VIATYS

DE LA DSP2 À L'OPEN BANKING :

LES IMPACTS SUR LE MODÈLE TRADITIONNEL BANCAIRE

VIATYS

DE LA DSP2 À L'OPEN BANKING :

LES IMPACTS SUR LE MODÈLE TRADITIONNEL BANCAIRE

Audrey DHELLEMMES, Thomas BERARD,
Pierre KOLLEN, Marion TASTES

EN RÉSUMÉ

Les changements technologiques et culturels ont modifié la manière de « consommer » le service bancaire traditionnel. Les clients recherchent dorénavant la facilité de l'usage et considèrent le parcours d'achat comme un produit à part entière.

Ces comportements impactent profondément le marché des services financiers qui se transforme avec l'arrivée de nouveaux entrants comme les FinTech et les GAFAM. Ils perçoivent la donnée comme la source principale de revenus contrairement aux acteurs bancaires traditionnels qui restent sur des services payants.

Qui plus est, l'évolution de la réglementation, avec l'entrée en vigueur de la DSP2, oblige les banques à mettre à disposition leurs données auprès de tous les nouveaux opérateurs, accélérant la remise en question de leur modèle.

Dans ce contexte, quelle stratégie d'ouverture les banques doivent-elles adopter, pour quel modèle de rémunération : développement des API internes, renforcement des partenariats ou mutation en « BaaS : Bank as a Service » et face à une désintermédiation latente, comment conserver une relation client forte ?

Ce livret vous apporte une vision détaillée de ces sujets et les pistes sur les actions à mener.

Chez Viatys, nous avons la conviction que les entreprises doivent dès à présent passer dans l'ère de l'API First pour développer leur marché. Plus spécifiquement, les banques auront alors deux nouveaux leviers de croissance : en interne, par la modernisation de leur SI, et en externe, pour une extension de leurs réseaux de distribution et l'intégration de services complémentaires.

SOMMAIRE

1. CONTEXTE

1.1. DES CLIENTS DE PLUS EN PLUS MOBILES

Depuis le lancement du premier smartphone iPhone par Apple en 2007, les usages ont drastiquement changé au travers d'une centralisation de technologies et de services sur des appareils mobiles (accès à internet, e-mail, applications pour tous types d'usages, reconnaissance biométrique).

La génération Y, qui focalise beaucoup l'attention, est symptomatique de ces évolutions, puisqu'elle est la prochaine grande génération par nombre de personnes : en France 15,4 millions d'individus sont nés entre 1980 et 2000. Les usages ont changé et s'adaptent à cette nouvelle génération considérée comme « Digital Native », première génération du numérique.

Pour s'adapter à cette mobilité, ces dernières années, les applications ont même été repensées pour passer d'un mode multicanal à un mode omnicanal. Le marketing multicanal implique une cohérence dans toutes les communications à destination des utilisateurs. Pour aller plus loin, le marketing omnicanal permet d'acheter ou de souscrire à des offres en changeant de support de communication (smartphone, tablette, web, service client, agence) durant le processus d'achat. Il devient possible de poursuivre sur un autre support, tablette ou web, une action entamée sur mobile par exemple. Les informations des clients doivent alors être centralisées pour être réutilisées et communiquées à tous les départements.

Cet usage tout mobile est aujourd'hui démocratisé et d'innombrables applications sont disponibles. Malgré cette offre pléthorique, l'utilisateur restreint souvent son usage à quelques applications.

En quelques chiffres:

- 80% des applications téléchargées sont supprimées après leur première utilisation.
- Une application téléchargée et non ouverte pendant 7 jours ne le sera jamais plus.
- 65% du temps passé sur des applications l'est à des fins d'amusement.

L'objectif des acteurs mobiles est donc de se rendre indispensables et que l'utilisation de leurs applications mobiles perdurent dans le temps. Dans ce marché, les applications bancaires sont bien positionnées. Les banques sont aujourd'hui l'un des rares acteurs sur le marché mobile à maintenir un usage élevé de ses applications.

1.2.
GAFAM ET FINTECH S'INTERMÉDIENT ENTRE LE CLIENT ET SA BANQUE

1.2.1.
Fortes de leurs usages devenus la norme pour les clients mobiles, les GAFAM proposent aussi des services bancaires

Les grands gagnants de ces changements de mode de consommation sont évidemment les GAFAM : Google, Apple, Facebook, Amazon et Microsoft. Inconnues pour la plupart du grand public il y a 20 ans, ce sont aujourd'hui des entreprises incontournables trustant **les premières places de la capitalisation boursière.** En bâtissant leurs empires sur le digital, les GAFAM comptent maintenant des centaines de millions d'utilisateurs.

Les GAFAM définissent **des usages qui deviennent la norme :** de la tablette d'Apple, aux assistants personnels digitaux (Apple avec Siri, Google avec Google Home, Amazon avec Alexa). Ces géants du web ouvrent désormais leur horizon et explorent d'autres secteurs d'activité tels que l'automobile, la culture et même le secteur bancaire (Google Wallet, Apple Pay, paiements dans Facebook Messenger, Amazon Pay, WhatsApp Payment).

1.2.2.
Les FinTech apportent de nouveaux usages

Depuis 2008 de nouveaux acteurs, en plus des GAFAM, s'intéressent au monde de la banque : les start-up financières, appelées **FinTech**. Celles-ci sont déjà 12 000 dans le monde et représentent en 2015 19 milliards de dollars d'investissements.

Si aujourd'hui elles sont considérées comme un danger pour les banques c'est parce que ces entreprises révolutionnent le monde bancaire, notamment pour les particuliers, **avec des usages plus adaptés aux changements culturels** en cours.

A n'en pas douter, pour beaucoup de FinTech, la véritable innovation ne provient pas que de la technologie mais des usages en réinventant l'acte de s'informer, de payer, de souscrire, et en s'adaptant à des nouveaux contextes d'achat et d'utilisation des comptes bancaires.

Elles savent aussi tirer le meilleur parti des données, en les exploitant, pour proposer des services innovants à forte valeur ajoutée et qui correspondent aux nouveaux besoins et usages des utilisateurs.

1.2.3.
GAFAM et FinTech s'intermédient dans la relation du client avec sa banque

Les services bancaires subissent une disruption : adoption rapide d'un nouvel usage face à un usage historique. En effet, les GAFAM et FinTech déploient aux services bancaires leurs principes : gratuité, design, qualité d'usage, valeur ajoutée des produits et, pour les GAFAM, confiance des utilisateurs, facilitant l'adoption rapide de ces derniers.

