

En quoi les Fintechs peuvent-elles
contribuer à la gestion des risques pour
les banques traditionnelles ?

Laurine LEMOINE

Introduction

Les investissements dans les *Fintechs* dans le monde croissent en permanence avec une augmentation de 27% du nombre de projets entre 2018 et 2019 en France selon le panorama 2019 de *France Fintech*, ce qui montre le développement des *Fintechs* et l'importance de leur prise en compte par les banques. D'après le président de *France Fintech*, Mr Alain Clot, les *Fintechs* sont des « Entreprises utilisant des modèles opérationnels, technologiques ou économiques innovants et visant à traiter des problématiques existantes ou émergentes de l'industrie des services financiers ». Cependant, la collaboration entre les établissements financiers et les *Fintechs* engendre certains risques, principalement en terme de conformité. La fonction conformité permet de limiter les risques de mauvaise réputation et d'assurer le bon respect des législations et des réglementations des établissements bancaires et financiers, c'est un réel enjeu car le non-respect de celles-ci entraîne des sanctions non négligeables par les autorités françaises. En 2017, l'Autorité de Contrôle Prudentiel et de Résolution ACPR a infligé une sanction de 2 millions d'euros au Crédit Agricole Atlantique Vendée pour des manquements dans la lutte contre le blanchiment et le financement du terrorisme. En 2019, la Commission Nationale de l'Information et des Libertés CNIL a imposé une amende de 500 000€ à la société Futura Internationale pour démarchage téléphonique illégal (CNIL, Novembre 2019). Il est donc nécessaire d'avoir une conformité exemplaire afin d'éviter ce type de sanctions. Cependant ces réglementations ont un coût : les plus grandes institutions financières du monde dépensent chaque année jusqu'à 1 milliard de dollars pour répondre aux nouveaux objectifs des autorités de régulation (Thierry Bonneau, 2017). Les établissements peuvent mettre en place des processus internes mais peuvent également externaliser une partie de la surveillance en déléguant à une *Fintech* afin de supprimer le coût humain de ces opérations. On peut partager les *Fintechs* en 5 grandes familles : la gestion et stockage de données bancaires, les services de financement, d'investissement et d'épargne, les services de paiement, les assurances et la réglementation. Nous allons principalement nous intéresser aux *Fintechs* liées à la réglementation, les *RegTechs*. Nous allons donc nous demander en quoi les *Fintechs* peuvent contribuer à la gestion des risques pour les banques traditionnelles. Tout d'abord, nous évoquerons l'expertise et la rentabilité que peuvent apporter les *Fintechs* aux établissements bancaires par leur spécialisation et leur agilité permanente. Enfin, nous verrons certaines limites liées à la coopération entre les banques et les *Fintechs* notamment par la divulgation d'informations confidentielles des banques et des clients mais aussi par des problèmes liés à la conformité.

En quoi les *Fintechs* peuvent-elles contribuer à la gestion des risques pour les banques traditionnelles ?

1. Présentation des RegTechs

La rentabilité des banques aujourd'hui est assez faible par rapport à d'autres secteurs et le risque réglementaire pèse lourd. Selon une étude du *Boston Consulting Group* parue en février 2018, entre 2009 et 2017 les banques ont payé 345 milliards de dollars en pénalités, amendes et règlements amiables divers auprès des différents régulateurs (Edouard Lederer, février 2018). C'est pour cette raison qu'il est nécessaire de trouver des solutions pour que les établissements bancaires puissent se conformer aux exigences réglementaires et gérer leurs risques. Les *RegTechs* sont nées pour pallier ce problème en utilisant l'innovation technologique, les coûts liés à la conformité sont moins élevés et les institutions financières se digitalisent plus rapidement.

