Galitt
Payment Consulting

DSP2 & OPEN API : menaces et opportunités pour le secteur bancaire

En route vers l'Open-Banking ?

LIVRE BLANC
Décembre 2016

DE GAULLE
FLEURANCE
& ASSOCIÉS
SOCIÉTÉ D'AVOCATS

Sommaire

A propos de ce document & remerciements

La société Galitt, spécialisée dans les paiements, et la société d'avocats De Gaulle Fleurance & Associés ont uni leurs compétences pour la rédaction d'un livre blanc portant sur l'Open-Banking et les enjeux de la transposition en France de la seconde Directive sur les Services de Paiements *(Directive 2015/2366)*, dite DSP2, qui abrogera la Directive 2007/64/CE *(DSP1)*, actuellement en vigueur en France au travers de sa transposition dans le Code monétaire et financier.

Pour leur participation et expertise, nous tenons à remercier vivement :

Joan Burkovic : *CEO de Bankin'*

Joan Burkovic, diplômé de l'ESSEC et de HEC Lausanne, a co-fondé Bankin' avec Robin Dauzon en 2011. Il est aussi l'un des fondateurs et membre du conseil d'administration de l'association France Fintech et porte-parole du « European AIS », le groupement des services d'information sur les comptes bancaires au niveau Européen.

Bankin' est une application qui agit comme un coach financier, personnel et intelligent pour aider ses utilisateurs à mieux gérer leurs finances au quotidien. Elle est aujourd'hui présente dans quatre pays : Royaume-Uni, Allemagne, Espagne, France, et compte plus de 1,5 millions d'utilisateurs.

Sébastien Taveau : *Chief Developer chez Early Warning*

Sébastien Taveau, est Chief Technologist chez Early Warning, où il supervise les opérations de technologie et d'innovation pour les solutions de paiement P2P. Fort d'une expérience de plus de vingt ans des technologies de paiement mobile, il se définit comme un résolveur de puzzle et un observateur d'horizon. Sébastien Taveau est un expert reconnu sur l'Open-API, avec de nombreux articles et interventions sur CNN, The Wall Street Journal, The Huffington Post, Mashables, Reuters, Forbes, Dark Reading, Digital Transactions, Newsweek...

Early Warning est une société spécialisée dans les technologies de paiement mobile. Créée il y a 25 ans par Wachovia, JPMorgan Chase, Bank of America, BB&T Corporation et Wells Fargo, Early Warning est au cœur de l'actualité avec le lancement de Zelle.

Jérôme Raguénès : *Responsable de la Coordination Numérique à la Fédération Bancaire Française (FBF)*

Jérôme Raguénès est responsable de la coordination numérique auprès de la Direction générale de la Fédération Bancaire Française depuis novembre 2015. Il est membre du Groupe de stratégie numérique du Comité exécutif de la Fédération bancaire européenne.

Il a une expérience de près de vingt ans dans les systèmes et moyens de paiement. Consultant pendant dix ans sur d'importants projets stratégiques pour des grands groupes bancaires, il est appelé par la FBF en 2002 pour coordonner le projet SEPA, prendre en charge les dossiers règlementaires des moyens de paiement et défendre les intérêts des banques françaises auprès des institutions nationales et européennes.

La Fédération Bancaire Française *(FBF)* est l'organisation professionnelle qui représente toutes les banques installées en France. Elle compte 378 entreprises bancaires adhérentes de toutes origines *(commerciales, coopératives ou mutualistes)*, françaises ou étrangères.

FEDERATION BANCAIRE FRANCAISE

A propos de De Gaulle Fleurance & Associés

La société De Gaulle Fleurance & Associés *(Paris et Bruxelles)* regroupe aujourd'hui plus de 110 avocats et juristes, dont 40 associés.

Tous les avocats ont une compétence transversale adossée à un ou plusieurs pôles d'excellence *(droit public et administratif, propriété intellectuelle, droit bancaire, nouvelles technologies, fiscalité, droit commercial, structuring corporate…)* en matière de conseil comme de contentieux, en ce compris la dimension internationale.

La société De Gaulle Fleurance & Associés est organisée autour de deux pôles :

- le pôle structure répond aux besoins concernant la structure du capital social et humain des décideurs, qu'ils soient publics ou privés et à leur gouvernance. Il s'agit de tout l'aspect organisationnel du service avec la recherche d'une optimisation des structures et l'exercice rationnel des compétences
- le pôle exploitation est dédié aux besoins concernant l'activité opérationnelle des décideurs publics ou privés avec la gestion des ressources humaines, la mobilisation des financements, l'optimisation des circuits décisionnels.
  Pour en savoir plus : www.degaullefleurance.com

Contact :
Thibault Verbiest
Avocat associé
+33 6 25 44 12 71
tverbiest@dgfla.com

A propos de Galitt

Référence dans le secteur de la monétique et des transactions électroniques, Galitt est leader en France dans l'ensemble de ses activités et dans le monde pour ses outils de tests et son expertise dans les technologies innovantes.

Galitt propose un ensemble de métiers et de savoir-faire complémentaires et reconnus pour assister ses clients sur tout le cycle de vie des projets et sur la totalité des composants de la chaine de valeur du paiement. Sa dimension lui permet d'appréhender des projets d'envergure, tout en conservant la réactivité, l'encadrement et les motivations d'une structure à taille humaine.

Galitt est la référence dans la mise en œuvre de technologies de paiement les plus avancées et la définition des architectures de demain.

L'offre de Galitt s'organise autour de 5 Business units :

- Les experts de **Payment Consulting** et leurs approches innovantes éclairent les choix stratégiques des décideurs
- Les consultants de **Payment Services** assistent les clients dans la mise en œuvre de leurs projets de paiement
- Les équipes de **Testing Solutions** développent des logiciels de test et participent aux phases d'industrialisation des tests ou de certification des solutions
- Les collaborateurs de **Payment Solutions** développent et opèrent des applications monétiques et transactionnelles à forte valeur ajoutée
- Les formateurs de **Payment Education** relayent l'expertise et le métier de Galitt lors de séminaires de formation

En 2015, Galitt a réalisé un chiffre d'affaires de 31 millions d'euros et employait 240 personnes.

Pour en savoir plus sur Galitt, rendez-vous sur notre site internet : www.galitt.com

Contact Galitt Payment Consulting :
Rémi Gitzinger
Directeur Exécutif
+33 6 20 66 77 40
r.gitzinger@galitt.com

Contexte

Proposée par la Commission Européenne, votée définitivement par le Parlement européen en 2015 et avec une transposition en droit français prévue au plus tard pour janvier 2018, la directive DSP2 ouvre la voie règlementaire à une nouvelle notion : l'Open-Banking. Désormais, la liberté des clients à disposer de leurs données bancaires pourra contraindre les banques à la mise à disposition de ces dernières à des tiers, au travers d'Interfaces de programmation *(API)*, avec pour objectif majeur de stimuler la concurrence et l'innovation dans le secteur.

Cette ouverture des données bancaires et leur mise à disposition à des tiers soulèvent de nombreuses interrogations et controverses, en France et en Europe, qui feront l'objet d'analyses détaillées dans ce document.

Problématique

La DSP2, comment transposer le droit d'accès et quels impacts sur l'écosystème bancaire ?

Dans une première partie, les incidences juridiques seront analysées. Afin d'enrichir ce document, trois interviews ont été réalisées permettant de présenter les enjeux pour les différentes parties prenantes. Dans une deuxième partie sera présenté le nouvel écosystème qui se met en ordre de marche en Europe, et seront analysées les conséquences en matières techniques et opérationnelles. Enfin, la troisième partie présentera les enjeux pour l'écosystème bancaire et les diverses initiatives déjà observables.

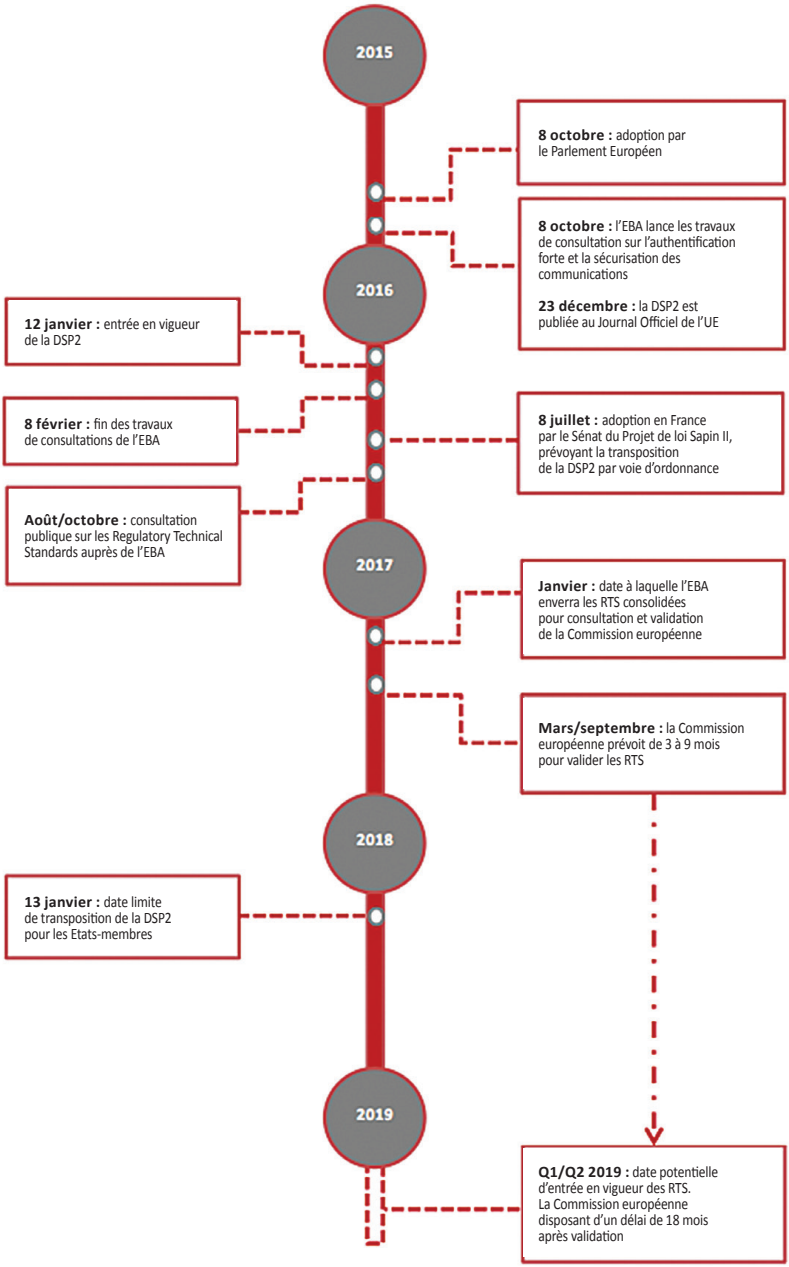
Afin de garder à l'esprit les échéances, un calendrier de mise en œuvre de la DSP2 est disponible dans ce livre blanc. Le mois d'octobre 2016 marque un avancement important dans le calendrier de la DSP2. Cette date met fin à la consultation de l'ensemble des acteurs européens par l'European Banking Authority *(EBA)*. Lancée en août 2016, cette consultation visait à recueillir les points de vue de l'ensemble des parties prenantes autour des aspects réglementaires et techniques, liés aux exigences d'authentification forte du client et aux exigences de sécurité des communications portées par cette directive.