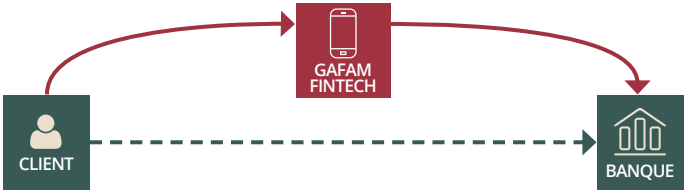
L'un des exemples les plus concrets concerne le paiement. L'utilisateur qui a renseigné sa carte bleue ou son RIB, a accès à de nouveaux services. Grâce à Apple Pay, Google Wallet et la fonctionnalité de Facebook Messenger, l'utilisateur peut facilement virer de

l'argent à ses contacts à partir du numéro de téléphone ou de l'adresse e-mail du bénéficiaire. Pour le même usage, l'utilisateur a aussi le choix d'accéder aux services de FinTech telles que Slim Pay (croissance de 4 068% en 4 ans) ou Leetchi (rachetée 50 Millions par le Crédit Mutuel Arkéa). Désormais, il n'est plus nécessaire de retirer de l'argent liquide ou encore renseigner un compte bénéficiaire sur son site bancaire, puis d'attendre un délai de sécurité pour pouvoir effectuer le virement.

Tous ces services sont gratuits, rapides, faciles à utiliser et basés sur des informations que le client a fourni volontairement aux « Third Party Provider », TPP. **Pour la banque, ces services représentent un intermédiaire** qui vient se positionner entre elle et ses clients.

La réduction des interactions avec les clients et l'utilisation des applications bancaires signifient de facto, pour la banque, une perte d'informations du comportement des clients et de leurs besoins. Cet éloignement peut réduire la capacité de la banque à proposer aux clients des produits et services adaptés à leurs besoins. **La perte de la relation client représente une menace majeure pour les banques.** Elles ont peur de devenir de simples fournisseurs de services de back office bancaire : tenue de compte, exécution de paiements, mise à disposition de liquidités, sans interaction directe possible avec le client.

La désintermédiation des banques



1.2.4.
Les néobanques viennent perturber le jeu…

Les néobanques se présentent comme des challengers sérieux dans la course à l'ouverture de comptes. Appelés Comptes Nickel, N26, Revolut, pour la plupart, elles ont en commun de ne pas avoir été créées par des acteurs bancaires.

Le tout digital est le maître mot (à l'exception de l'ouverture de compte chez Compte Nickel) pour ces nouveaux arrivants qui ont un taux de pénétration sur le marché important, notamment grâce à des services gratuits et innovants. Cependant les néobanques ne bénéficient pas encore du même capital confiance que les banques traditionnelles comme en atteste une étude de Next Content. Selon cette étude, seules 24% des personnes interrogées sont prêtes à ouvrir un compte dans une néobanque.

Pour autant, les néobanques auront un rôle à jouer dans l'évolution du marché bancaire. Pour développer leurs services et concurrencer les banques traditionnelles, elles devront, au moins dans un premier temps, s'appuyer sur des partenariats externes.

L'exemple le plus probant étant celui de la néobanque Starling Bank qui a lié des partenariats avec Pension Bee, Habito, WealthSimple et Kasko pour étendre ses services aux pensions de retraite, crédits hypothécaires, solutions d'investissement et à l'assurance voyages (via API). Près de 25 services devraient bientôt étayer le catalogue de Starling Bank d'ici fin 2018. Cette stratégie de partenariats fait de la néobanque un challenger sérieux, avec une gamme de services plus complète.

1.2.5.

… et la banque peine à suivre le rythme

Rompus aux méthodologies Agile, GAFAM et FinTech lancent rapidement des services novateurs, qui sont ensuite améliorés en fonction des retours clients. Les banques s'inspirent des nouvelles méthodologies projets (Agile, Lean) et lancent même leurs laboratoires internes pour incuber des projets innovants (Labs). Mais, **par la multitude de ses métiers, le nombre de produits bancaires, la complexité de ses processus internes et l'historique de ses systèmes, la banque n'est pas aussi flexible** et s'efforce de suivre, avec plus de difficultés, la cadence imposée.

1.3.

CES NOUVEAUX USAGES PERMETTENT AUSSI DE COLLECTER ET D'EXPLOITER DES DONNÉES

Comme il est d'usage, les FinTech et les GAFAM proposent gratuitement de nouveaux services bancaires à l'ensemble de leurs utilisateurs, déjà très nombreux pour les GAFAM. Par l'utilisation des nouveaux services, **ces nouveaux intermédiaires bancaires collectent les données bancaires.**

Pour remettre les données en perspective, rappelons que chaque jour, il est produit autant d'informations que l'humanité n'en a produites jusque-là fin du 20e siècle.

C'est désormais la course à la donnée : sa collecte, son stockage structuré, son exploitation et sa valorisation via de nouveaux services. Nombreuses sont les entreprises qui revoient leurs infrastructures afin d'accueillir ce changement de paradigme : Big Data et capacités analytiques.

Les entreprises exploitent les données pour comprendre et anticiper les besoins des consommateurs. Il devient possible de valoriser les données en proposant de nouveaux services B2B/B2C, qui eux seront **rémunérés.**

58 %

des personnes interrogées se disent confiantes sur l'exploitation de leurs données par les banques selon Etude Next Content

C'est un défi majeur pour **les banques qui possèdent une véritable mine de données** (revenus, emprunts, typologies et moyens d'achat, dates d'opération etc.). Elles bénéficient en plus de la confiance de leurs clients. Toujours selon l'étude Next Content, environ 58 % des personnes interrogées se disent confiantes sur l'exploitation de leurs données par les banques. Pour les FinTech, la collecte de données est un enjeu majeur, d'autant que le sentiment de confiance est moins présent.

1.4.
DES USAGES PERMIS GRÂCE À DES PROCÉDÉS DE COLLECTE DE DONNÉES (SCREEN SCRAPING ET API) ET ENCADRÉS PAR LE RÉGULATEUR

1.4.1.
Les données bancaires récupérées par le procédé de Screen Scraping

Pour assurer leurs services, **les TPP utilisent le procédé de Screen Scraping.**

Pour bénéficier des services des TPP, les clients doivent donner leur accord mais surtout leurs identifiants et mots de passe, enfreignant ainsi, le plus souvent sans le savoir, leur contrat avec leur banque. Les informations de connexion permettent aux TPP de se connecter aux sites des banques en se faisant passer pour les clients, par la simulation des actions du client. Les données des sites bancaires sont récupérées pour être restituées au client ou, possiblement, pour être stockées et analysées.