Les différents métiers de la Regtech

MÉTIERS		NATURE DES SERVICES		
1 2	LUTTE ANTI-BLANCHIMENT (LAB)	KYC ON BOARDING	- Reconnaissance faciale, digitale, vocale - Vérification de la cohérence des informations - Scoring lors de l'entrée en relation	
		SURVEILLANCE DES OPÉRATIONS	- Screening des listes PPE et sanctions - Recoupage de bases externes - Analyse de l'historique des transactions	
3	PROTECTION DES DONNÉES	- Pilotage conformité RGPD - Stockage sécurisé de données - Accès sécurisés aux données bancaires (DSP II)		
4	GESTION DE LA CONFORMITÉ	- Gestion des contrats - Appétence au risque (MiFID II) - Enregistrement des transactions (MiFID II) - Gestion des conflits d'intérêts - Pilotage des exigences réglementaires		
5	VEILLE RÉGLEMENTAIRE	- Base de données réglementaires - Alertes sur l'actualité réglementaire - Pré-analyse et cartographies réglementaires - Gestion du changement réglementaire		
6	REPORTINGS RÉGLEMENTAIRE	- Data management - Assistance à l'automatisation - Qualité de données (BCBS 239) - Reportings de transactions (MiFID, SEC)		
7	GESTION DES RISQUES	- Gestion des risques de non-conformité - Optimisation du risque opérationnel		
8	GESTION D'ACTIFS	- Conformité avec AIFMD - Reportings fonds d'investissement - Evaluation de la performance		

Source: KPMG France

En quoi les Fintechs peuvent-elles contribuer à la gestion des risques pour les banques traditionnelles ?

Les *RegTechs* utilisent des technologies innovantes pour se développer :

Le **Cloud computing**: permet de stocker et d'avoir un accès à des données via internet. Les entreprises l'utilisent pour partager leurs fichiers, suivre des projets à tout moment et n'importe où dans le monde.

L'**Application Programming Interface API**: établit des connexions entre plusieurs logiciels pour échanger des données ou enrichir un programme.

L'**Intelligence Artificielle**: repère les transactions frauduleuses.

Le **Big Data**: analyse rapidement de grands volumes de données afin de satisfaire le Know Your Customer KYC.

Le **Machine Learning**: utilisé par le BigData pour effectuer des prédictions ou découvrir des fraudes potentielles sur un large ensemble de données.

Le **Scoring de risques**: vérifie le niveau de risque d'un individu en fonction des données collectées afin de savoir si un prêt peut être accordé.

La **Biométrie**: sécurise les transactions et identifie formellement un client. Le système capture un élément d'identification d'une personne et le compare à un ensemble de données biométriques déjà enregistrées dans une base de données afin de vérifier l'identité.

La **Blockchain**: « stocke et transmet des informations en toute transparence et sécurité sans utiliser d'organe central de contrôle, ce qui permet de partager des bases de données sans intermédiaire, c'est à chacun de vérifier la validité de la chaîne » d'après la définition de Blockchain France. Le partage des données via une blockchain permet aux banques d'accélérer le règlement des transactions en toute transparence et sécurité.

2. Les atouts des Fintechs

Le savoir-faire et l'évolution permanente des *Fintechs* séduisent les banques qui travaillent avec elles afin de faire bouger leur propre structure en termes de savoir-faire et rester en constante innovation. De plus, les *Fintechs* sont des structures moins denses que les banques et ont une plus grande capacité d'agilité et de développement, c'est ce qui permet leur collaboration. Les *Fintechs* vont se pencher vers des financements sur lesquels les banques ne voudraient pas suivre tant qu'ils ne sont pas sûr de la sécurité envers les entreprises, elles vont prendre des risques que les banques ne peuvent pas se permettre de prendre avant que cela soit testé et fiable. De plus, l'agilité des *Fintechs* est indispensable afin de se conformer à la réglementation changeante. Laurent Girard, cofondateur et COO de Yomoni, une *Fintech* robo-conseiller, a expliqué « Le réglementaire n'agit pas sur nous comme une contrainte mais comme une réelle opportunité de développement et de projection », cela illustre l'avantage incomparable des *Fintechs* sur la réglementation. De plus, les *Fintechs* sont en avance sur les banques du fait de leur taille et sont soumises à des contraintes moindres par rapport aux établissements bancaires et financiers. En effet, la réglementation n'existe pas encore pour les premiers services lancés ce qui leur permet de mettre en place tous les produits qu'elles souhaitent.

En quoi les Fintechs peuvent-elles contribuer à la gestion des risques pour les banques traditionnelles ?