Définitions issues de l'European Banking Authority [1]

- **EBA** *(European Banking Authority ou Autorité Bancaire Européenne)* : autorité indépendante de l'Union Européenne qui œuvre afin de garantir un niveau de règlementation et de surveillance prudentielle efficace et cohérent dans l'ensemble du secteur bancaire européen.
- **RTS** *(Regulatory Technical Standards ou Standards Techniques)* : ensemble des standards techniques préparés par l'Autorité Bancaire Européenne en collaboration avec la BCE *(Banque Centrale Européenne)* et les banques centrales nationales. Ces standards techniques sont discutés avec l'ensemble des parties prenantes au travers des « discussions papers ». Ils portent essentiellement sur l'authentification forte et les moyens de communication sécurisés, afin de permettre la mise en œuvre opérationnelle de la directive. Ces standards seront soumis à la Commission Européenne en 2017 pour application règlementaire.
- **API** *(Application Programming Interface ou Interface de programmation)* : ensemble normalisé de classes, de méthodes ou de fonctions mises en œuvre pour accéder à des services ou à des données. Ces interfaces doivent être évolutives, réutilisables et sécurisées, tout en offrant une facilité d'utilisation pour les développeurs informatiques.
- **Open-API :** principe consistant à exposer à des tiers autorisés, externes à la structure, une interface de programmation permettant l'accès à des données et/ou services propres pour répondre à tout type de besoin.
- **Open-Data :** concept portant sur l'ouverture des données afin qu'elles soient librement accessibles, utilisables et reproductibles par tous, sans restrictions de droits d'auteurs, de brevets ou d'autres mécanismes de contrôle.
- **Open-Banking :** concept actuellement en cours d'élaboration autour de l'évolution de la banque. L'Open-Banking est fondé sur le principe de la transparence bancaire ; il prône le recours aux Open APIs afin de permettre à des tiers d'accéder aux informations dans le but de développer leurs propres applications.

*1 - **EBA** : Definitions / Open APIs and Open-Banking*

LES DATES CLÉS DE LA DSP2



1. Le cadre juridique

1.1. Quelques définitions posées par la DSP2

- **PSU** *(Payment Service User ou Utilisateur d'un service de paiement)* : utilisateur particulier ou professionnel possédant un ou plusieurs comptes bancaires et/ou utilisateur d'un service de paiement.
- **ASPSP** *(Account Servicing Payment Service Provider ou Prestataire de services services de paiement gestionnaires de comptes)* : prestataire au sein duquel un client *(PSU)*, détient un ou plusieurs comptes et/ou au sein duquel le PSU initie des paiements. Chaque ASPSP doit posséder le statut d'Établissement de Paiement *(EP)**, avec si nécessaire un passeport lui permettant d'exercer dans différents pays ; les établissements de crédit, de monnaie électronique et les établissements de paiement déjà agréés sont considérés comme étant ASPSP.

> ** **Précision - Etablissement de Paiement (EP) :** ils ont été créés suite à la Directive sur les Services de Paiement (DSP) de 2009. Auparavant, seuls les banques et les établissements de crédit avaient l'autorisation de fournir des services de paiement. Avec le développement du paiement en ligne, de nouveaux acteurs, de tailles plus petites se sont vu accorder le droit d'obtenir ce statut afin de rendre le paysage plus concurrentiel. Ce statut est délivré par les autorités financières du pays dans lequel la demande est effectuée ; en France il s'agit de l'Autorité de Contrôle Prudentiel et de Résolution (ACPR), liée à la Banque de France. L'obtention et la conservation d'un agrément relèvent de procédures rigoureuses afin d'apporter des garanties fortes aux utilisateurs des services de paiements.*[2]

- **TPP** *(Third Party Provider ou PSP Tiers)* : prestataire pouvant initier des paiements à la demande du payeur, sans détenir les fonds et à partir de comptes qu'il ne gère pas, et offrir des informations consolidées sur ces comptes.

  Il comprend les deux catégories de prestataires suivants :

  - **PISP** *(Payment Initiation Service Provider ou Prestataire de Services d'Initiation de Paiement)* : prestataire proposant un service qui consiste à initier un ordre de paiement à la demande d'un PSU à partir d'un compte bancaire détenu par un ASPSP.
  - **AISP** *(Account Information Service Provider ou Prestataire de Services d'Information sur les Comptes)* : prestataire fournissant un service de consolidation des informations relatives à un ou plusieurs comptes détenus par un PSU auprès d'un ou plusieurs ASPSPs.

2 - ***ACPR** : Définition Etablissement de paiement*

Sans conteste, la principale innovation de la DSP2, et celle qui fait le plus débat, est la reconnaissance de deux nouveaux services de paiement qui permettent à un tiers de s'interposer entre un utilisateur et son ASPSP : le service d'initiation de paiement et le service d'information sur les comptes.

Ces nouveaux prestataires de paiement bénéficient de conditions d'exercice allégées et d'exigences prudentielles assouplies par rapport aux ASPSPs. Ces nouveaux prestataires devront toutefois, comme les autres établissements de paiement, faire l'objet d'un agrément *(d'un enregistrement pour le service d'information sur les comptes)* et être couverts par une assurance responsabilité civile professionnelle équivalente couvrant les territoires où ils fournissent leurs services et dont le montant minimal devra être défini selon des critères définis par une orientation à venir de l'EBA.

1.2. Droit d'accès

Les articles 66 et 67 de la DSP2 ont instauré d'une part, un droit d'accès au compte de paiement pour les prestataires de services d'initiation de paiement *(« PISP »)* et d'autre part, un droit d'accès aux données du compte de paiement pour les prestataires de services d'information sur les comptes *(« AISP »)*.

Ces droits d'accès sont assortis d'un certain nombre de garanties :

1. La limitation aux seuls comptes de paiement accessibles en ligne ;
2. L'exigence d'un consentement explicite donné par l'utilisateur des services de paiement pour chaque communication de ses données ;
3. La non-détention de fonds du payeur par les PISPs ;
4. L'inaccessibilité des données de sécurité personnalisées *(données d'authentification ou credentials)* à des tiers et leur transmission à l'utilisateur et à l'émetteur au moyen de canaux sûrs et efficaces ;
5. La communication de manière sécurisée avec les seuls prestataires de services de paiement gestionnaire du compte *(« ASPSP »)*, payeurs et bénéficiaires conformément aux futures normes techniques de réglementation de l'ABE ;
6. L'absence de modification par les PISPs des caractéristiques de l'opération *(montant, bénéficiaire, etc.)* ;
7. La limitation de l'accès des AISPs aux seules informations provenant des comptes de paiement désignés et des opérations de paiement associées ;
8. L'absence de stockage par les PISPs des données de paiement sensibles concernant l'utilisateur de services de paiement ; Il faut entendre par données de paiement sensibles « des données, y compris les données de sécurité personnalisées, qui sont susceptibles d'être utilisées pour commettre une fraude ». La catégorie recouvre les données de sécurité personnalisées et ...

... exclut, mais seulement vis-à-vis de l'activité des PISPs et AISPs, le nom du titulaire du compte et le numéro dudit compte ;

9. L'absence de demande de communication par les AISPs des données de paiement sensibles liées à des comptes de paiement ;

10. La limitation des données pouvant être demandées à l'utilisateur de services de paiement à celles uniquement nécessaires pour fournir le service d'initiation de paiement ou le service d'information sur les comptes ;

11. L'utilisation, la consultation et le stockage des données aux seules fins de fournir le service d'initiation de paiement ou le service d'information sur les comptes ;

12. La faculté pour les ASPSPs de refuser l'accès des PISPs et des AISPs à un compte de paiement pour des raisons objectivement motivées et documentées liées à un accès non autorisé ou frauduleux, y compris l'initiation non autorisée ou frauduleuse d'une opération de paiement.

1.3. Prohibition des données de paiement à des fins commerciales ?

La DSP2 ne prohibe pas expressément l'utilisation des données de paiement à des fins commerciales *(à la différence du droit anti-blanchiment)*. L'enjeu tient en effet dans la propriété des données bancaires et leur réutilisation par les nouveaux entrants dans le cadre du Big Data. Toutefois les articles 66 et 67 de la DSP2 devraient être interprétés comme prohibant l'utilisation des données bancaires à des fins commerciales :

- le prestataire de service d'initiation de paiement « n'utilise, ne consulte ou ne stocke des données à des fins autres que la fourniture du service d'initiation de paiement expressément demandée par le payeur » *(art. 66, § 1, g)* ;
- le prestataire de service information sur les comptes « n'utilise, ne consulte ou ne stocke des données à des fins autres que la fourniture du service d'information sur les comptes expressément demandée par l'utilisateur de services de paiement, conformément aux règles relatives à la protection des données » *(art. 67, §2, f)*.

Au-delà de cet éclairage juridique, il est important de souligner que les PSP Tiers *(Third Party Providers)* se sont développés bien avant la directive. La Commission européenne a souhaité intervenir afin de réguler ces nouvelles pratiques avec pour objectifs majeurs de leur octroyer un nouveau cadre réglementaire adapté et de favoriser leur développement dans une logique de libre concurrence.

Ces nouveaux acteurs, leurs offres de services et leur intégration au sein de la chaîne de paiement sont décrits et analysés dans cette seconde partie. Un éclairage relatif aux incidences techniques liées aux partages des données des banques sera également apporté.