Le Screen Scraping a notamment permis ces deux nouveaux usages :

- **L'agrégation de comptes.** Elle permet aux utilisateurs disposant de plusieurs comptes bancaires de bénéficier d'une vision consolidée et interactive de l'ensemble de leurs comptes tenus dans différentes banques via une seule et unique interface, y compris l'historique des transactions et le solde de leurs comptes.
- **L'initiation de paiements.** Elle offre la possibilité aux utilisateurs de demander à un intermédiaire de présenter des opérations de paiement. Par exemple, un virement peut être effectué par l'initiateur du paiement en simulant l'action du client auprès de sa banque, en utilisant son identifiant et son mot de passe. Puisque l'action a été réalisée « en son nom », le client reste le seul responsable de l'exécution de l'opération.

FOCUS

QU'EST-CE QUE LE SCREEN SCRAPING ?

- En s'inscrivant à des services tiers (TPP), le client communique ses informations de connexion à sa banque : identifiant et mot de passe.
- Les automates des tiers simulent l'action du client en se connectant à sa place sur le site de la banque.
- Les automates récupèrent l'ensemble des données disponibles sur le site et les restituent à l'utilisateur.
- Il n'y a pas de contrôle de l'acteur tiers ni des données récupérées.
- Un automate est développé par site : cette solution est donc sensible aux modifications de pages Internet.

Au-delà d'une vision exhaustive et d'une analyse de tous les revenus, de toutes les dépenses, **les agrégateurs peuvent proposer à leurs clients des services complémentaires,** par exemple :

- L'analyse des offres du marché pour identifier les produits les plus compétitifs et répondant le mieux à leurs besoins.
- Le regroupement d'informations administratives pour souscrire de nouveaux produits et/ou services.

- Le coffre-fort numérique, la gestion des factures, la proposition des opérations de cashback, le conseil personnel sont également envisageables en fonction de l'évolution des usages et de la capacité d'innovation des acteurs.
- L'initiation de paiement pour optimiser la gestion des comptes de leurs clients en réalisant les paiements appropriés pour éviter de payer des intérêts de découvert, pour augmenter leur épargne…

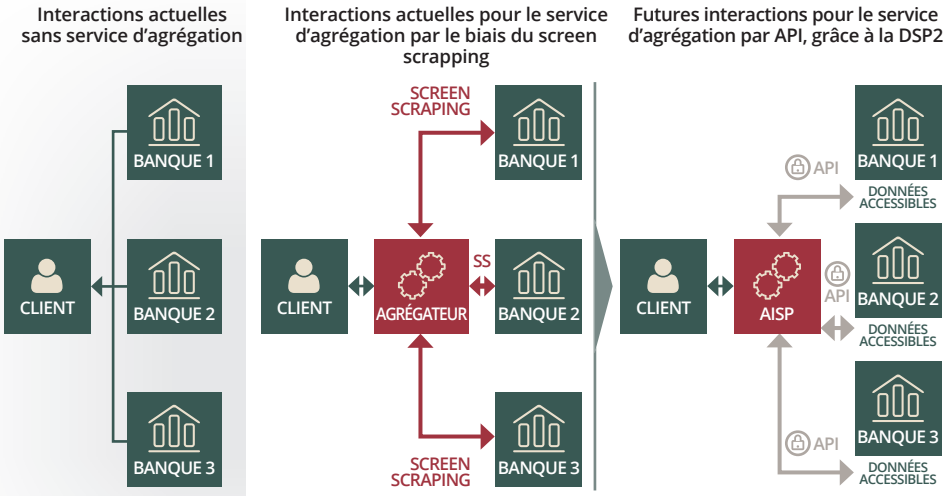
Si le Screen Scraping est si décrié, c'est que ce procédé absorbe bien plus de données que les seules données nécessaires à l'utilisation du service et celles dont l'utilisateur a conscience. Même si les FinTech ont fait des efforts de sécurisation de leurs systèmes, les utilisateurs restent vulnérables en cas de fraudes ou de fuites de données. Le régulateur a souhaité, par la DSP2 et la RGPD notamment, encadrer les pratiques et protéger les utilisateurs.

1.4.2.

L'API comme prérequis à la mise en conformité

Au cœur de la directive DSP2 se trouve l'obligation pour les banques d'accorder à des tiers un accès sécurisé aux informations sur les comptes des clients. **L'accès sécurisé se fera à l'aide d'API**

Exemples des interactions entre client, agrégateurs de comptes et banques pour consulter l'ensemble des comptes que le client détient dans différentes banques :



Le client consulte ses comptes sur chacune des applications de ses banques

Le client utilise un service d'agrégation pour consulter l'ensemble de ses comptes.

L'agrégateur récupère l'ensemble des données via screen scrapping. Il n'y a aucune identification de l'acteur tiers auprès des banques agrégées.

Le client utilise un service d'agrégation pour consulter l'ensemble de ses comptes.

L'AISP s'identifie auprès des banques à agréger et ne récupère que les données pour lesquelles il a le droit d'accès (via API).

(Application Programming Interface) qui est un standard d'échange de données entre deux applications informatiques.

En France, le standard a été initié par la Fédération Bancaire Française (FBF) et défini par la STET, opérateur français de plateformes de paiement de détail. L'API et ses spécifications ont été publiées le 18 juillet 2017.

FOCUS

QU'EST-CE QU'UNE API ?

- API, Application Programming Interface, est une interface d'échange de données.
- Le flux de données est sécurisé et contrôlé.
- L'API est nécessairement développée par le fournisseur, pour donner accès à des tiers à ses données.
- Les API sont mises à disposition sur une plateforme d'API management qui permet la gestion du cycle de vie de l'API, le contrôle des accès des applications qui consomment les API et le suivi leur utilisation.

1.4.3.
Le calendrier normatif et règlementaire

Pour garantir la protection des utilisateurs et de leurs données, pour encadrer les nouveaux usages et face à la multiplicité des risques de sécurité et d'attaques cyber criminelles, le régulateur met en place des lois et des directives réglementaires. Les contraintes impacteront l'ensemble des acteurs. Dorénavant, les FinTech et les GAFAM sont même associés aux discussions sur les futures règlementations.

FOCUS

LE CALENDRIER RÉGLEMENTAIRE ET NORMATIF : UNE MISE EN CONFORMITÉ POUR :

Loi pour une République numérique

Promulguée le 7 octobre 2016, cette loi a pour objectifs principaux de :

- Promouvoir l'innovation dans le développement de l'économie numérique ;
- Créer un cadre de confiance clair, garant des droits des utilisateurs et protecteur des données personnelles ;
- Construire une République numérique ouverte et inclusive, pour que les opportunités liées à la transition numérique profitent au plus grand nombre.