Enfin, il est impératif de contrôler les *Fintechs* afin de respecter le principe du « *level playing field* ». Cela consiste à traiter tous les acteurs de la même manière, avec les mêmes règles, c'est-à-dire que les *Fintechs* doivent répondre aux mêmes règles que les établissements bancaires pour un même service ou un même produit afin d'avoir une compétitivité et une concurrence loyale entre tous les acteurs. C'est pourquoi, en France, les *Fintechs* sont soumises aux règles de droit commun et doivent demander un agrément lorsqu'elles ont une activité bancaire et financière. L'AMF et l'ACPR ont tout de même pris des initiatives en faveur des *Fintechs* principalement pour simplifier les procédures et appréhender au mieux les modalités de supervision. Cependant, une réglementation allégée pour les *Fintechs* afin d'expérimenter des nouveaux services n'est pas encore d'actualité par les autorités de régulation. Malgré la réglementation de plus en plus accrue, les *Fintechs* arrivent à développer de nouveaux concepts. Leur adaptation rapide leur permet d'investir dans de nombreux domaines et de toucher tant les entreprises que les particuliers.

3. La coopération entre établissements bancaires et Fintechs

Il y a quelques années, les banques travaillaient seules, il était inconcevable de travailler avec quelqu'un d'autre, cela était synonyme de faiblesse. Aujourd'hui, c'est presque inconcevable de ne pas travailler avec des *Fintechs* aux vues de tous les bienfaits qu'elles apportent. Le mouvement des banques vers la collaboration est en phase d'accélération, ayant pris conscience qu'il faut bouger rapidement car la pression économique sur les banques est considérable. Les *Fintechs* permettent de développer de nouvelles technologies afin de fabriquer du savoir-faire moins cher et plus efficace. On pourrait dire que les banques et les *Fintechs* sont complémentaires. En effet, les banques garantissent stabilité et fiabilité tandis que les *Fintechs* apportent de l'agilité, de l'innovation et une expertise. Les *Fintechs* doivent tout de même rester indépendantes afin de s'adapter continuellement aux évolutions du marché et aux attentes du consommateur et pouvoir conserver leurs propres atouts.

Ainsi, pour faciliter la coopération entre les grands groupes et les *scale-ups*, la *Fintech* Capgemini a lancé en 2018 un label *Capgemini ScaleUp Qualification*. Une *scale-up* est une *start-up* mûre, ayant déjà levée au moins 1 millions d'euros. Le label permet d'évaluer la maturité des *scale-ups* par rapport à l'équipe, les finances, le business et la technologie afin de les mettre en relation avec des grands groupes. Cela permet donc, par exemple, à une banque française d'être mise en relation avec une *Fintech* du monde entier pour l'aider à se développer sur un certain sujet qu'elle ne parvient pas à résoudre en interne. Les *Fintechs* reçoivent une attestation de Capgemini qui va renforcer sa crédibilité et sa visibilité auprès des banques. Capgemini a un rôle d'entremetteur entre les banques et les *Fintechs* afin qu'ensemble, elles se complètent et se développent.

La coopération entre les banques et les *Fintechs* est indispensable car elles s'apportent mutuellement de la valeur ajoutée. Cependant, il y a certaines limites à la coopération car les *Fintechs* utilisent les données

En quoi les Fintechs peuvent-elles contribuer à la gestion des risques pour les banques traditionnelles ?

des banques pour se développer qui peuvent ensuite être relayées si la *Fintech* travaille avec plusieurs établissements bancaires, ce qui peut être réticent pour les banques.

4. Qu'en est-il de la conformité des Fintechs ?

La conformité est le fait de respecter les normes réglementaires au sein des établissements financiers afin d'éviter d'éventuels sanctions et de donner une bonne image à l'entreprise. Cela permet aussi d'évaluer les risques liés par exemple au blanchiment d'argent et au financement du terrorisme, un des enjeux majeurs des établissements bancaires pour garder leur crédibilité auprès de leurs clients. Les *Fintechs* s'adaptent rapidement pour échapper aux contrôles et contourner la pénibilité réglementaire imposée aux acteurs traditionnels. Cependant, cela peut engendrer des problèmes de non-conformité et nuire à leur collaboration avec les banques qui sont très pointilleux à ce sujet.