ENCART 1 INTERVIEW

Jérôme Raguénès

Responsable Coordination Numérique - Fédération Bancaire Française

Galitt : *pouvez-vous nous exposer la manière dont les banques appréhendent l'arrivée de nouveaux acteurs facilitée en cela par le développement du numérique et les nouvelles règlementations ?*

Jérôme Raguénès : le secteur bancaire est très concurrentiel et le devient encore davantage par la mise en œuvre successive de règlementations contraignantes qui permettent désormais à de nouveaux acteurs de venir concurrencer les banques sur plusieurs de leurs activités :

- sur les services de financement : le durcissement de la règlementation bancaire a permis le développement de nouvelles formes d'accès au crédit proposées par des plates-formes de financement participatif ;
- sur les services d'investissement : les firmes de négociation à haute fréquence représentent un quart des volumes traités sur le marché action mais jouissent d'un cadre règlementaire leur permettant d'opérer sans grand capital alors que les banques sont contraintes par des exigences en fonds propres importantes ;
- sur les services de paiement via l'émergence de tiers de paiement rendue possible par la DSP2.

En considérant le seul cas de la DSP2, on peut juger singulier le cadre de relations imposé par cette directive qui contraint, d'une part, les banques à autoriser l'accès aux données des comptes de leurs clients et, d'autre part, permet aux tiers de paiement *(Third Party Provider - TPP)* de mouvementer les comptes dont les banques ont la responsabilité.

Bien que la règlementation fixe certaines règles, elle omet d'en préciser le cadre, ainsi :

- alors que la règlementation impose aux banques de créer des infrastructures ad hoc pour accueillir ces nouveaux acteurs, il n'y a rien, à ce stade, dans les textes *(directive ou RTS en cours d'élaboration)* qui interdise formellement l'usage du « *web scraping* » ;
- de plus, les banques ne peuvent exiger de relations contractuelles avec les TPP ni les empêcher d'agir, rendant difficile tout développement de modèle économique.

Par ailleurs, on peut considérer que si le législateur a souhaité que la banque demeure le premier recours en cas de contestation et qu'elle rembourse le client en cas de problème avec un TPP, c'est bien la preuve qu'il considère, sans le dire, la banque comme l'acteur le plus fiable pour le client.

Cependant, le législateur a prévu d'assurer un minimum de sécurité et a demandé à l'Autorité Bancaire Européenne *(ABE)* de définir des normes techniques règlementaires visant à définir les modalités d'interaction entre agents afin de préserver la sécurité des services de paiement.

A ce stade, s'agissant des dérogations à l'authentification forte telle que promue par l'ABE, on peut regretter l'absence du principe d'approche par les risques alors que celui-ci est efficace et permet une lutte ciblée contre la fraude grâce à des mesures proportionnées et adaptées au contexte.

A cette réalité règlementaire, qui a pour objet d'accroître une concurrence déjà forte entre les banques, s'ajoute une révolution technique sans précédent apportée par le numérique.

D'un point de vue bancaire, il importe que la conjugaison de ces deux phénomènes ne vienne pas éroder la confiance des clients et menacer la sécurité des échanges, car la confiance et la sécurité constituent l'actif numéro un des banques ! La protection des données des clients et de leurs fonds est un sujet sur lequel les banques n'accepteront jamais de transiger ! C'est pour cette raison que la réglementation, à laquelle sont soumises les banques dans le cadre de leurs activités, doit également s'appliquer aux nouveaux entrants *(GAFA et FinTech)*. Il en va de la sécurité du secteur financier et du client final ainsi que du respect des règles de concurrence.

Innovantes et sûres, les banques françaises sont à même de jouer un rôle majeur pour développer la filière du numérique dans le secteur financier en France et y soutenir un écosystème créatif avec les FinTech. Elles le font de multiples manières selon leur propre culture, leurs besoins, ceux de leurs clients.

Banques et FinTech évoluent ensemble, chacune ayant besoin l'une de l'autre pour se développer, appréhender les enjeux du numérique et apprécier convenablement les risques auxquels nous devons collectivement faire face.

2. Le nouvel écosystème issu de la DSP2

2.1. Une évolution de la relation entre les acteurs

La DSP2 vise à encadrer de nouveaux acteurs de paiements en sus de l'écosystème des établissements de paiements et des banques.

> ***Précision - FinTech :*** *combinaison des termes « finance » et « technologie », il s'agit d'une startup innovante qui utilise la technologie pour repenser et proposer des services financiers et bancaires à moindre coût pour le client final. Plusieurs catégories de FinTech existent : crowdfunding, monnaies virtuelles, applications mobiles, paiements électroniques, robot-conseillers, etc.*

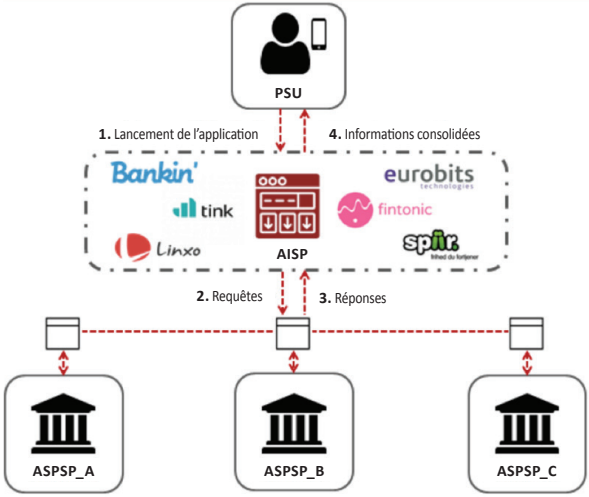
Le positionnement de chacun de ces acteurs et les fonctions qu'ils couvrent dans la chaîne de valeur des paiements sont présentés ci-dessous.

2.1.1 Le rôle des AISPs *(Account Information Service Providers)*

Les AISPs offrent à leurs clients *(PSU)* la possibilité d'agréger leurs différents comptes détenus dans plusieurs établissements *(ASPSP)*, au sein d'une même application offrant une vision consolidée de leurs données.

Le service d'agrégation prévu par la directive est le suivant : après avoir obtenu le consentement du client, l'agrégateur va se connecter aux différents ASPSPs détenant les informations du client *(PSU)*, au travers d'une interface dédiée.

FONCTIONNEMENT D'UN AISP PRÉVU PAR LA DSP2



Après avoir récupéré les données de compte auprès de chaque ASPSP, l'application analyse les données recueillies et les restitue avec une interface ergonomique présentant une situation agrégée des comptes.

Deux agrégateurs dominent actuellement le marché en France, **Linxo** et **Bankin'**. La première société créée en 2010 comptabilise actuellement 900 000 utilisateurs, et fait office d'outsider. La seconde, **Bankin',** est une FinTech parisienne qui comptabilise aujourd'hui 1,3 million d'utilisateurs au travers de quatre pays européens. Une autre startup s'est démarquée en France : **Fiduceo**. Elle a cependant été rachetée en 2015 par Boursorama, la banque en ligne de la Société Générale.

D'autres agrégateurs se sont également largement développés en Europe. Les principaux étant **Tink** en Suède, **Spiir** au Danemark ou encore **Fintonic** et **Eurobits** en Espagne, comptabilisant environ 350 000 utilisateurs chacun.

Afin de se démarquer, ces plateformes développent d'autres services à valeur ajoutée comme la gestion des finances personnelles *(analyses de dépenses)*, ou encore la gestion documentaire *(factures, notes de frais…)*. Le client est au cœur de la stratégie de ces nouveaux acteurs avec un objectif de faciliter leurs expériences utilisateurs au travers de services innovants et intuitifs.

ENCART 2 INTERVIEW

Joan Burkovic - *CEO de Bankin'*

Galitt : *pourriez-vous présenter Bankin' ?*

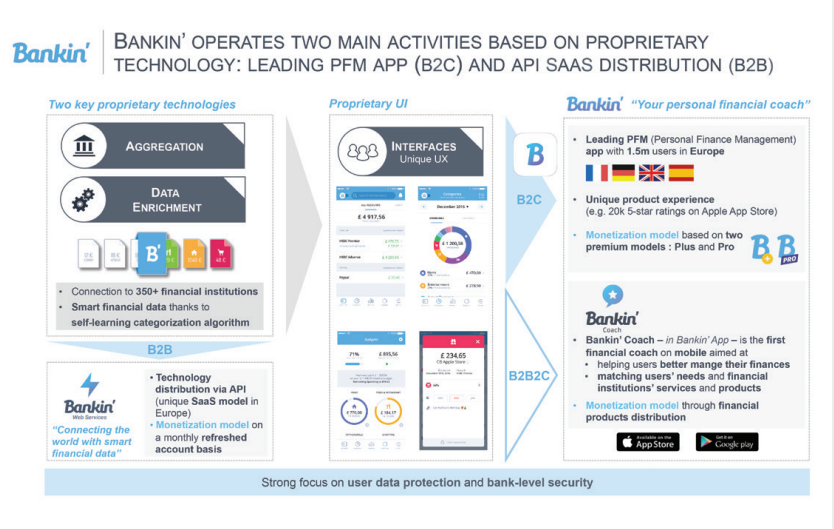
Joan Burkovic : Bankin' est une application qui agit comme un coach financier, personnel et intelligent pour aider nos utilisateurs à mieux gérer leurs finances au quotidien. Nous sommes aujourd'hui présents dans quatre pays en Europe : Angleterre, Allemagne, Espagne, France, et nous comptons plus de 1,5 millions d'utilisateurs.

La technologie d'agrégation a été développée par Bankin' afin de pouvoir connecter la ou les banques de nos utilisateurs avec notre service. L'agrégation est en effet nécessaire pour proposer nos services, mais ce n'est pas notre principale valeur ajoutée.

Notre business model est triple :

- **Le premier est un modèle B2C ou B2B2C.** Dans celui-ci, l'application Bankin' est un coach financier qui permet à nos clients de mieux gérer leurs finances et de recevoir des recommandations personnalisées. Ainsi, si nous constatons qu'un utilisateur a l'opportunité de renégocier un prêt, souscrire à une assurance vie, nous leurs soumettons l'idée et nous pouvons les mettre en relation avec des partenaires spécialisés, en toute indépendance. Nous sommes le seul acteur …

... à être totalement indépendant sur le marché Européen. L'indépendance est la clé pour être légitime auprès de nos utilisateurs. Nous travaillons avec une grande palette de partenaires *(assurances, banques, FinTech...)* pour proposer les solutions les plus pertinentes possibles à nos utilisateurs. Dans ce modèle, Bankin' est à la fois un coach financier et un apporteur/indicateur d'affaires.