Cette loi comprend un nombre de décrets avec des calendriers spécifiques. Les thèmes légiférés sont :

- Open data, au sein des services publics ;
- Formation, recherche et statistiques sur les données ;
- Plateformes : portabilité des données, loyauté et déclaration des locations courte durée ;
- Protection des internautes, avec notamment les sanctions CNIL jusqu'à 3 millions d'euros, la protection des hackers blancs, le droit à la mort numérique ;
- Télécommunications : non-discrimination pour l'accès au réseau, accélération du très haut débit et expérimentations ;
- Nouveaux usages : l'identité numérique, le coffre-fort numérique, le recommandé électronique, le statut de joueurs de jeux vidéo, le don par SMS ;
- Accessibilité téléphonique et numérique et le maintien de la connexion.

CE QU'IL FAUT RETENIR

Dans l'ensemble de ces décrets promulgués et à venir, il est important de relever pour les activités bancaires :

- **Le renforcement de l'obligation d'information.** Le client doit savoir que ses données sont collectées et à quel effet elles sont exploitées.
- **La mise en place d'un dispositif d'exercice des droits par voie électronique.** Pour faire valoir ses droits de récupération de ses données, l'utilisateur doit pouvoir en effectuer la demande via le site Internet, et plus uniquement par courrier postal.
- L'adaptation des procédures internes, pour **l'exercice des droits suites au décès d'une personne.**

Le non-respect de ces dispositions engendre une sanction avec un plafond de 3 millions d'euros.

Directive Network and Information Security (NIS)

L'Union européenne (UE) a adopté le 6 juillet 2016 la directive NIS sur la sécurité des réseaux et des systèmes d'information. La directive prévoit :

- Le **renforcement des capacités nationales de cyber-sécurité.** Les états membres devront se doter d'autorités nationales compétentes en matière de cyber-sécurité, d'équipes nationales de réponse aux incidents informatiques et de stratégies nationales de cyber-sécurité.
- L'établissement d'un **cadre de coopération volontaire** entre Etats membres de l'UE, pour faciliter le partage d'informations techniques sur les risques et les vulnérabilités.
- Le renforcement par l'état de la cyber-sécurité des opérateurs de services essentiels au fonctionnement de l'économie et de la société. Ils devront se conformer aux règles établies par l'état et seront obligés de **notifier les incidents** ayant un impact sur la continuité de leurs services essentiels.
- L'instauration de **règles européennes communes** pour les prestataires de services numériques (Cloud, moteurs de recherche, places de marché en ligne).

Les états membres ont jusqu'au 9 mai 2018 pour transposer la directive dans leur droit national. Ils devront y inclure les sanctions.

General Data Protection Regulation (RGPD)

La RGPD est un règlement européen, adopté en avril 2016 qui s'appliquera dès mai 2018.

Il constitue le droit fondamental et inaliénable, pour chaque citoyen, **de protéger sa vie privée et ses données personnelles.** La RGPD impacte **toute entreprise qui collecte, traite et stocke des données personnelles** dont l'utilisation peut directement ou indirectement **identifier une personne.**

La directive E-Privacy

La directive E-Privacy est mise à jour pour se conformer à la RGPD. Elle est prévue pour le 25 mai 2018 et encadrera :

- **Les cookies.** L'internaute donnera expressément son consentement pour le dépôt de cookies, à l'exception des cookies pour les communications électroniques (Internet Explorer, Chrome, etc.), pour les services auxquels il a souscrit ou pour ceux mesurant l'audience. L'utilisateur devra pouvoir gérer tous les autres cookies dans un système centralisé. Le droit de retrait de l'utilisateur lui sera rappelé tous les six mois.
- **Les métadonnées.** Pour la circulation des données, elles peuvent être traitées sans le consentement de l'utilisateur. Les contenus devront être supprimés ou anonymisés après réception par leurs destinataires. Les métadonnées devront également être supprimées ou anonymisées dès qu'elles ne seront plus nécessaires pour la transmission de la communication.
- Les Over The Top. **Les OTT**, tels que Skype, WhatsApp, Facebook Messenger, Viber, seront désormais concernés.

CE QU'IL FAUT RETENIR

LES PRINCIPES CLÉS DE LA GRPR SONT :

- **Précision :** les données personnelles doivent être précises et mises à jour et toutes les étapes raisonnables doivent être prises pour assurer la rectification ou l'effacement de données inexactes sans délai.
- **Limitation de stockage :** les données personnelles ne peuvent pas être conservées plus longtemps que nécessaire aux fins pour lesquelles elles sont traitées.
- **Intégrité et confidentialité :** une protection adéquate (technique et organisationnelle) avec une sécurité et une protection appropriées contre tout traitement, perte, dommage ou destruction non autorisés. C'est un composant de sécurité de l'information de la vie privée.
- **Responsabilité :** le contrôleur est responsable et doit démontrer sa conformité aux principes ci-dessus relatifs au traitement des données personnelles.

LES OBLIGATIONS DE LA RGPD :

- **Consentement :** lors de l'obtention du consentement pour l'utilisation des données, les entreprises ne peuvent pas utiliser des termes et conditions incompréhensibles remplis de jargon juridique. Il doit être aussi facile de retirer son consentement que de le donner.
- **Notification de recherche :** en cas de violation de données, les processeurs de données doivent informer leurs contrôleurs et clients de tout risque dans les 72 heures.
- **Droit d'accès :** les titulaires de données ont le droit d'obtenir la confirmation du contrôleur de données pour savoir si leurs données personnelles sont en cours de traitement. Le contrôleur de données doit fournir gratuitement une copie électronique de données personnelles aux personnes concernées.
- **Droit à l'oubli :** lorsque les données ne sont plus pertinentes par rapport à leur but initial, les personnes concernées peuvent demander au contrôleur de données d'effacer leurs données personnelles et de cesser sa diffusion.
- **Portabilité des données :** elle permet aux individus d'obtenir et de réutiliser leurs données personnelles pour leurs propres besoins en les transférant dans différents environnements informatiques.
- **Confidentialité par conception :** elle demande l'inclusion de la protection des données dès la conception des systèmes et la mise en œuvre de mesures techniques et d'infrastructures appropriées.
- **Responsable de la protection des données :** les agents qualifiés doivent être nommés dans les autorités publiques ou les organisations (> 250 employés) surveillant ou traitant des données personnelles sensibles.

La RGPD comporte donc l'obligation de répondre à un client qui effectue une **demande d'information, de réclamation, voire de rectification de ses données personnelles (suppression, modification).**

Le non-respect de cette réglementation peut entrainer des amendes de 20 millions d'euros par violation ou 4 % du chiffre d'affaires annuel mondial de l'exercice précédent (le montant le plus important étant retenu).