Les risques de blanchiment d'argent et de financement du terrorisme

Les *Fintechs* arrivent parfois à esquiver certaines dispositions législatives et réglementaires liées aux activités bancaires. Cependant, cela peut leur causer des torts, par exemple l'ACPR a sanctionné Lemon Way en 2015 pour manquement d'identification pour la lutte anti-blanchiment. Lemon Way est une *Fintech* de solution de paiement automatisée pour les places de marché ou les plateformes de crowdfunding. Elle mettait à disposition ses solutions de paiements aux sites de cartes prépayées et de bitcoins, qui sont des opérations sujettes à des risques de blanchiment d'argent et de financement du terrorisme. Après un contrôle, l'ACPR a observé que la *Fintech* n'avait pas respecté toutes les obligations et les vérifications d'identité et de connaissance de ses clients, qu'il y avait un manquement dans la détection et dans la déclaration de soupçon des personnes politiquement exposées et que le dispositif d'analyse des relations d'affaires était défaillant. L'ACPR a donc infligé une amende de 80 000€ à Lemon Way. Après cela, la *Fintech* a bien-sûr fait le nécessaire pour changer son modèle de développement et répondre aux exigences de conformité (Revue Banque, n°809, mai 2017). On remarque tout de même que les défaillances des *Fintechs* peuvent engendrer des manquements envers la lutte contre le blanchiment et salir les établissements bancaires s'ils sont en collaboration. Les prestataires de services de paiement comme Lemon Way sont très nombreux mais très peu sont agréés par l'ACPR. Le directeur de Tracfin, Bruno Dalles rappelle que « Aujourd'hui, il y en a 400 qui interviennent en France. Mais seuls 35 sont agréés » (Valentin Bontemps, décembre 2016).

De plus, les plateformes de crowdfunding sont susceptibles de générer des risques de financement du terrorisme. En effet, les fonds peuvent aller jusqu'à 300 millions d'euros et c'est impossible de contrôler l'utilisation de toutes les cagnottes, qui peuvent servir à financer des activités liées au terrorisme (Valentin Bontemps, décembre 2016). Ce sont souvent des cagnottes à caractère humanitaire, avec des sommes relativement élevées et une récolte anormalement rapide des fonds. Cette pratique est de plus en plus utilisée car il est difficile de connaître l'utilisateur final lorsque la plateforme de crowdfunding

En quoi les Fintechs peuvent-elles contribuer à la gestion des risques pour les banques traditionnelles ?

n'a pas adopté de vérification KYC. Le service de renseignement Tracfin évoque ce qu'il s'est passé en 2016, l'État Islamique Daech avait utilisé une cagnotte en ligne, soi-disant une aide humanitaire, afin de financer leurs attentats.

Enfin, d'autres produits innovants peuvent semer le doute dans le contrôle de la conformité des *Fintechs*, principalement ceux qui favorisent l'anonymat comme les cartes prépayées anonymes qui sont une source importante de blanchiment d'argent. Il y a également les dispositifs où peuvent s'échanger anonymement de la monnaie électronique tel que la crypto monnaie, qui n'ont aucun statut juridique. Les fonds échangés sont presque intraquables ce qui favorise le contournement des règles. De même pour les Initial Coin Offerings ICO qui sont des jetons numériques utilisés pour des opérations de levées de fonds en crypto-actifs, n'ayant aucune réglementation, des fonds illégaux peuvent être financés avec ces jetons puis convertis en monnaie légale et perçus comme le financement d'un projet quelconque (Anne Vidalie, Novembre 2018). On peut aussi identifier les applications de transfert d'espèces permettant de retirer de l'argent liquide dans des points de vente en utilisant un code échangé par sms, il n'y a aucune réglementation pour les transferts d'espèces ce qui rend facile l'échange de monnaie illégale.

La Banque de France estime que les *Fintechs* peuvent « créer dans le système financier de nouvelles vulnérabilités dans la lutte contre le blanchiment et le financement du terrorisme si ces dispositifs de contrôle ne sont pas au niveau ». C'est pourquoi de plus en plus de dispositifs sont mis en place afin de limiter les risques et de les contrôler.

