank; understanding the major risks run by the bank, setting acceptable levels for these risks and ensuring that senior management takes the steps necessary to identify, measure, monitor and control these risks; approving the organisational structure; and ensuring that senior management is monitoring the effectiveness of the internal control system. The board of directors is ultimately responsible for ensuring that an adequate and effective system of internal controls is established and maintained.
	Principle 2	Senior management should have responsibility for implementing strategies and policies approved by the board; developing processes that identify, measure, monitor and control risks incurred by the bank; maintaining an organisational structure that clearly assigns responsibility, authority and reporting relationships; ensuring that delegated responsibilities are effectively carried out; setting appropriate internal control policies; and monitoring the adequacy and effectiveness of the internal control system.
	Principle 3	The board of directors and senior management are responsible for promoting high ethical and integrity standards, and for establishing a culture within the organisation that emphasises and demonstrates to all levels of personnel the importance of internal controls. All personnel at a banking organisation need to understand their role in the internal controls process and be fully engaged in the process.
Risk Recognition and Assessment	Principle 4	An effective internal control system requires that the material risks that could adversely affect the achievement of the bank's goals are being recognised and continually assessed. This assessment should cover all risks facing the bank and the consolidated banking organisation (that is, credit risk, country and transfer risk, market risk, interest rate risk, liquidity risk, operational risk, legal risk and reputational risk). Internal controls may need to be revised to appropriately address any new or previously uncontrolled risks.
Control Activities and Segregation of Duties	Principle 5	Control activities should be an integral part of the daily activities of a bank. An effective internal control system requires that an appropriate control structure is set up, with control activities defined at every business level. These should include: top level reviews; appropriate activity controls for different departments or divisions; physical controls; checking for compliance with exposure limits and follow-up on non-compliance; a system of approvals and authorisations; and, a system of verification and reconciliation.
	Principle 6	An effective internal control system requires that there is appropriate segregation of duties and that personnel are not assigned conflicting responsibilities. Areas of potential conflicts of interest should be identified, minimised, and subject to careful, independent monitoring.
Information and communication	Principle 7	An effective internal control system requires that there are adequate and comprehensive internal financial, operational and compliance data, as well as external market information about events and conditions that are relevant to decision making. Information should be reliable, timely, accessible, and provided in a consistent format.
	Principle 8	An effective internal control system requires that there are reliable information systems in place that cover all significant activities of the bank. These systems, including those that hold and use data in an electronic form, must be secure, monitored independently and supported by adequate contingency arrangements.
	Principle 9	An effective internal control system requires effective channels of communication to ensure that all staff fully understand and adhere to policies and procedures affecting their duties and responsibilities and that other relevant information is reaching the appropriate personnel.
Monitoring Activities and Correcting Deficiencies	Principle 10	The overall effectiveness of the bank's internal controls should be monitored on an ongoing basis. Monitoring of key risks should be part of the daily activities of the bank as well as periodic evaluations by the business lines and internal audit.
	Principle 11	There should be an effective and comprehensive internal audit of the internal control system carried out by operationally independent, appropriately trained and competent staff. The internal audit function, as part of the monitoring of the system of internal controls, should report directly to the board of directors or its audit committee, and to senior management.
	Principle 12	Internal control deficiencies, whether identified by business line, internal audit, or other control personnel, should be reported in a timely manner to the appropriate management level and addressed promptly. Material internal control deficiencies should be reported to senior management and the board of directors.
Evaluation of Internal Control Systems by Supervisory Authorities	Principle 13	Supervisors should require that all banks, regardless of size, have an effective system of internal controls that is consistent with the nature, complexity, and risk inherent in their on- and off-balance-sheet activities and that responds to changes in the bank's environment and conditions. In those instances where supervisors determine that a bank's internal control system is not adequate or effective for that bank's specific risk profile (for example, does not cover all of the principles contained in this document), they should take appropriate action.

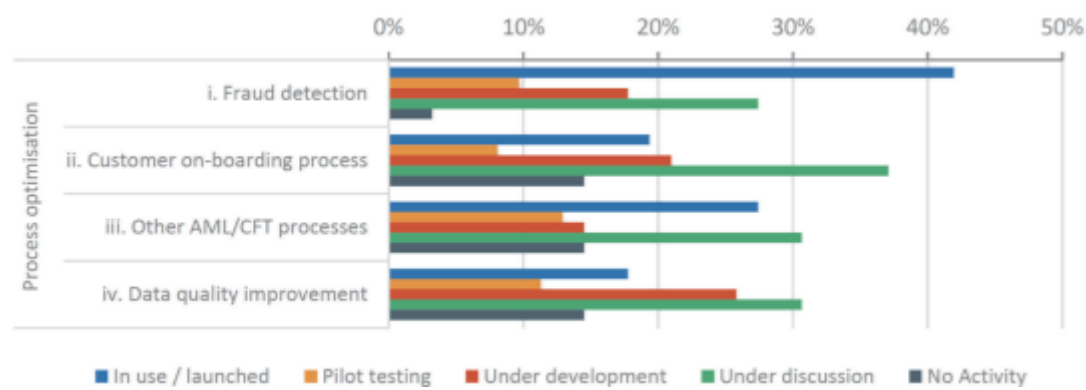
Source : BCBS (1998, pp. 2-5), Framework for internal control systems in banking organisations

Annexe 14 : Degré d'utilisation d'applications IA pour la gestion du risque



Source : EBA (2019, p. 38) Risk Assessment Questionnaire – Summary of the results

Annexe 15 : Degré d'utilisation d'applications IA pour les activités de back office



Source : EBA (2019, p. 38) Risk Assessment Questionnaire – Summary of the results

Annexe 16 : Les applications IA et RPA sur les risques de crédit, fraude, et conformité pour les deux banques de notre échantillon

	<i>BGL BNP Paribas</i>		<i>BNP Paribas Fortis</i>	
	<i>IA</i>	<i>RPA</i>	<i>IA</i>	<i>RPA</i>
<i>Risque de crédit</i>	A/ Nouveau modèle de scoring pour les PME (en utilisation) B/ Outil de validation automatique des dépassements sur compte courant (en développement) C/ Proposer de nouveaux crédits (en discussion) D/ Tarification des clients (opportunité)	A/ Robot lecteur des états financiers (en utilisation) B/ Demandes de crédit (opportunité)	A/ Développement de modèles de scoring plus performants (en discussion)	A/ Reconnaissance de documents (opportunité) B/ Établissement de documents (opportunité)
<i>Risque de fraude</i>	A/ Outil IA de détection de fraude (en utilisation)	/	A/ Outil IA de détection de fraude (en utilisation)	/
<i>Risque de conformité</i>	A/ KYT - Profil client et évaluation de la conformité des transactions (en utilisation)	A/ Mettre en place des processus pour évaluer la conformité (opportunité)	A/ KYT - Augmented intelligence pour la reconnaissance des clients sur base de documents et la correspondance avec les données de la banque (en utilisation) B/ Speech to text - Évaluation de la conformité des appels passés pour la vente de produits (en développement)	/

Source : Contribution personnelle de l'auteur