Les sanctions applicables seront similaires à celles de la RGPD.

Cette règlementation offre l'opportunité d'exploiter de façon plus libre et étendue les données personnelles une fois le consentement de l'utilisateur obtenu.

DSP2

Le détail de la Directive de Services de Paiement n°2 (DSP2) et des RTS (Regulatory Technical Standards) permettant la mise en application de la DSP2 sont présentés dans le chapitre suivant.

Dans ce contexte, les FinTech ont un avantage de taille : leur système d'information est jeune et repose souvent sur des architectures Cloud bien moins contraignantes à maintenir, à auditer et à faire évoluer que les anciens systèmes des banques. Elles **pourront s'adapter aux nouveaux standards d'échange de données** (API). Les **banques,** quant à elles, **disposent de réelles expertises dans la mise en conformité et,** bien que cela ne se voit pas toujours, **en matière de sécurité informatique.**

FOCUS

DES EXEMPLES DE FAILLES DE SÉCURITÉ :

Avec la directive NIS et la RGPD, il devient donc obligatoire pour l'entreprise de **notifier des attaques sur ses failles de sécurité** qu'elle aurait subie, et ce dans les 72 heures. C'est un changement important puisqu'auparavant les entreprises cherchaient à ne pas communiquer sur les failles de sécurité en raison de leur image.

En décembre 2016, un chercheur en sécurité a découvert une faille de sécurité concernant la néobanque allemande N26. Cette brèche aurait pu coûter cher aux clients et à N26 si elle avait été exploitée par des personnes mal intentionnées.

Plus récemment la société de partage de voiture Ouicar a été averti publiquement par la CNIL pour une faille de sécurité élémentaire. Une simple requête sur leurs API permettait d'accéder à la liste des données véhicules. Il était alors possible d'accéder aux données personnelles des utilisateurs à l'aide d'une URL et de leurs identifiants (nom, prénom, adresse, téléphone, numéro de permis de conduire, etc.).

2. DE LA DSP2 ...

L'industrie des paiements est en pleine mutation. Autrefois réservée aux seules banques, elle s'est ouverte aux nouveaux acteurs que sont les prestataires de services de paiement (PSP).

L'Europe aspire à créer un véritable marché des paiements et la DSP2 constitue la suite logique des précédentes réglementations sur l'adoption de la monnaie unique, sur la création du SEPA et l'harmonisation des moyens de paiement.

Si les premières réglementations portaient spécifiquement sur la monnaie fiduciaire et la création de l'euro, la DSP1 sur les systèmes de paiement tels que les virements, les prélèvements et les paiements par carte, c'est donc fort logiquement que la DSP2 s'attaque aux services de paiement en ligne et aux prestations associées à l'environnement bancaire, de plus en plus digital.

A l'heure où nous écrivons, les discussions sont toujours en cours entre les banques et les FinTech. Elles s'opposent sur certains points, essentiellement la possibilité de poursuivre la pratique du Screen Scraping et ses conséquences. Si l'application du texte reste à acter, via les « Regulatory Technical Standards », RTS, l'esprit de la directive DSP2 est ancré chez les acteurs.

2.1. QU'EST-CE QUE LA DSP2 ?

La DSP2 poursuit plusieurs objectifs :

- Favoriser la **concurrence** et **l'innovation** avec l'émergence de services innovants d'agrégation de comptes et d'initiation de paiement ;
- Faciliter et **développer l'utilisation des services de paiement** en ligne sur Internet ;
- Améliorer la **protection des utilisateurs** et consommateurs contre la fraude, les incidents de paiement et les paiements abusifs ;
- Renforcer les **droits des consommateurs ;**
- Encourager une **baisse des prix** sur les services de paiement ;
- Etendre le rôle de l'European Banking Authority, **EBA,** pour coordonner les autorités de **surveillance** et dessiner les **standards techniques** de demain.

CE QU'IL FAUT RETENIR

PAR LA DSP2, LA COMMISSION EUROPÉENNE ENTEND :

- Offrir un **cadre législatif aux nouveaux usages d'agrégation de comptes et d'initiation de paiement** ;
- Donner une **reconnaissance juridique aux nouveaux acteurs intermédiaires** sur la mise à disposition d'informations bancaires et sur le marché des paiements ;
- Garantir un **fort niveau de sécurité** indispensable pour ces services :
  - Sécurité des utilisateurs via la généralisation de **l'authentification forte ;**
  - Sécurité des échanges de données entre les acteurs par la mise en place de normes de communication ouverte, communes et sécurisées **(API).**

Adoptée définitivement par le parlement européen le 25 novembre 2015, elle doit être **transposée dans leur législation par les états membres avant le 13 janvier 2018.** En France, cette transposition est réalisée par le Trésor. Celle-ci pourrait prévoir une extension du cadre prévu par l'UE à un périmètre de comptes plus importants, par exemple une extension des comptes courants aux comptes épargne.

Adossés à la DSP2, les Regulatory Technical Standards, **RTS, sont les standards techniques** permettant l'application de la directive. Ils ont été publiés en février 2017 par l'EBA, et doivent être validés par la Commission Européenne avant fin 2017. L'application des RTS au niveau national interviendra 18 mois après la validation de la Commission Européenne, soit, selon les estimations, entre Juin et Septembre 2019.

2.2. QUEL CALENDRIER ?

DSP2 : calendrier

- **23 février 2017 :** le draft des RTS, rédigé par l'EBA, est proposé à la Commission Européenne dans sa version finale
- **9 août 2017 :** la directive DSP2 est transposée dans le droit français
- **27 novembre 2017 :** la version finale des RTS est adoptée par la Commission Européenne
- **19 décembre 2017 :** l'EBA édite une opinion relative à la période transitoire entre la DSP1 et la DSP2
- **13 janvier 2018 :** la DSP2 entre en application au niveau européen
- **5 février 2018 :** les premiers amendements sur la période transitoire entre DSP1 et DSP2 sont soumis à l'Assemblé Nationale et au Sénat en France
- **2e semestre 2019 :** date butoir pour les pays européens pour l'entrée en application des RTS de la DSP2

○ Règlementation française ○ Règlementation européenne

Ce calendrier a été réalisé fin février 2018.

2.3.
DES ACTEURS ET DES RÔLES RECONNUS PAR LA DSP2

La DSP2 redéfinit les rôles de l'ensemble des acteurs bancaires et offre aux nouveaux acteurs des possibilités d'accès à des comptes dont ils ne sont pas gestionnaires.