- **Le second business model est celui proposé au travers de Bankin' Web Services.** Dans celui-ci nous sommes en B2B, et licencions notre API en mode SaaS. Nous proposons à nos clients *(banques, assurances, acteurs du crédit...)* de bénéficier de notre technologie d'agrégation et de traitement intelligent de la donnée financière. Notre API permet à nos partenaires de répondre à de multiples cas d'usages. Cette API permet de se connecter à 350 institutions financières en quelques clics. Nous proposons notre technologie en mode SaaS via une API Plug & Play très simple à intégrer.
- **Le troisième business model est celui de Bankin' Plus & Bankin' Pro.** Il permet à nos utilisateurs de coupler le coach financier avec des services et des fonctionnalités supplémentaires. Nous venons par exemple de développer un service d'agrégation de notes de frais, pour simplifier la vie de nos utilisateurs ayant des dépenses dans le cadre de leur travail.

Galitt : *comment percevez-vous la DSP2 pour votre business ?*

Joan Burkovic : la DSP2 est un grand souffle positif sur le marché, car elle crée un cadre légal pour notre activité. Cela permet de créer plus de confiance sur nos services. Cela facilite également la collaboration et accroit les possibilités ...

... d'innovation. De plus, cela nous permet de devenir à la fois agrégateurs et initiateurs de paiement, ce qui est intéressant pour nos utilisateurs.

Galitt : *quels seront les impacts en termes techniques ?*

Joan Burkovic : aujourd'hui nous utilisons la technique du « *web-scraping* » et nous participons à l'élaboration de futurs des standards techniques avec l'EBA et la Commission Européenne dans le cadre de la DSP2. Cette technique est un vrai avantage, car elle nous permet d'accéder aux mêmes informations que le client lui-même. Cette technique demande cependant un gros savoir-faire en termes de développement et de maintenance.

On entend beaucoup parler des APIs avec la DSP2. Nous avons déjà travaillé avec des partenaires bancaires au travers d'API. Cependant sans véritable standardisation et harmonisation les APIs peuvent s'avérer contraignantes : Sont-elles fiables ? Tiennent-elles la charge ? Fournissent-elles les mêmes données ? L'idée d'une API universelle est intéressante et on y arrivera en France et en Europe, mais j'en doute à court terme. Bankin' collabore avec les régulateurs Français et Européens pour le développement d'une standardisation. Si rien n'est fait, nous continuerons à utiliser la technique du « *web-scraping* ».

Concernant la sécurité, notre application est auditée très régulièrement par des acteurs spécialisés en sécurité informatique. De plus dans la mesure où nous travaillons avec des banques qui utilisent notre API en mode SaaS, nous sommes régulièrement audités par des acteurs bancaires. Le vrai risque aujourd'hui pour les banques est l'arrivée des GAFA. Ils disposent d'une réelle force financière qui leur permet d'innover à leur guise. Pour les FinTech, les GAFA peuvent être des opportunités ou des menaces. Pour les banques, il s'agit juste d'une menace. Sans innovation de leur part, elles ont beaucoup à craindre. L'enjeu fondamental est de toujours innover pour servir les utilisateurs.

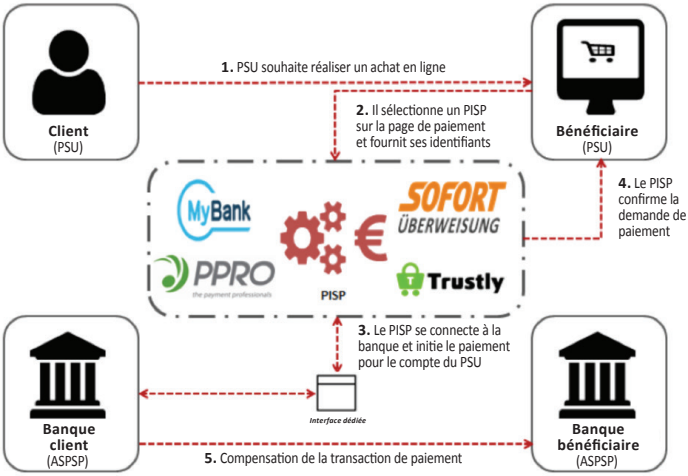
2.1.2 Le rôle des PISPs *(Payment Initiation Service Providers)*

Les initiateurs de transaction de paiement interviennent sur le marché du e-commerce. Ces acteurs proposent d'initier des paiements directement depuis le compte des consommateurs *(PSU)*. Ainsi, un e-commerçant peut élargir sa palette de paiement en intégrant ces tiers au côté des réseaux de paiement : **CB** / **Visa** / **MasterCard** / **American Express** ou encore **PayPal**. Au moment du règlement, les clients *(PSU)* pourront alors choisir d'utiliser un PISP pour payer. L'offre se veut simple, sans obligation d'inscription en amont de la transaction. Le client PSU devra simplement autoriser le PISP à accéder à son compte en renseignant ses identifiants de connexion de banque en ligne. Ce procédé permettra l'exécution d'un paiement par virement ou prélèvement au bénéfice de l'e-commerçant.

Les offres des PISPs s'orientent majoritairement vers les pays ou l'usage de la carte bancaire est moins répandu. Les PISPs ont ainsi une position bien établie dans le nord de l'Europe, notamment en Allemagne avec **Sofort** *(une entreprise du groupe suédois **Klarna**)*, ou encore en Suède avec **Trustly**. De la même manière que les agrégateurs, ces applications peuvent se coupler à d'autres fonctionnalités pour proposer des services plus élaborés.

Trustly offre ainsi à ses clients une vision sur le solde de leurs différents comptes disponibles (épargne ou compte courant) et leur permet de choisir lequel sera utilisé pour le paiement. Son offre supporte aujourd'hui l'ensemble des banques suédoises, danoises, finlandaises et espagnoles. **Trustly** élargit actuellement son réseau autour des plateformes de jeux, des marketplaces et également des services de transfert d'argent.

FONCTIONNEMENT D'UN PISP PRÉVU PAR LA DSP2
(PAIEMENT RÉALISÉ PAR VIREMENT)



Au travers de la création de la société **Sofort** en Allemagne en 2005 et du retentissement que le nouveau service de virement en ligne proposé a suscité, le marché des paiements en Europe s'est retrouvé dans une situation inédite jusqu'à présent.

En Allemagne tout d'abord, les banques se retrouvant dans l'incapacité d'empêcher **Sofort** de se connecter à leurs interfaces, ont décidé de consulter le législateur afin de contester la légitimité d'une telle ouverture aux interfaces et l'accès possible aux comptes bancaires de leurs clients.

Au niveau européen, dans le cadre de la construction du Single European Payment Area *(SEPA)*, ce nouvel acteur a été perçu par le législateur, notamment la Commission européenne, comme un acteur innovant capable de développer de nouveaux services de paiement peu coûteux et efficaces. Dans son projet de DSP2, ...

... la Commission européenne a, en conséquence, décidé de favoriser ce type de nouveaux services, en proposant le cadre réglementaire adapté à sa mise en œuvre, prévoyant notamment que les échanges de données entre les PSP Tiers et les ASPSPs devront se faire au travers de nouveaux standards et protocoles de communication.

Ces PSP Tiers opérant déjà, comme l'indiquent des initiatives de type **Sofort**, nous présentons ci-après leur mode opératoire actuel, appelé « *web-scraping* », ainsi que leur mode opératoire futur : les Open-API, dans la droite ligne de la DSP2.

2.2. De la technique du « *web-scraping* »...

Actuellement la plupart des AISPs et certains PISPs utilisent la technique dite du « web scrapping » pour fonctionner.

Cette technique de « *web-scraping* », est une technique d'extraction du contenu de sites Web, via un script ou un programme qui va lire le code html, dans le but de le transformer pour permettre son utilisation dans un autre contexte. Cette technique est celle utilisée, par exemple, par les sites de comparateurs de prix *(trivago.fr, liligo.com...)*.

Dans le cas présent, un PSP Tiers, va demander à son client *(PSU)* ses identifiants de connexions à son ASPSP *(ex : banque en ligne)*. Il va ensuite les intégrer dans un programme qui va agir comme un robot, simulant l'action de connexion à la place du client. Il va ensuite récupérer au sein de cette page l'ensemble des informations nécessaires à son fonctionnement.

2.2.1 Cette technique du « *web-scraping* » pose toutefois plusieurs problèmes

- **Pour les ASPSPs :** avoir un robot qui passe continuellement sur sa page internet peut ralentir son fonctionnement. En cas de nombreuses connexions en simultanée, ce mode opératoire peut provoquer ce que l'on appelle une attaque par déni de services *(un trop grand nombre de requêtes que le serveur ne peut prendre en charge conduisant alors à son arrêt)*.
- **Pour les PSPs tiers :** ce mode nécessite de configurer autant de robots qu'il y a d'ASPSP, dans la mesure où les sites ne sont pas standards, ce qui engendre alors un temps de programmation important et peut être rendu obsolète si l'ASPSP décide de modifier sa page.
- **Pour le PSU :** en en donnant son consentement à un PSP Tiers, le PSU donne accès à la totalité des informations contenues dans sa banque en ligne. Bien que les nouveaux services proposés soient légitimes et que les PSPs garantissent la confidentialité des données, ils sont aujourd'hui dans la capacité de récupérer l'ensemble des informations détenues sur les comptes des clients : soldes, virements, prélèvements, et toutes les métadonnées liées *(lieu, date, heure, ...*

... commerce, montant, montant du loyer, remboursements, emprunts, opérateur téléphonique, assurances, salaire, remboursements médicaux, habitudes de consommation, etc.).

- **Pour les trois acteurs réunis :** le problème majeur de la technique du « *web-scraping* » réside dans le partage de responsabilité et le principe de la preuve. Prenons le cas d'une fraude par exemple, ou un virement a été initié depuis le compte d'un PSU à son insu. Dans la mesure où il a donné ses identifiants de banque en ligne et son consentement à un PSP Tiers, il peut être difficile de déterminer la chaîne de responsabilité : lui-même, le PSP Tiers ou l'ASPSP ?

ENCART 3

Le régime de responsabilité de la DSP2

L'une des pierres d'achoppement de la DSP2 concerne le régime de responsabilité institué entre les acteurs de la chaine de paiement.

Les articles 73 et 90 ont en effet instauré un régime de responsabilité des prestataires de paiements gestionnaires de comptes *(« ASPSP »)* envers les utilisateurs en cas d'opérations de paiements non autorisées, non exécutées ou mal exécutées, alors même que l'opération de paiement a été initiée par l'intermédiaire d'un prestataire de services d'initiation de paiement *(« PISP »)*. Les banques dénoncent ce régime de « responsabilité de plein droit » comme étant exorbitant de droit commun. La DSP2 a toutefois prévu un certain nombre de garanties :

1. une présomption de responsabilité du PISP,
2. un droit de remboursement à première demande de l'ASPSP contre le PISP,
3. le droit pour l'ASPSP de vérifier en amont que le PISP satisfait bien les conditions posées par la DSP2,
4. et le transfert de l'obligation de remboursement de l'utilisateur au PISP qui ne respecte pas les conditions posées par la DSP2.