Les risques de divulgation d'informations confidentielles des banques par les Fintechs

Selon une étude d'ImmuniWeb sur les 100 plus grandes *Fintechs* du monde, seules 2 ont une cybersécurité acceptable. En effet, seulement BrexInc et N26 ont un chiffrement SSL complet, respectent les recommandations PCI DSS (Payment Card Industry Data Security Standard) et sont conformes aux exigences du Règlement Général sur la Protection des Données RGPD (Laurent Mavallet, Août 2019). La cybersécurité a pour but de protéger les données et les ressources informatiques de la société afin de contrer tous les pirates. Si des failles existent, cela signifie que les données peuvent être récupérées illégalement et utilisées à des fins non voulues. Les banques ont un nombre massif de données confidentielles, tant sur leur client que sur leur stratégie commerciale et leurs informations personnelles. Ainsi, les banques acceptant de travailler avec des *Fintechs* doivent aussi accepter de partager des données confidentielles. Cela peut avoir un impact sur leur décision de coopérer ou non car les banques ne peuvent pas se permettre de donner des informations strictement confidentielles et pouvant être relayées par la *Fintech* si celle-ci coopère avec d'autres établissements bancaires.

En quoi les Fintechs peuvent-elles contribuer à la gestion des risques pour les banques traditionnelles ?

Tout d'abord, le principe d'open banking, depuis janvier 2018, impose les banques à partager leurs données avec d'autres acteurs, comme les *Fintechs*. Les banques n'ont pas le choix de partager ces informations et accepter le développement des *Fintechs* mais l'Open Banking ne touche pas aux informations purement personnelles des banques c'est pourquoi celles-ci vont choisir avec quelles *Fintechs* elles souhaitent collaborer. Les banques peuvent par exemple imposer aux *Fintechs* de réaliser des stress-tests afin de connaître leur résistance aux situations critiques. Un stress-test modélise et analyse des scénarios pour établir des prévisions tout au long de l'année. Si le stress-test de la *Fintech* est positif, cela montre la fiabilité de celle-ci. Cependant, malgré un stress-test positif, si l'entreprise travaille avec plusieurs banques, les informations peuvent être relayées et utilisées pour autre chose, il faut donc prendre du recul sur les stress-tests.

De nombreuses banques utilisent des serveurs internes afin que leurs données restent bien au sein de leur entreprise car les règles des autres pays peuvent être différentes. Par exemple, si le serveur est basé en Angleterre, en Irlande ou aux États-Unis, la loi du patriot act est prise en compte c'est-à-dire que pour tout soupçon de fraude, de financement du terrorisme ou autres, les autorités américaines auront accès aux données, ce qui est à l'encontre du principe de protection des données. La solution des banques pour ne pas se faire désintermédier par les *Fintechs* est de racheter des parts de la société et ainsi prendre le contrôle de celle-ci. C'est le cas de la Société Générale qui a racheté Boursorama ou encore BNP Paribas avec Hello Bank. Les banques sont vigilantes dans les partenariats et dans la façon de collaborer, il faut que la *Fintech* soit sérieuse, que le service réponde bien au problème et qu'il y ait un intérêt économique.

Les risques de divulgation d'informations confidentielles de la clientèle bancaire par les Fintechs

La plupart des *Fintechs* ont besoin des données clients pour faire fonctionner leur activité. Cependant, les banques sont régies par le secret bancaire et n'ont normalement pas le droit de donner des informations sur leurs clients à des tiers. Cet engagement permet d'avoir la pleine confiance de leurs clients, très importante pour l'éthique de la banque. Si malheureusement la *Fintech* se fait hacker ou qu'il y a une fuite des données, c'est l'image et la réputation de la banque qui est remise en question.

Par exemple, les agrégateurs sont de plus en plus utilisés par les *Fintechs*, ils permettent à un utilisateur de centraliser ses données bancaires sur une seule application s'il possède des comptes dans différents établissements bancaires. Pour utiliser un agrégateur, il faut que le client lui confie tous ses identifiants et mots de passe d'accès à ses comptes bancaires pour que l'agrégateur télécharge ses données et les mette à disposition sur son site ou son application. Les agrégateurs ne sont pas soumis aux mêmes obligations que les banques car ce n'est pas à proprement parler un service bancaire et la protection des données peut faire l'objet de questionnement. On ne peut pas réellement savoir si l'agrégateur n'utilisera plus les données d'accès lorsque le client souhaitera arrêter le service. Les banques remettent en cause