Par la DSP2, l'UE reconnaît deux nouveaux acteurs : **les agrégateurs de comptes (AISP)** et **les initiateurs de paiement (PISP).** Ces derniers seront soumis au contrôle de l'ACPR, responsable de la fourniture de ces deux nouveaux agréments.

La directive européenne sur les services de paiement (DSP1), adoptée en 2007, a garanti un accès équitable et ouvert au marché des paiements, puis a renforcé la protection des utilisateurs. Elle a également encouragé la concurrence en permettant à des institutions non financières d'entrer sur le marché des paiements. Elle a défini le statut de Prestataire de Service de Paiement (PSP) en tant qu'établissements de crédit ou établissements de paiement. Avec la DSP2, ce statut devient le **Prestataire de Services de Paiement Emetteur d'Instruments de Paiement (PIISP)**.

Les **Prestataires de Service de Paiement Gestionnaire de Comptes (ASPSP)** sont les banques traditionnelles qui détiennent les comptes et les fonds de leurs clients.

Des acteurs et des rôles reconnus par la DSP2

Par défaut, les banques disposeront de l'ensemble des agréments ci-dessous. Les TPP devront en faire la demande auprès de l'ACPR. Lorsqu'un TPP se connectera à un ASPSP, l'ASPSP vérifiera que le TPP dispose bien de l'agrément (eIDAS)

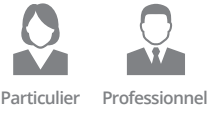
AISP	PISP	PIISP
Account Information Service Provider **AGRÉGATION DE COMPTES** Un client souhaite avoir sur un seul et même outil une vision de ses comptes issus d'une ou plusieurs banques.	Payment Initiation Service Provider **INITIATION DE PAIEMENTS** Un client, depuis un site marchand, souhaite payer en effectuant un virement.	Payment Instrument Issuer Service Provider **FOURNISSEUR DE CARTES DE PAIEMENT** Un client veut payer avec une carte de paiement. L'établissement fournisseur de cartes de paiement pourra interroger la banque pour savoir si le client possède suffisamment de fonds sur son compte.

ACTEURS TRADITIONNELS

PSU

UTILISATEUR D'UN SERVICE DE PAIEMENT (PAYMENT SERVICE USER – PSU)

Un utilisateur est un client, particulier ou professionnel, qui possède un ou plusieurs comptes bancaires, et / ou utilise un service de paiement.



ASPSP

PRESTATAIRES DE SERVICE DE PAIEMENT GESTIONNAIRE DE COMPTE (ACCOUNT SERVICING PAYMENT SERVICE PROVIDER - ASPSP)

Les prestataires de services de paiement gestionnaires de comptes sont les établissements bancaires ou de crédit qui détiennent les comptes et les fonds de leurs clients, tels que les banques traditionnelles.

NOUVEAUX ACTEURS RÉGULÉS PAR LA DSP2

AISP

PRESTATAIRES DE SERVICES D'INFORMATION SUR LES COMPTES (ACCOUNT INFORMATION SERVICE PROVIDER - AISP)

Les prestataires fournissant un service de consolidation des informations d'un ou plusieurs comptes détenus par un client auprès d'un ou plusieurs ASPSP.

PISP

PRESTATAIRES DE SERVICES D'INITIATION DE PAIEMENTS (PAYMENT INITIATION SERVICE PROVIDER - PISP)

Les prestataires proposant un service qui consiste à initier un ordre de paiement à la demande d'un client payeur à partir d'un compte bancaire détenu chez un ASPSP.

ACTEURS EXISTANTS AVEC PÉRIMÈTRE ÉLARGI PAR LA DSP2

PIISP

PRESTATAIRES DE SERVICES DE PAIEMENT EMETTEUR D'INSTRUMENTS DE PAIEMENT (PAYMENT INSTRUMENT ISSUERS SERVICE PROVIDER - PIISP)

Le rôle d'émetteur d'instruments de paiement, qui avait été préalablement règlementé comme Prestataire de Service de Paiement (PSP) dans le cadre de la DSP1, voit son périmètre modifié par la DSP2. Avec la DSP2, ces acteurs deviennent des PIISP et auront la possibilité d'aller interroger directement l'établissement gestionnaire de compte (ASPSP) afin d'obtenir une confirmation de disponibilité des fonds.

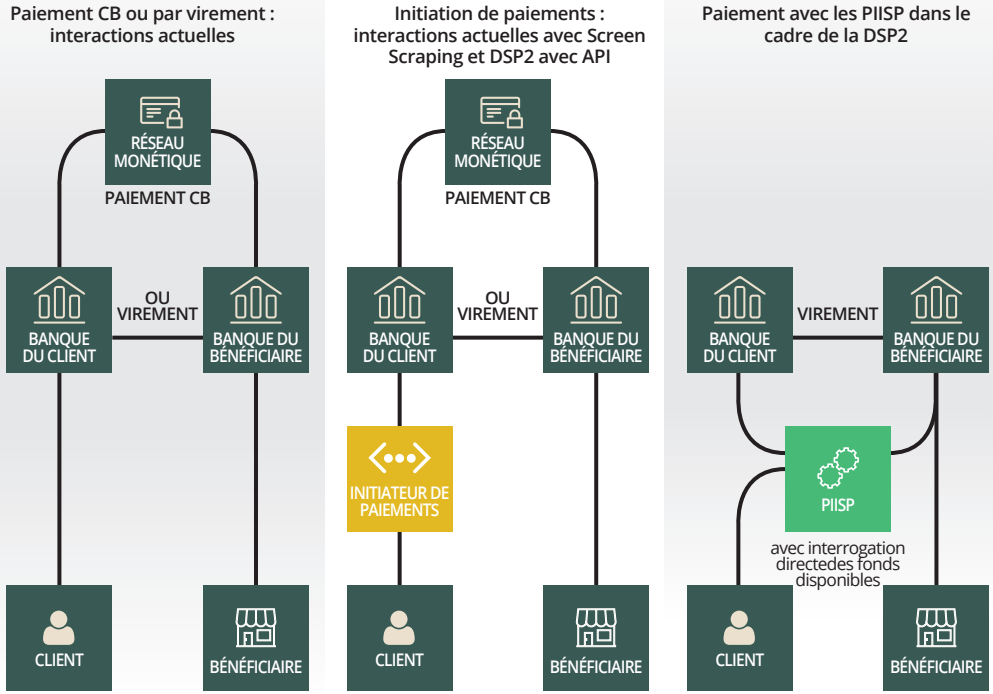
A l'évidence, l'innovation majeure proposée par la DSP2 est la reconnaissance d'intermédiaires qui se positionnent entre les clients et les banques traditionnelles, gestionnaires de leurs comptes.