Cependant, la directive n'impose pas la contractualisation entre parties : un PISP peut exiger l'accès au compte même s'il n'a pas contractualisé avec l'ASPSP. Ce point est sévèrement critiqué, au motif qu'il conviendrait de garantir le droit des ASPSPs de contractualiser leurs relations avec ces tiers, sous la surveillance des autorités bancaires de contrôle prudentiel telles que l'ACPR.

A défaut, le régime de responsabilité instauré par les articles 73 et 90 de la DSP2 pourrait être en contrariété avec le droit primaire européen, et en particulier au droit fondamental à la propriété et à la liberté d'entreprise des ASPSPs, ainsi que le droit à la vie privée des utilisateurs, tels que consacrés par les articles 16, 17 et 7 de la Charte européenne des droits fondamentaux.

2.2.2 La sécurité des données au cœur des préoccupations actuelles

Lorsque l'on parle de transmettre des informations bancaires, la question de la sécurité s'impose de fait. La protection de la confidentialité et de l'intégrité des données sont au cœur des préoccupations des banques aujourd'hui. L'European Banking Authority *(EBA)* a ainsi été chargée par la Commission européenne de mettre en place des mesures spécifiques afin de limiter les risques en matière de sécurité.[3]

La démarche a été initiée en décembre 2015, au travers des « Consultations Papers » *(à destination de l'ensemble des parties prenantes)* sur l'authentification forte et la sécurisation des communications. Ces travaux de consultation se sont terminés en février 2016 avec l'élaboration de documents sur les *Regulatory Technical Standards (RTS)*. Ces derniers ont à nouveau été soumis à l'ensemble des parties prenantes au travers des « Discussions Papers », émis par l'EBA en août 2016, pour recueil de commentaires en octobre 2016. Actuellement, tous les éléments sont à disposition de l'EBA qui va devoir compiler l'ensemble des remarques et valider ses conclusions en remettant à la Commission européenne des propositions de standards techniques. *(Cf. Dates clés de la DSP2)*.

2.2.3 Les principales conclusions des travaux de l'EBA sur les RTS

1. Procédure d'agrément d'établissement de paiement spécifique :

la première mesure concerne l'obligation pour tous les AISPs et les PISPs d'obtenir un agrément d'établissement de paiement auprès des autorités nationales afin d'étudier la fiabilité des services proposés notamment. Cette procédure d'agrément sera complète pour les PISPs et allégée pour les AISPs. En France, l'entité en charge de délivrer ces agréments reste l'Autorité de contrôle prudentiel et de résolution *(ACPR)*.

2. Utilisation de certificats conforme au règlement eIDAS[4] par les ASPSPs et TPPs :

le règlement eIDAS *(electronic IDentification And trust Services)* est entré en vigueur le 1er juillet 2016. Son objectif est « *d'instaurer un climat de confiance dans l'environnement en ligne* » en fournissant un cadre européen intersectoriel complet pour des transactions électroniques sécurisées, fiables et simplifiées entre citoyens et entreprises. L'EBA souhaite recourir à l'utilisation de certificats conformes à l'eIDAS pour authentifier les ASPSPs, les AISPs et les PISPs. Cependant, il n'est pas sûr qu'en janvier 2018, date de la transposition prévue dans les États-Membres, les autorités nationales soient à même de fournir ces certifications dans les délais impartis, en raison de la construction en cours de l'infrastructure de certification.

*3 - **EBA** : Consultation Paper & Discussion Paper 11.2016*
*4 - **ANSSI** : Le règlement EIDAS*

3. Recours à l'authentification forte :

afin de limiter les risques de fraude, et conformément à la DSP2, l'EBA a imposé au travers des Standards Techniques *(RTS)* le recours à l'authentification forte afin que les Tiers puissent identifier les clients. Ainsi, pour chaque consultation ou opération de paiement, le PSU devra s'identifier de manière forte afin que l'on soit sûr dans un premier temps de son consentement et de son intention de réaliser l'action qu'il a entreprise. En matière de sécurité des systèmes d'information, on parle d'authentification à deux facteurs ou authentification forte pour désigner une procédure d'authentification qui requiert au minimum deux facteurs pouvant faire partie des éléments suivants :

- Ce que l'on connait : un code secret *(ex. : code PIN)*
- Ce que l'on est : biométrie *(ex. : empreintes digitales)*
- Ce que l'on possède : un jeton d'authentification ou Token

La procédure d'authentification demeurera entièrement du domaine de compétences de l'ASPSP gestionnaire de comptes, mais pourra se faire au travers du PISP en cas d'accord contractuel. Il appartient donc à la banque *(ASPSP)* de définir les procédures de sécurité à appliquer lorsqu'un tiers initie un paiement.

4. Les exemptions de recours à l'authentification forte :

L'agrégation sera exemptée d'authentification forte :

- S'il ne s'agit pas d'une première connexion à leur service, et que cette connexion est réalisée dans un délai d'un mois après la dernière connexion authentifiée
- Si le service de consultation est limité à des informations qualifiées de non sensibles *(Le nom et le numéro de compte)*

L'initiation de paiement sera exemptée d'authentification forte pour les transactions :

- En paiement sans contact de moins de 50 euros, sans que le montant cumulé excède 150 euros
- En paiement électronique à distance pour des montants de moins de 10 euros, sans que le montant cumulé excède 100 euros

5. Les nouveaux standards et protocoles de communication entre les acteurs :

Conformément aux articles 97*(5)*, 66*(3)*b et 67*(2)*b de la DSP2, les ASPSPs devront mettre à disposition des AISPs et PISPs une interface de communication sécurisée afin de partager les informations de leurs clients. L'EBA laisse ouvert aux acteurs le champ des implémentations techniques en posant les conditions suivantes :

- Avoir les mêmes fonctionnalités et disponibilités que les interfaces de banque en ligne

- Garantir les échanges de données sécurisées, au travers de standards de communication ouverts et universels, imposant le recours à l'utilisation des éléments de la norme ISO 20022 qui régit les échanges de données informatisées dans le domaine financier [5]
- Ecarter la seule utilisation des standards génériques d'Internet comme HTTP, HTTPS, TLS et SSL qui n'offrent pas les garanties de sécurité nécessaires aux échanges de données financières [6]

Cet accès inquiète le secteur bancaire car celui-ci y voit un risque systémique pour le système financier. L'utilisation des données de sécurité personnalisées *(données d'authentification ou credentials)* par les PISPs et AISPs s'apparenterait en effet à la « transmission des clés d'un coffre à un inconnu », quand bien même l'accès au coffre serait limité dans le temps et pour une seule opération, et s'effectuerait « au moyen de canaux sûrs et efficaces ». D'un point de vue pratique, il eût été possible de permettre le développement des services d'initiation de paiement et d'information sur les comptes sans pour autant confier « les clés » aux nouveaux acteurs qui en ont la charge, alors que ces derniers bénéficient de règles d'agrément et de contrôle prudentiel assouplies *(exigence en fonds propres très limitée)* et sont particulièrement exposés aux risques systémiques de cyber-attaques.

Il aurait été techniquement possible pour les PISPs et les AISPs d'avoir respectivement accès au compte de paiement et aux données du compte de paiement, sans connaître ni utiliser les données d'identification, en créant une API, comme nous le verrons ci-après.

En cas de refus de la banque de donner accès au compte de paiement ou aux données du compte de paiement autrement que par le recours à une API, qui n'est pas fondé sur des raisons objectivement motivées et documentées liées à un accès non autorisé ou frauduleux, le législateur devrait prévoir un droit de recours devant l'ACPR au motif que « l'impératif de préserver la sécurité des données de sécurité personnalisées ne doit cependant pas empêcher ou compliquer le recours à des AISPs ou PISPs ». Une telle analyse est, à notre sens, conforme au principe du privacy by design consacré par le nouveau règlement européen sur les données personnelles : donner accès à l'information nécessaire aux services d'initiation de paiement et d'informations sur les comptes serait moins dangereux pour la protection des données personnelles que donner un accès pur et simple au compte bancaire, tout en permettant la fourniture de ces nouveaux services.

2.3. ...Au déploiement d'Interfaces de programmation *(API)*

La notion d'API a déjà largement fait son apparition avant même la mise en œuvre de la DSP2. Même si le texte de la directive ne mentionne pas la notion d'API en tant que telle et que l'EBA se contente de lister des exigences techniques, les APIs apparaissent comme la solution la plus adéquate pour prendre en compte l'ensemble des exigences mentionnées précédemment.

*5 - **ISO 20022** : Universal financial industry message scheme*
*6 - **Consultation Paper EBA** : 06.2016*

ENCART 4 INTERVIEW

Sébastien Taveau - *Chief Developer chez Early Warning*

Afin d'apporter un éclairage sur les notions d'API et d'Open API, nous avons fait appel à Sébastien Taveau, Technologist chez Early Warning

Galitt : *pourriez-vous définir ce que le terme « API » signifie selon vous ?*

Sébastien TAVEAU : une API est un moyen structuré pour exposer des services ou des données à des tierces parties via une passerelle contrôlée et sécurisée. Dans l'absolu, il s'agit ni plus ni moins que d'une logique de questions-réponses.

Ainsi dans le cas d'un agrégateur de données *(AISP)*, il enverra depuis son application une requête demandant de récupérer des données définies. Cette requête va transiter via une passerelle, l'API, qui va interroger le service en question au sein de l'ASPSP afin de récupérer les données. Les données transiteront en retour par cette passerelle vers l'application de l'AISP, qui les compilera *(Cf. Schéma p.16)*.

ILLUSTRATION D'UNE API

Developper <-> Apps Request <-> Data Gateway <-> API Services <-> Data <-> Data

Galitt : *qu'entend- on par Open API ?*

Sébastien TAVEAU : il existe plusieurs types d'API, dont les principales sont :

- **API Privées :** il s'agit d'une intégration 1:1. Dans ce cas, l'API a été conçue pour un partenaire spécifique et ne sera utilisable que par celui-ci. Les APIs privées sont très généralement utilisées pour le partage de données sensibles présentant des risques pour les parties *(listes noires, données personnelles…)*.
- **API Publiques :** ce sont les APIs les plus largement répandues, ne présentant pas de sensibilité particulière. Nous pouvons mentionner le cas de l'API de Google Maps ou celle des fils d'actualité de Twitter par exemple. Une inscription est encouragée, pas nécessaire.
- **API Ouvertes ou** *(Open API)* **:** Ce sont des APIs conçues pour un public plus large que celui des APIs privées. Elles exigent de la part du PSP Tiers d'accepter les termes et conditions d'utilisation et nécessitent un processus de garantie et de sécurité via un enrôlement d'authentification « Oauth ». L'inscription est nécessaire pour utiliser ce service. Dans le cadre fourni par la DSP2, les Open API sont celles qui correspondent le mieux aux attentes concernant le recours à des interfaces dédiées, car elles permettent à l'ASPSP de contrôler les utilisateurs qui se connecteront afin de venir récupérer des données.