En quoi les Fintechs peuvent-elles contribuer à la gestion des risques pour les banques traditionnelles ?

l'activité des agrégateurs par rapport à la conservation des données sur des serveurs insuffisamment sécurisés (Aline Fauvarque, janvier 2019). En effet, pour une banque, si leurs données clients se retrouvent utilisées pour d'autres choses par les agrégateurs, cela porte atteinte à l'image de la banque et à sa fiabilité. De plus, si une fraude a lieu, c'est la banque qui est tenue de rembourser le client alors que le problème pourrait venir de l'agrégateur, ce qui n'enchant pas spécialement les banques.

On doit aussi se méfier de l'usage des *API* qui, comme vu précédemment, servent à établir des connexions entre plusieurs logiciels pour échanger des données. En effet, lorsqu'un établissement bancaire fournit des données à une *Fintech* via des *API*, il est responsable de leur bon usage. S'il y a un usage frauduleux de certaines données ou une usurpation d'identité, la banque sera fautive et se verra infligée une lourde amende par le RGPD (Revue Banque, Avril 2019). C'est pour cela que les banques doivent prendre des précautions en tant que fournisseurs de données aux *Fintechs*.

5. Les solutions apportées aux problèmes de non-conformité

Les transactions des *Fintechs*, la plupart du temps anonymes et avec des montants élevés sont souvent facteur de risque de blanchiment et de financement du terrorisme. C'est pourquoi les *Fintechs* prennent des mesures réglementaires afin de vérifier leurs transactions et lutter contre le blanchiment et le financement du terrorisme et garder la confiance des banques. Tout d'abord, pour pouvoir exercer son activité, la *Fintech* doit choisir un statut réglementé pour éviter les risques de non-conformité (Bankobserver, Octobre 2017). Le statut agréé permet d'obtenir un agrément de la part de l'ACPR sur le statut de l'entreprise : établissement de crédit, de paiement, de monnaie électronique, d'investissement, d'assurance, société de financement, prestataire de services d'information sur les comptes ou prestataire de services d'initiation de paiement. Pour obtenir l'agrément, la *Fintech* doit remplir certaines conditions comme un respect des obligations réglementaires de Lutte contre le Blanchiment de Capitaux et le Financement du Terrorisme LCB/FT ou encore un dispositif de contrôle interne et de conformité. Ce statut permet à la *Fintech* d'être crédible auprès des établissements bancaires et de montrer sa conformité. Le statut d'intermédiaire nécessite une déclaration auprès de l'ACPR ou de l'Organisme pour le Registre unique des Intermédiaires en Assurance ORIAS en tant qu'agent financier, distributeur, intermédiaire en opérations de banque et services de paiement, en assurance, en financement participatif, conseiller en investissement participatif ou financier. Les *Fintechs* ayant le statut d'intermédiaire sont assujetties au dispositif LCB/FT et devront donc vérifier régulièrement la traçabilité des circuits financiers et la lutte contre l'anonymat. La collaboration entre une banque traditionnelle et une *Fintech* bénéficiant d'un des statuts précédents se fait plus facilement car cela prouve l'engagement de la *Fintech* dans la LCB/FT.

Les *Fintechs* peuvent utiliser les outils des *RegTechs* pour contrer les malfaiteurs. La technologie *blockchain* stocke toutes les transactions, elle peut donc identifier les transactions suspectes grâce à sa

En quoi les Fintechs peuvent-elles contribuer à la gestion des risques pour les banques traditionnelles ?

décentralisation et la sécurisation de ses données (Bankobserver, Décembre 2018). Pour cela, les analystes Anti-Money Laundering AML, des analystes de lutte contre le blanchiment d'argent qui surveillent et enquêtent sur les activités financières suspectes, devront collaborer avec les auditeurs et les employés des banques pour rendre le blanchiment d'argent plus facile à détecter. Pour le moment, la lutte contre le blanchiment est très individualisée au niveau des institutions mais aussi de chaque pays qui ont leurs propres lois. Si les régulateurs du monde entier coopèrent et adoptent la technologie *blockchain*, les transactions risquées seront détectées et traitées rapidement ce qui permettrait aux *Fintechs* d'aider les institutions financières dans leur lutte contre le blanchiment d'argent. C'est ce qui s'est passé en 2017, la *Fintech* « Know Your Customer » a gagné le *Fintech* Startup Challenge organisé par le Village by Crédit Agricole. Le Know Your Customer permet, grâce au numérique, d'identifier et de vérifier rapidement l'identité du client et de contribuer aux fonctions de conformité et à la gestion des risques afin de réduire ou même de supprimer le risque de blanchiment d'argent et de financement du terrorisme (Finextra, Mars 2018).