Les intermédiaires, AISP et PISP, bénéficient de conditions d'exercice allégées et d'exigences assouplies par rapport aux établissements gestionnaires de comptes (ASPSP). En plus de l'obtention d'agréments, ces nouveaux prestataires devront aussi être couverts par une assurance responsabilité civile professionnelle sur les territoires où ils fournissent leurs services.

2.4. DES RÈGLES COMMUNES DE SÉCURITÉ INCLUSES DANS LA DSP2

Les apports de la DSP2 sont également importants pour la sécurité des opérations réalisées par les consommateurs. Par les RTS, la Commission Européenne spécifie les exigences en termes **d'authentification forte** lors de l'accès du client sur son compte de paiement, lors de l'initialisation d'une opération de paiement ou lors de l'exécution d'une action de paiement à distance susceptible d'être frauduleuse.

Evolution paiements



FOCUS

QU'EST-CE QU'UNE AUTHENTIFICATION FORTE ?

C'est la combinaison de 2 facteurs d'authentification, parmi les 3 suivants :

CE QUE J'AI

Téléphone, calculatrice token

CE QUE JE SAIS

Code, mot de passe, date de naissance

CE QUE JE SUIS

Retine, empreinte, voix ...

Un nouveau facteur voit jour : « ce que je fais » ou « behavior analytics » qui analyse par exemples l'utilisation de la souris, la fréquence à laquelle l'utilisateur tape sur le clavier.

Les RTS spécifient aussi **les exemptions** à l'authentification forte prenant en compte le niveau de risque de l'opération, le montant ou la récurrence, etc.

Quelques exemples d'opérations risquées nécessitant le recours à l'authentification forte :

- Pour l'inscription au service d'un AISP ou PISP ;
- Pour la consultation d'informations sans communication de données confidentielles de paiement : lors de la **première connexion** puis a minima **tous les 90 jours** si la banque dispose d'un outil de lutte contre la fraude en temps réel;
- Pour **l'ajout d'un bénéficiaire** dans la liste blanche, sans nécessairement effectuer un virement ;
- Pour un virement si le bénéficiaire n'est **pas inclus dans la liste préétablie des bénéficiaires ;**
- Pour un paiement sans contact d'un montant **supérieur à 50 €** ou pour une somme cumulée de 150 € de paiement sans contact ou pour plus de 5 paiements sans contact consécutifs ;
- Pour des **transactions successives d'un même montant** avec le même bénéficiaire pour la première fois (paiement récurrent) ;
- Pour un paiement électronique supérieur à 30 € ou pour une somme cumulée de 100 € de paiement électronique ou pour plus de 5 paiements électroniques consécutifs ;
- Pour l'exécution d'une action susceptible de comporter un risque de fraude en matière de paiement ou pour toute autre transaction potentiellement frauduleuse.

Les RTS en version finale précisent que les banques devront impérativement

tester leurs API pendant 6 mois avant de les mettre en production (3 mois en recette puis 3 mois en pré-production).

Les RTS définissent également un taux de **risque de fraude en deçà duquel une exemption est possible.** Cela permettrait d'alléger les étapes d'authentification pour un parcours client sans couture pour accélérer le paiement pour les opérations moins risquées. Cela implique :

- La création d'obligations en matière de **gestion des risques** de fraude et de sécurité ;
- La mise en place d'une procédure de **notification des incidents.**

2.5. LES IMPACTS DE LA DSP2 POUR ...

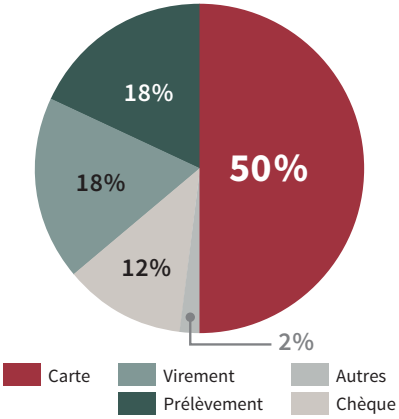
2.5.1. Les banques

Par l'ouverture de l'accès aux comptes des clients et par la possibilité d'initier des paiements par des tiers, la DSP2 oblige les banques à se transformer en revoyant leurs systèmes, leurs processus opérationnels et leur organisation.

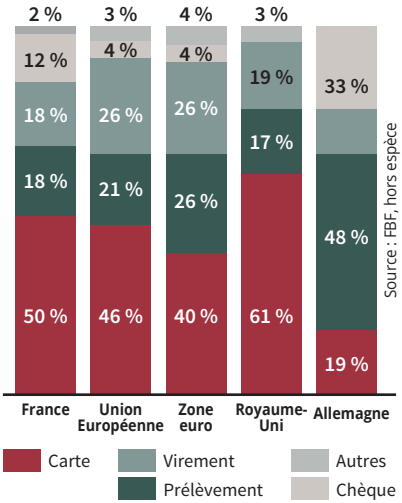
- **Le système d'information :** mise à disposition d'interfaces d'échanges **API**, sur un socle d'API management, avec une architecture garantissant **performances et disponibilités** identiques à celles fournies directement au PSU. L'ASPSP devra garantir aussi le même niveau de secours que celui mis en œuvre pour les PSU (délais de rétablissement notamment).
- **La sécurité** et la **traçabilité des données :** mise en place de contrôles en amont, du monitoring des transactions et de la traçabilité des opérations, pour que seules les données nécessaires à l'opération réalisée soient accessibles.
- Le **référentiel tiers** et le **processus d'autorisation des tiers** : mis en place pour gérer les droits d'accès des TPP et les autoriser à accéder aux données.
- **L'authentification forte** du client (via le protocole OAuth).
- La **sécurité informatique :** mise en place de systèmes de lutte contre la fraude, basés sur un monitoring en temps réel, pour éviter d'utiliser l'authentification forte à chaque consultation des comptes.
- La **gestion des incidents :** adaptation nécessaire des procédures de réclamation client et de gestion des contentieux, permettant notamment de **rembourser le client à J+1.** A ce propos, l'ASPSP sera responsable en cas de problème sur une transaction. La banque aura toutefois la possibilité de se retourner contre l'initiateur de paiement en prouvant la négligence.
- La **gestion des risques** et la **mise en conformité :** renforcement des activités dans ces domaines.
- L'**organisation** de la banque: valorisation de nouvelles compétences (API), apparition de nouveaux métiers (Chief API Officer) et rapprochement des entités métier sur les paiements. Plus que jamais, les métiers de la banque au quotidien devront échanger pour mutualiser les réflexions autour des paiements et les prioriser.