Un autre élément important à noter est que certaines API sont génératrices de revenus tandis que d'autres n'apportent pas de forte valeur ajoutée (utilisées pour la diffusion de contenu media gratuit ou comme service d'accroche, mais sans perspective économique sur ces API). Par exemple, les APIs publiques ne sont pas orientées pour générer du profit, mais il est important de mentionner que le coût de maintien et l'ajout de données, pour tout type d'API, ont un impact financier non négligeable. Le business model réside alors dans l'utilisation des APIs à grande échelle ainsi que dans la pollinisation croisée avec d'autres API, ou au travers de services payants sous-jacents à l'utilisation d'une API. Il est envisageable de regrouper plusieurs fonctionnalités en fonction de la capacité de mappage des APIs.

Galitt : *quels sont les avantages liés à l'Open API ?*

Sébastien TAVEAU : les APIs et plus particulièrement les Open APIs offrent une grande flexibilité car elles permettent de maintenir une couche de sécurité tout en forçant l'administrateur à penser aux usages qui pourront être faits par les tierces parties. Je compare souvent une API ouverte à un objet dans une boite en verre trempé : on peut voir l'objet, on peut secouer cette boite, mais on ne peut pas le toucher.

Une API comme nous avons pu le voir est un ensemble d'appels prédéfinis accédant à un service via une passerelle. Cette dernière apparait comme le point critique en termes de sécurité dans la mesure où le PSP tiers, au travers de l'API, va directement interroger le SI des ASPSPs. Il est techniquement facile de construire dans le mécanisme un moyen de verrouiller la communication si un problème est détecté. De plus, avec l'Open API, l'authentification OAuth est obligatoire, ce qui limite encore davantage le risque. OAuth n'est pas un protocole d'authentification, mais un protocole de délégation d'autorisation, ainsi il permet d'autoriser une application à utiliser une API sécurisée pour le compte d'un utilisateur. Il s'agira donc d'une couche de sécurité supplémentaire en plus de celle représentée par l'authentification forte. Encore une fois, l'analogie de l'objet dans du verre trempé est très parlante. De plus la réponse fournie par l'API est la seule chose que le TPP peut collecter ce qui est primordial.

Pour résumer cette partie, on constate que de la directive va entièrement bouleverser les relations entre les acteurs tant en matière juridique que technique.

L'impact majeur de ces innovations concerne aujourd'hui la banque à proprement parler. Dans la partie suivante sont analysées les différentes possibilités qui s'offrent aujourd'hui et les initiatives observables.

3. Un tournant stratégique pour l'écosystème bancaire

3.1. Trois business models envisageables

L'enjeu principal aujourd'hui pour les banques consiste à appréhender le positionnement adéquat à ces innovations.

Selon une étude de **Finextra** parut en 2015, 88% des banques européennes sont toujours préoccupées par les risques de sécurité[7]. Elles sont également indécises sur le format des interfaces de communication et les protocoles de sécurité à mettre en place. Un risque majeur pour la banque est de voir l'usage des cartes bancaires réduit au profit des services des PISPs. Elles doivent donc dès à présent envisager les évolutions de leurs business models leur permettant de conserver leurs relations clients et leur profitabilité sur les services de paiement.

Les banques semblent conscientes de la nécessité de réagir sur ces sujets. Selon cette même étude de Finextra, 54% des banques européennes se disent être actuellement en train de repenser leur modèle de relation client et les business models associés.

3.1.1 | Trois types de business models se distinguent

Modèle Interne :

Le modèle interne consiste pour la banque à s'appuyer sur ses ressources internes *(départements stratégie et R&D)* afin d'innover. L'avantage défendu par ce business model est de pouvoir garder le contrôle sur l'ensemble des canaux d'interaction avec le client dont la banque dispose *(applications, TPE, cartes...)*. L'inconvénient est que, pour fonctionner, la banque devra mobiliser de nombreuses ressources humaines, techniques et financières afin d'anticiper au mieux ce marché très concurrentiel et proposer des services innovants.

Modèle Mixte :

Dans ce modèle, la banque s'appuie directement sur l'écosystème des FinTech ou des PSPs Tiers. L'objectif est de capitaliser sur la connaissance et les capacités techniques de ces nouveaux acteurs pour proposer rapidement des services susceptibles d'intéresser les clients. L'enjeu pour la banque est de prendre le contrôle de ces innovations au travers d'opérations d'acquisition ou de créations de joint-venture. Les FinTech apparaissent dans ce modèle comme un laboratoire de R&D extérieur que la banque pourra absorber. Cela permettra ainsi à la banque de limiter ses efforts en interne, et de réagir de manière rapide.

Modèle de Rupture :

Le modèle en rupture actionne le mode opératoire de l'Open-Banking. La banque ...

*7 - **Finextra**: PSD2 and XS2A - Regulation or Opportunity?*

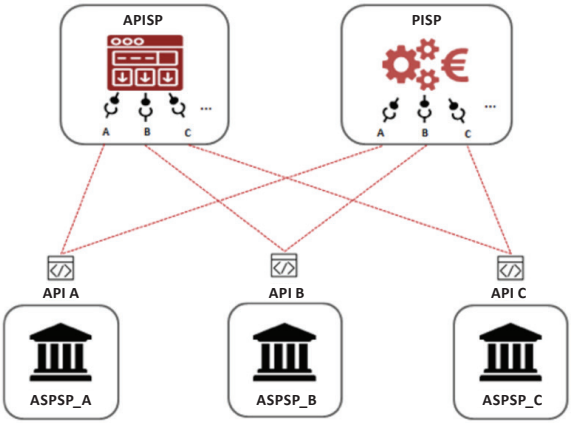
... donne accès à son back-office au travers des Open APIs au profit d'autres acteurs. La banque accentue de façon prioritaire son rôle de coffre-fort de données et offre à ses clients une gamme complète de solutions au travers d'applications tierces. Un problème majeur se pose toutefois avec ce modèle, celui de la standardisation *(cf. Schéma ci-dessous)*. En l'absence de standards et de volonté forte de la part des gouvernements, ce modèle apparait encore incertain les incidences en termes techniques étant trop importantes. Enfin, le risque majeur est le risque de disruption entrainant une domination de ces nouveaux services par des acteurs tiers.

3.1.2 La standardisation des APIs, indispensable pour un modèle en rupture

La standardisation est un élément fondamental du déploiement d'un modèle en rupture. Pour fonctionner, les PSP Tiers doivent se connecter au travers d'une interface sécurisée, dans l'absolu des APIs, fournies par les ASPSPs, afin de récupérer les informations nécessaires.

Le schéma ci-dessous illustre la mise en place d'API par les APSPs pour le compte des PSP Tiers.

UNE API PAR ASPSP



Ce schéma montre que pour se connecter à une banque A, les PSPs Tiers *(AISPs ou PISPs)*, doivent identifier le moyen technique de permettre à leurs applications de se connecter à l'API de l'ASPS_A et d'interpréter les données fournies. Cette opération de développement est à répéter pour chaque d'ASPSPs. Les PSPs Tiers doivent donc être en capacité de gérer de nouvelles complexités techniques relatives à la variété des programmations d'API et à celle des données hiérarchisées.

Ce constat fut celui de l'**Open Bank Project** [8], créé en 2012 par l'entreprise allemande **Tesobe** afin d'initier des travaux sur la création d'une API universelle pour le monde bancaire.

OPENBANKPROJECT

8 - ***OpenBankProject***

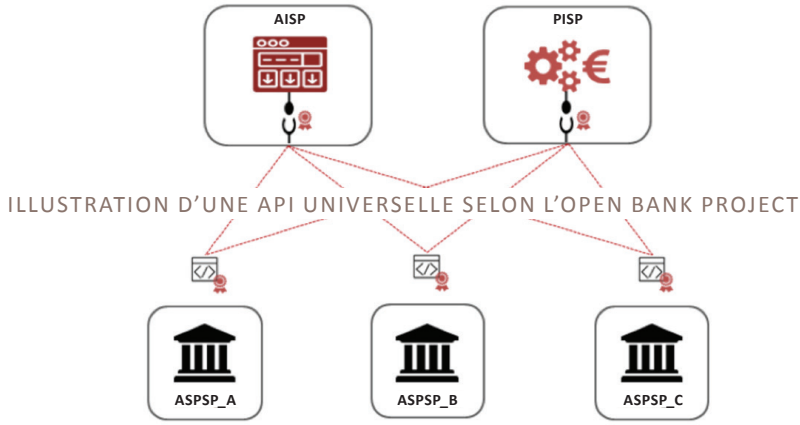
Objectif : créer un projet Open Source d'API pour les banques afin de faire fonctionner de manière intelligente l'ensemble de l'écosystème et entrer dans l'ère de l'Open-Banking. Les principes de standardisation et d'universalité en sont les éléments fondateurs.

Pour ce faire, l'Open Bank Project, Think tank de l'Open API, a réalisé une vaste enquête auprès de l'écosystème bancaire afin de connaitre les attentes de chacun en la matière. Le projet Open Source réuni à ce jour plus de 5 000 développeurs, avec pour objectifs majeurs de fournir un catalogue d'API, un environnement de tests sécurisé et une communauté d'experts à disposition de ceux qui le souhaitent.

« Nous apportons un standard, un modèle de données, une plate-forme déployable en interne dans les banques, et un accès à une communauté mondiale de développeurs et de FinTech. C'est un moyen de transition d'une architecture rigide et fermée vers les standards du web, beaucoup plus simple à utiliser et accessible à un grand nombre de développeurs. Car en donnant à d'autres le moyen de bâtir des services à partir des leurs, les banques se mettent en position de devenir des plates-formes distribuant toutes sortes d'applications via leur propre « appstore ».

Ismail Chaib, directeur opérationnel de Tesobe / Open Bank Project[9]

Le projet défendu par l'Open Bank Project est détaillé dans le schéma suivant :



Dans ce schéma les PSP Tiers et les ASPSPs utilisent les mêmes standards de communication. Ainsi chaque API est identique, une seule programmation est désormais nécessaire. La standardisation facilite la relation entre les acteurs. Allant plus loin dans la démarche, la volonté au travers de ce projet est d'ouvrir la voie de l'Open-Banking. La banque devient une plateforme modulaire où les acteurs interagissent au travers d'API.