Le service de renseignement Tracfin et les institutions de réglementations comme l'ACPR et l'AMF ont mis en place un cadre juridique encadré afin de réguler les nouvelles *Fintechs*. Comme vu précédemment, le crowdfunding est source de blanchiment d'argent et de financement du terrorisme s'il n'est pas surveillé et réglementé. C'est pourquoi la réglementation est plus accrue et les gérants de plateformes de crowdfunding ont maintenant la responsabilité de contrôler les différents projets et doivent envoyer une déclaration de soupçon à Tracfin dès qu'un doute apparaît. Des réglementations sont mises en place par la publication de l'ordonnance du 1^{er} décembre 2016 obligeant les plateformes de crowdfunding à acquérir le statut d'intermédiaire en financement participatif délivré par l'ORIAS et contrôlé par l'ACPR (Mipise, Février 2018). Ces organismes vont soutenir et réguler les plateformes afin de prévenir des pratiques frauduleuses et dangereuses. Les plateformes doivent aussi être immatriculées au registre de l'ORIAS, les utilisateurs pourront ainsi vérifier l'agrément de la plateforme et si elle a les garanties suffisantes. De plus, la France est très impliquée dans la LCB/FT car les menaces que soulèvent le terrorisme ainsi que la nécessité de préserver l'intégrité du système financier est la priorité pour notre pays. C'est pourquoi le Conseil d'Orientation de la Lutte contre le Blanchiment de capitaux et le financement du terrorisme COLB a publié l'analyse nationale des risques en 2019 afin d'identifier à l'échelle nationale les principaux risques que peut engendrer chaque vecteur du blanchiment et du financement du terrorisme (Didier Banquy, Septembre 2019). Cette analyse va permettre aux banques et aux *Fintechs* de connaître les adaptations à effectuer et les vigilances à prendre en fonction de l'évolution permanente de ces risques.

Enfin, l'entrée en vigueur de la DSP2 – Directive Européenne sur les Services de Paiement – où les normes sont appliquées depuis septembre 2019, est en faveur des banques (Meilleurtaux.com, Février 2019). En effet, les établissements bancaires refusent systématiquement toutes dispositions concernant

En quoi les Fintechs peuvent-elles contribuer à la gestion des risques pour les banques traditionnelles ?

les agrégateurs afin de se protéger et de garder leurs données sécurisées. Par exemple, les agrégateurs doivent passer par les banques pour effectuer certaines opérations comme la modification des bénéficiaires de virement ou pour demander l'IBAN d'un client qui est parfois refusé par la banque. Ainsi, malgré la méfiance des banques sur les *Fintechs*, la loi soutient les banques et les clients afin d'éviter au maximum les fraudes et de garantir la protection des données. On peut donc coopérer avec des *Fintechs* et leur faire confiance sur la protection des données dans certains cas même s'il faut continuer à être méfiant et ne pas tout accepter.