Ce principe de « bank-as-a-platform » est présenté au travers du cas d'usage de **SolarisBank** détaillé ci-contre.

*9 - **AGEFI** : Les API portent l'innovation dans les banques LIEN*

ENCART 5

SolarisBank, la banque de demain ?

SolarisBank a été créée en 2015 par le groupe Financier allemand **FinLeap**. Elle se veut la première banque 100% digitale et a obtenu sa licence bancaire auprès du régulateur financier allemand BAfin, pour pouvoir fonctionner en accord avec la réglementation existante.

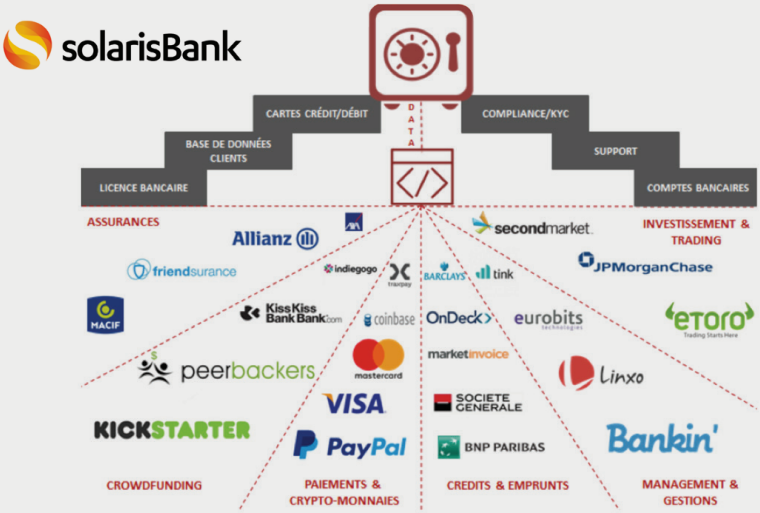
Axant sa stratégie vers les jeunes entreprises, **SolarisBank** opère avec un business model B2B2C qui est typiquement celui de l'Open-Banking. Sa volonté est de proposer une plateforme en marque blanche au travers de laquelle les services bancaires sont fournis à la carte par les FinTech qui souhaitent collaborer. Le client peut alors interagir directement afin de créer son environnement bancaire avec les applications qui l'intéressent.

La banque agit ainsi comme une boite à outils modulaires au travers de son API.

« Nos services sont comme des briques Lego : nos partenaires peuvent choisir les briques dont ils ont besoin et assembler des solutions personnalisées pour répondre à leurs propres attentes. Les partenaires peuvent accéder aux services de Solaris Platform via notre API. L'intégration est simple et permet aux utilisateurs de se concentrer sur leurs métiers. De plus, nos services sont sécurisés et garantissent la confidentialité des données de nos utilisateurs. » ...

Andreas Bittner, Managing Director SolarisBank [10]

ILLUSTRATION DE L'OPENBANKING



10 - ***SolarisBank*** : *Présentation*

... De plus, **SolarisBank** agit de manière modulaire au travers de plusieurs API. Il y a une notion d'interopérabilité entre les différents acteurs qui la composent. En résumé, il est possible d'utiliser cette plateforme en marque blanche pour créer sa propre banque. **SolarisBank** conserve les fonctions clés de la banque telles que la base de données clients, l'émission de cartes, la gestion des comptes bancaires, la conformité, la gestion des risques etc. Elle fait cependant intervenir différents acteurs pour implémenter chacune de ces briques.

Dans le modèle de banque plateforme, les banques se placent au centre d'une nouvelle économie dans laquelle les APIs sont sources de revenus et permettent d'adresser plus efficacement les besoins hétérogènes des clients.

SolarisBank n'est pas la première à proposer ce genre de modèle. La pionnière dans le domaine est **Fidor Bank**, récemment rachetée par le groupe BPCE.

3.2. Le modèle britannique : une transposition anticipée de la directive ?

Le Royaume-Uni constitue un pays clef et stratégique pour le secteur car le gouvernement britannique a clairement pris position en faveur des APIs, de la standardisation et plus généralement de l'Open-Banking.

En 2015, le gouvernement britannique, au travers de l'autorité de la concurrence *(Competition and Markets Authority, CMA)*, a lancé des travaux sur le marché de la banque de détail[11]. Les résultats ont ainsi démontré que les banques traditionnelles avaient de grandes difficultés à innover et que les FinTechs étaient freinées dans leurs efforts d'innovation par le manque d'accès aux informations bancaires des clients. De plus, cette enquête a démontré que les clients principalement les petites et moyennes entreprises *(PME)* étaient désireuses d'accéder aux informations détenues par leurs banques, afin de faciliter leur quotidien, notamment dans le domaine des émissions de factures. Elles étaient intéressées par l'ouverture de leurs données à des tiers afin d'obtenir plus simplement et rapidement des conseils sur leurs placements et investissements, mais également de pourvoir réaliser plus simplement des transactions bancaires vers leurs clients. Anticipant la DSP2, les autorités britanniques ont décidé d'aller plus loin dans la démarche.

Ainsi en septembre 2016, le Département du Trésor a décidé de créer l'*Open Banking Working Group*[12]. Ce groupe de travail regroupant des banques, des entreprises du secteur, des associations de consommateurs, des instituts de recherche et surtout l'Open Bank Project, a eu pour feuille de route de faire du territoire national le pionnier de l'Open-Banking.

*11 - **CMA** : Retail banking market investigation*
*12 - **Open Banking Working Group***

Il a ainsi axé ses travaux sur le thème de l'*Open Banking Standard* [13], afin de déterminer la structure à donner à ces APIs, leur développement et leur maintenance mais également sur les standards des données à transmettre. L'*Open Banking Working Group* a également prévu de nommer un organe directeur, une entité référente en charge de sa mise en œuvre.

Enfin, il a été décidé que les banques britanniques devraient adopter une norme numérique commune avant le 13 janvier 2018, date finale de transposition de la DSP2 dans l'ensemble de l'Union Européenne. Ainsi, les autorités britanniques ont décidé que la norme numérique à utiliser sera celle de l'API. A l'heure actuelle, le projet suit son cours et semble fonctionner de manière constructive entre tous les acteurs.

La position défendue par le législateur britannique est importante, car elle pourrait orienter le marché européen. Ce pays référence en matière de FinTechs et actuelle place financière mondiale souhaite conserver sa place de leader. Il a anticipé les bénéfices que cela pourrait lui procurer, pouvant ainsi devenir une référence en la matière en cas de succès.

« Le Royaume-Uni a le potentiel d'être un leader mondial dans le traitement des données pour aider à la concurrence et stimuler l'innovation dans le secteur bancaire, ce qui donnera plus de choix aux clients pour les aider à économiser de l'argent. »

Anthony Browne Président de la British Bankers Association (BBA) [14]

L'incertitude autour de cette initiative porte sur le niveau d'harmonisation relatif à toutes les interfaces avec pour risque potentiel de devoir dupliquer en parallèle de nouvelles infrastructures. Aujourd'hui, le gouvernement britannique affirme ne pas travailler en silo, mais bien en partenariat avec le législateur européen afin d'éviter ce risque.

Deux questions se posent : Le Royaume-Uni anticiperait-il la transposition de la directive en testant le développement d'un standard autour des APIs ? Ou au contraire, le récent évènement autour du Brexit traduit-il la volonté accrue du gouvernement de se démarquer de l'Europe en étant proactif sur la règlementation et les standards ?

3.3. Des initiatives identifiées en France

En France différentes initiatives ont été prises par les banques sur ce sujet. Comme nous l'avons déjà présenté dans l'encart 2 sur **SolarisBank**, le groupe **BPCE** a annoncé en juillet 2016 le rachat de **Fidor Bank** [15]. Cette action s'inscrit dans le plan stratégique du groupe « Grandir Autrement ». L'objectif est annoncé : renforcer et accentuer la transformation digitale de la banque.

13 - ***Open banking Standard***
14 - ***Finextra*** *: UK sets out open banking API framework*
15 - ***Groupe BPCE*** *: communiqué de presse sur l'acquisition de Fidor Bank*

Fidor Bank créée en 2009 à Munich est la première néo-banque entièrement digitale. Comme **SolarisBank,** elle s'inscrit sur le modèle en rupture où l'Open-Banking est mis en avant. Pour **Fidor Bank**, l'entrée d'un actionnaire important à son capital lui offre les moyens de poursuivre et d'accélérer sa stratégie offensive, résolument tournée vers l'innovation et le client. En effet, cette entité est orientée vers les particuliers, à l'inverse de **SolarisBank** qui se concentre principalement sur les professionnels. **Fidor Bank** s'appuie sur une communauté composée de 350 000 membres, dont 125 000 sont clients, encouragés à participer à la stratégie de la banque en contribuant à la définition de services supplémentaires ou à des changements sur l'offre existante. La communauté, à la façon d'un réseau social, partage ses conseils, y compris lorsqu'ils portent sur les produits de banques concurrentes. Les membres actifs sont d'ailleurs financièrement récompensés.

Concernant l'analyse des *business models*, le groupe **BPCE** fait office d'exception en diversifiant sa stratégie, dans la mesure où il a opté pour un modèle mixte consistant à racheter une startup, qui a, quant à elle, un modèle basé sur la rupture et sur l'Open-Banking.

Le modèle mixte est le modèle qui semble aujourd'hui le plus suivi par les banques françaises.

Ainsi **HSBC France**, a développé un partenariat avec **Linxo** en octobre 2016, afin d'offrir à ses clients la technologie et le service de cet agrégateur en marque blanche [16], leur offrant ainsi la possibilité de les aider à mieux gérer leurs finances personnelles.

Le groupe **Société Générale** au travers de sa banque de détail, **Crédit du Nord** a lancé son agrégateur de services baptisé « Synthèse multi-banque », en s'appuyant sur la technologie développée par Fiduceo. L'objectif annoncé est de proposer à ses clients un système d'agrégation de leurs comptes en vue d'élargir par la suite l'offre autour de l'émission de factures. La Société Générale a annoncé également travailler aujourd'hui sur son application d'agrégation de comptes qui utilisera la technologie de **Fiduceo**. [17]

Le **Crédit Agricole** a depuis de nombreuses années entrepris de développer son API afin de collaborer avec le monde des développeurs. Cette API baptisée « Simone », a vu le jour en 2012, afin de permettre à des développeurs d'enrichir les fonctionnalités de son application bancaire. Le principe est simple, la banque fournit au travers de cette API, un kit de développement logiciel afin de permettre aux développeurs d'avoir un accès sécurisé aux données bancaires de ses clients. La banque a également été plus loin dans la démarche, anticipant les risques de vol de données, en assumant l'entière responsabilité juridique en cas de fraude ou de vol. Il est important de souligner que cette initiative a été une première mondiale.