Conclusion

Le but de cette étude était de comprendre en quoi les *Fintechs* pouvaient contribuer à la gestion des risques pour les banques traditionnelles. Les *Fintechs* sont indispensables aux banques, leurs spécialisations leur permettent d'être expertes dans un domaine en particulier et pouvoir développer certains aspects que les banques n'ont pas le temps de traiter en interne. De plus, grâce à leur taille restreinte, les *Fintechs* sont agiles et s'adaptent rapidement aux évolutions bancaires et financières, ce qui est un atout primordial pour leur collaboration avec les banques traditionnelles, qui ne peuvent se conformer aussi rapidement aux exigences réglementaires par exemple. Cependant, par leur agilité, les *Fintechs* ont la capacité de contourner les réglementations ce qui les confrontent au risque de non-conformité et dégrade la relation de confiance avec les banques. Les plateformes de crowdfunding sont parfois responsables de financement du terrorisme lorsque celles-ci ne sont pas réglementées, ce qui peut freiner une éventuelle collaboration avec les banques qui vont avoir peur de salir leur image. C'est pourquoi des solutions sont mises en place pour contrôler les *Fintechs* comme les institutions financières et réglementaires tel que la RGPD, l'ACPR ou encore l'AMF qui vont surveiller les activités des *Fintechs* et vérifier si elles sont bien en accord avec la réglementation actuelle. En ce qui concerne la lutte contre le blanchiment et le financement du terrorisme, le service de renseignement Tracfin recueille, analyse et enrichit les déclarations de soupçons déclarées, cela permet de renforcer la LCB/FT, d'identifier les malfaiteurs et de voir si les *Fintechs* sont impliquées dans cette lutte, un des enjeux majeurs des établissements financiers.

Les *Fintechs* sont en pleine expansion depuis quelques années mais avec la crise actuelle, vont-elles pouvoir rebondir face aux nouvelles dynamiques de marchés et à la reprise tardive de l'économie ?

Bibliographie

Livres :

Régis Bouyala, 2018, « La révolution Fintech : acte 2 », Revue Banque.

Thierry Bonneau et Thibault Verbiest, 2017, « Fintech et Droit », Revue Banque.

Articles :

Aline Fauvarque, Janvier 2019, « Peut-on faire confiance aux agrégateurs de comptes bancaires ? », lerevenu.com, référence du 01 mars 2020. <https://www.lerevenu.com/finances-privees/banque/peut-faire-confiance-aux-agregateurs-de-comptes-bancaires>

Anne Vidalie, Novembre 2018 « Cryptomonnaies : Tracfin tire la sonnette d'alarme », leexpress.fr, référence du 04 avril 2020. https://www.lexpress.fr/actualite/societe/justice/cryptomonnaies-tracfin-tire-la-sonnette-d-alarme_2050598.html.

Bankobserver-wavestone.com, Octobre 2017, « Décryptons le cadre réglementaire appliqué aux Fintechs », Risques et conformité, Décryptage, référence du 19 avril 2020. <https://www.bankobserver-wavestone.com/decryptons-cadre-reglementaire-applique-aux-fintechs/>

Bankobserver-wavestone.com, Décembre 2018, « La Blockchain et son impact sur la lutte contre le blanchiment d'argent », Risques et conformité, Éclairage, référence du 19 avril 2020. <https://www.bankobserver-wavestone.com/blockchain-impact-lutte-contre-blanchiment-dargent/>

Capgemini ScaleUp Qualification, référence du 15 mars 2020. <https://scaleup-qualification.capgemini.com/landing>

Didier Banquy, Septembre 2019, « Analyse nationale des risques de blanchiment de capitaux et de financement du terrorisme en France », Rapport du COLB, référence du 18 mars 2020.

Finextra, Mars 2018, « Know Your Customer wins Crédit Agricole startup challenge », finextra.com, référence du 15 mars 2020. <https://www.finextra.com/pressarticle/73077/know-your-customer-wins-credit-agricole-startup-challenge>

Laurent Mavallet, Août 2019, « Graves manquements en cybersécurité dans les Fintechs », CIO, référence du 20 mars 2020.

Mipise.com, Février 2018, « La réglementation des plateformes de financement participatif au service de la lutte contre le blanchiment des capitaux et contre le financement du terrorisme », référence du 18 mars 2020. https://www.mipise.com/fr/platform_blog_posts/lutte-contre-blanchiment-capitaux-et-contre-le-financement-du-terrorisme-et-plateformes-de-financement-participatif

Revue banque, n°809, Mai 2017, « L'APCR sanctionne une Fintech », référence du 15 mars 2020.

Revue banque, n°379, Avril 2019, « API : comment organiser l'exposition des données ? », référence du 15 mars 2020.

Valentin Bontemps, Décembre 2016, « Le développement des « Fintech », un défi pour la lutte anti-blanchiment », OLJ, référence du 20 mars 2020.

En quoi les Fintechs peuvent-elles contribuer à la gestion des risques pour les banques traditionnelles ?