*16 - **Linxo** : communiqué de presse sur le partenariat avec HSBC France*
*17 - **Capital** : Société générale et crédit du Nord*

La banque a par la suite créé son propre *app store*, le « CAstore », afin de permettre aux développeurs, appelés « Les Digiculteurs » de proposer leurs applications aux clients de la banque. Le modèle économique mis en place est innovant [18] : le client qui utilise de 1 à 10 applications par mois paye un montant forfaitaire, les fonds récoltés sont utilisés pour entretenir la plateforme, la part restante revenant aux développeurs.

La plateforme connait aujourd'hui un franc succès et le Crédit Agricole organise régulièrement des hackathons dans le but de stimuler l'innovation au travers de concours thématiques. Comme en mai 2015 avec le challenge *Mobile Banking Factory* [19], ou encore en janvier 2016 avec un concours autour des l'habitat connecté [20].

Notons par ailleurs que les applications développées ne sont pas toutes orientées vers l'univers bancaire. L'objectif était de pouvoir proposer à ses clients sociétaires de bénéficier de services innovants au travers de leurs données. C'est pourquoi la banque est entrée au capital de **Linxo** en janvier 2016 [21]. La banque va initier ce service avec un test auprès des clients de **BforBank** en 2017. Elle étendra l'application à l'ensemble de ses entités si le test est concluant.

*18 - **Finextra** : UK sets out open banking API framework*
*19 - **Crédit Agricole** : Challenge Mobile Banking Factory*
*20 - **Crédit Agricole** : Habitat Connecté*
*21 - **Linxo** : communiqué de presse sur l'entrée au capital du Crédit Agricole*

En conclusion, le business model qui semble aujourd'hui être privilégié par les banques en France est le modèle mixte. Il permet aux banques de bénéficier de la technologie offerte par les agrégateurs en gardant le contrôle tant sur leur image et que sur leur relation client.

ENCART 5

La banque responsable de son app store ?

Que se passerait-il si l'une des applications était contraire à la loi ? La banque serait-elle responsable d'une application illégale développée par un tiers et éditée via son app store ?

La réponse est donnée par la loi pour la confiance dans l'économie numérique du 21 juin 2004[22] *(LCEN)*, qui est applicable à toutes les communications au public en ligne, y compris les « app stores » fournis par des banques.

La LCEN distingue deux types d'acteurs: l'éditeur de contenus, qui engage automatiquement sa responsabilité ; et l'hébergeur qui ne peut voir sa responsabilité engagée que s'il n'a pas agi promptement pour retirer tout contenu illicite à compter du moment où le caractère illicite dudit contenu lui a été notifié. En application de la LCEN, la banque devrait être considérée comme éditeur des applications disponibles si elle effectue une validation de ces dernières avant mise à disposition au public. Dans le ca cas contraire, elle devrait être considérée comme simple hébergeur des applications.

3.4 Des tiers hors de l'écosystème bancaire lorgnent sur les données bancaires

Trois typologies d'acteurs tiers s'intéressent également de près aux données bancaires.

Les premiers sont les assureurs, qui voient dans la DSP2 la possibilité de devenir des établissements de paiement et de proposer à leurs clients mutualistes des possibilités d'agréger leurs comptes. En France, **la MAIF** vient de lancer son service d'agrégation de comptes bancaires baptisé « Nestor », conçu en marque blanche avec la technologie de **Linxo**.

« Le digital entraîne un abaissement généralisé des barrières à l'entrée. Partant de ce constat, nous sommes défensifs sur notre cœur de métier, mais rien ne nous interdit d'être offensifs sur des métiers qui ne sont pas les nôtres »,

Pascal Demurger, Directeur Général de la MAIF.[23]

*22 - **Legifrance** : Loi n°2004-575 du 21 juin 2005 pour la confiance dans l'économie numérique*
*23 - **La MAIF***

Les seconds acteurs sont les opérateurs téléphoniques. Pour exemple, le lancement d'Orange Bank prévu en 2017 marque la volonté de l'opérateur de proposer des services bancaires à ses clients. **Orange** est de surcroît entré au capital de **Groupama Banque** via une prise de participation majoritaire. Objectif : 2 millions de clients à terme.

Enfin, les derniers et plus inquiétants concernent les GAFA *(Google, Apple, Facebook et Amazon)*. Ces géants du web au cœur de la gestion des données, et de ce que l'on appelle plus largement le Big Data, affirment leur ambition de bousculer les acteurs traditionnels bancaire du marché. Leur arrivée sur ce marché témoigne de leur volonté d'acquérir tout type de données pour une connaissance client toujours plus poussée. Citons par exemple le comparateur de prix de **Google** lancé en 2016 et **Apple Pay** en 2015, ou Messenger Payments pour **Facebook** la même année. **Amazon** a également franchi le cap, en allant vers le crédit, avec la solution Amazon Lending lancée en 2012 et Amazon Store Card en 2015. L'enjeu pour eux est immense : pouvoir contrôler l'ensemble de la chaine de valeur, et rendre le parcours client plus fluide, mais surtout intensifier leur cœur de métier sur la collecte des données et ainsi pouvoir connaitre plus facilement leurs utilisateurs et leurs habitudes. Ils restent pour l'heure discrets, mais inutile de souligner que leur force de frappe financière leur permettront d'absorber aisément les Fintech qui se positionnent aujourd'hui au travers de la DSP2. Opportunités ou menaces, les questions se posent, la DSP2 ouvre la voie d'une nouvelle ère bancaire.

Conclusion

Sommes-nous à l'aube d'un open data bancaire ?

La DSP2 s'inscrit certainement dans ce mouvement, déjà entamé par le service de mobilité bancaire *(prévu par les lois Hamon et Macron)* et plus récemment par la loi du 7 octobre 2016 pour une République numérique, qui consacre un droit à la portabilité permettant aux consommateurs de récupérer leurs données auprès de leurs prestataires de services numériques et de les transférer auprès d'autres prestataires. Ce droit vient compléter le droit à portabilité prévu par le règlement européen de protection générale des données du 27 avril 2016. Les banques ne sont pas exclues du champ d'application de ce texte.

Au contraire, l'essor des services en ligne des banques fait de ce secteur une cible privilégiée de cette nouvelle réglementation qui vise essentiellement à ouvrir le marché à de nouveaux entrants, et ce, au profit du consommateur, tout comme la DSP2.

A partir du 25 mai 2018, ce droit à la portabilité permettra au consommateur *(notamment de services de banque en ligne)* de récupérer, par une requête unique, l'ensemble de ses fichiers ou données de consommation. A cet effet, les fournisseurs des services en ligne devront prendre toutes les mesures nécessaires notamment en termes d'interface de programmation et de transmission des informations nécessaires au changement de fournisseur. Voilà à nouveau que les APIs pointent leur nez…

Au travers de ce livre blanc, les APIs et plus particulièrement les Open APIs apparaissent comme une réelle alternative au « *web-scraping* » et un point d'équilibre entre sécurité et innovation. Toutefois, il reste encore un chemin important à parcourir pour parvenir à une standardisation des APIs et de la structure des données, permettant une interopérabilité entre les services sur ce nouvel écosystème.

On constate que les banques françaises après avoir été réticentes ont compris l'enjeu et l'opportunité de développer des projets dans ce domaine. Elles ont été inspirées par certaines banques Allemandes, comme **SolarisBank** et **Fidor Bank** qui ont ouvert la voie vers l'Open-Banking en Europe.

Mais jusqu'où ce mouvement ira-t-il ? Jusqu'à une banalisation de la donnée bancaire, jusqu'ici sanctuarisée par une tradition du secret et de la sécurité ?

Il est en tous cas vital pour le secteur bancaire de mesurer les évolutions en cours. Au lieu de subir les assauts de nouveaux entrants souvent plus agiles et moins lourdement réglementés, il pourrait saisir le taureau par les cornes, en se plaçant au centre du jeu, par une définition équilibrée et responsable des conditions d'accès aux comptes bancaires. Et en créant les conditions d'un nouvel écosystème créateur de valeur pour lui.

A PROPOS DES AUTEURS

Thibault Verbiest
De Gaulle Fleurance & Associés

Avocat et ancien entrepreneur, Thibault Verbiest dispose d'une expérience approfondie notamment en propriété intellectuelle, et dans le secteur des technologies, des médias et des télécommunications.

Il conseille les clients de notre société dans des opérations variées, allant de la dématérialisation des services bancaires et financiers, à la transformation digitale des entreprises, en passant par les fusions & acquisitions dans le domaine technologique. Il assiste également nos clients sur certains dossiers de contentieux, notamment en propriété intellectuelle ou en responsabilité liée à la cybersécurité.

Plusieurs collaborateurs de la société d'avocats De Gaulle Fleurance & Associés sont intervenus sur le projet :

Jonathan Souffir : Avocat Associé

Jean-Sébastien Mariez : Avocat Senior Counsel

Hermien Van Der Vynckt : Juriste

Paul Noel
Galitt - Payment Consulting

Diplômé de l'Ecole de Guerre Economique (EGE), Paul Noel est actuellement Business Analyst au sein de la Business Unit Payment Consulting de Galitt.

Plusieurs collaborateurs de Galitt sont intervenus sur le projet :

Hervé Ammeux : Stream Director

Emmanuel Caron : Stream Director

Benjamin Deblauwe : Chef de Projet

Gérard de Moura : Directeur Général Délégué

Stéphane Dubois : Stream Manager

Jérémie Fave : Payment Consultant

François Flouriot : Practice Manager

Vincent Mesnier : Directeur Exécutif - Testing Solutions

Anne-Sophie Mouraud : Payment Consultant

Isabelle Pujadas : Directrice de la communication

Gérard Tchakgarian : Président

Diane Walch : Business Development Director

Galitt

17 route de la Reine
92100 Boulogne-Billancourt - France
Tél. : +33 1 77 70 28 00
contact@galitt.com
www.galitt.fr

DE GAULLE
FLEURANCE
& ASSOCIÉS

SOCIÉTÉ D'AVOCATS

9 Rue Boissy d'Anglas
75008 Paris - France
Tél. : +33 1 56 64 00 00
www.degaullefleurance.com

Création graphique : www.jean-charles-dart.weonea.com