Les ASPSP profiteront aussi de ces nouveaux rôles puisqu'elles obtiendront automatiquement les agréments AISP et PISP. Les banques n'ont d'ailleurs

L'utilisation des moyens de paiements en France et en Europe



L'utilisation des moyens de paiement en Europe varie selon les pays



UE : Allemagne, Autriche, Belgique, Bulgarie, Chypre, Croatie, Danemark, Espagne, Estonie, Finlande, France, Grèce, Hongrie, Irlande, Italie, Lituanie, Lettonie, Luxembourg, Malte, Pays-Bas, Pologne, Portugal, République tchèque, Roumanie, Slovaquie, Slovénie, Suède. **Zone Euro :** Allemagne, Autriche, Belgique, Chypre, Espagne, Estonie, Finlande, France, Grèce, Irlande, Italie, Lettonie, Lituanie, Luxembourg, Malte, Pays-Bas, Portugal, Slovaquie, Slovénie.

pas attendu la DSP2 : nombreuses sont celles qui, dès aujourd'hui, ont lancé leurs services d'agrégation de comptes externes à leur environnement (Société Générale, HSBC, Caisse d'épargne). Il est d'ailleurs intéressant de noter qu'une majorité des banques s'est alliée à une FinTech pour pouvoir obtenir les données bancaires externes.

Suite à la mise en place de la DSP2 et à l'accès à des API normalisées, il est fort à parier que les banques reverront également leur stratégie pour internaliser les développements afin de réaliser par elles-mêmes, sans avoir à payer des flux aux FinTech.

2.5.2.
Les fournisseurs de cartes

La carte de paiement est utilisée pour la moitié des transactions en Europe et reste le moyen de paiement préféré des Français. **Les paiements par carte bancaire, hors espèces, constituent en France plus de 95% du montant total des transactions.** Ils sont en constante progression depuis plusieurs années. A l'instar des britanniques, les français privilégient ce type de paiement, contrairement aux habitants des pays nordiques et aux allemands, **plus adeptes** des virements et des prélèvements.

La DSP2 apporte de nombreuses opportunités pour les fournisseurs de cartes, qui vont pouvoir proposer aux banques des nouveaux services digitaux via API. Par exemple, une communication par API entre Apple Pay et Visa permettrait à Visa de proposer les services d'Apple Pay à ses clients.

La DSP2 va également permettre de faire avancer d'autres types de transactions

comme le Push Payment (paiement initié par le payeur) et ainsi développer le paiement de particulier à particulier.

Un autre champ d'application concerne l'authentification et plus précisément la mise en place des solutions d'authentification biométrique. On peut également imaginer des fonctions de paiement d'objet à objet : à l'image de Jaguar avec le paiement du plein d'essence, directement depuis le tableau de bord, dans les stations Shell.

En 2016, les revenus liés aux paiements (hors espèces) représentent 16% des revenus des banques en Europe Occidentale. Par ailleurs, le volume des transactions des paiements en ligne devrait continuer à progresser à un taux annuel de croissance de 6 à 11% au cours des 5 années à venir. Cette **augmentation des volumes de paiement électronique ne devrait toutefois pas générer des revenus complémentaires pour les banques,** en raison de plusieurs facteurs :

- La poursuite de la réduction des commissions d'interchange liées aux paiements par carte bancaire. Cette commission a baissé de plus de 50% depuis 2011 (source FBF).
- La concurrence de nouveaux acteurs prenant des parts sur le marché des paiements, comme Apple Pay par exemple.

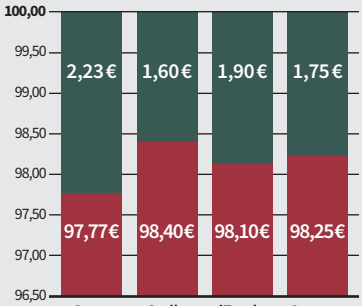
Les banques et les émetteurs de cartes, en premier lieu VISA, Mastercard et American Express sont **menacés par des acteurs d'un nouveau genre :** les prestataires d'initiation de service de paiement (PISP) et les Prestataires de Service de Paiement Emetteur d'Instruments de Paiement (PIISP). Les **paiements électroniques réalisés en ayant recours à un initiateur de paiement seront des virements. Ils se substitueront à un règlement par carte bancaire, plus rémunérateur pour les banques.**

En 2020, 5 à 10% des volumes de paiement pourraient être réalisés, en Europe, par initiation de paiement. Ce pourcentage devrait varier en fonction de la maturité du pays et des habitudes en termes de moyen de paiement utilisé. L'Allemagne par exemple, fortement utilisatrice des virements et habituée à la présence de PISP bien installés, tel que le prestataire Sofort, devrait être plus impactée que des pays comme la France et le Royaume-Uni.

Pour assurer leur maintien, les

FOCUS

LES COMMISSIONS BANCAIRES POUR LES COMMERÇANTS



*Les commissions variables de la carte bancaire sont divisées en 2 catégories :

- La commission interbancaire à 0,23%
- La commission Visa/Mastercard à 2%

Abonnement pour les cartes bancaires : environ 25 € /mois.

Prix des terminaux (à payer une fois et sans abonnement) : Smile & Pay : 29 €, iZettle : 59 €, Sum up : 29 €

acteurs historiques disposent d'une forte **capacité d'investissement,** de **compétences technologiques** et d'un accès au réseau de valeur (relations avec toutes les parties prenantes existantes).

2.5.3.

Les FinTech

Après avoir bâti des services sur des nouveaux usages et profité d'une absence de règlementation, les FinTech vont devoir **moderniser leurs outils** pour se mettre aux normes et respecter le cadre de la DSP2.

L'ère du screen scraping, bien que non révolue, devrait peu à peu disparaitre au profit des API. En l'état, la DSP2 impose aux banques de fournir des API uniquement pour les comptes de paiement. Pour les autres typologies de comptes, les FinTech pourraient conserver le screen scraping. Elles seront alors **contraintes de travailler avec deux technologies** pour fournir le même périmètre qu'aujourd'hui et risquent de rencontrer des problèmes de maintenance et de performance. En France, depuis le 5 février 2018, des échanges parlementaires sont en cours pour déterminer si l'interdiction du screen scraping doit être étendue à d'autres types de comptes.

Avec la mise en place des plateformes d'API management, les banques pourraient aussi mettre à disposition des API pour tout type de comptes et négocier cette mise à disposition avec les FinTech qui n'auraient alors plus à utiliser le screen scraping. Rappelons que la transposition en droit français pourrait prévoir une extension du périmètre prévu par l'UE à un périmètre de comptes plus important.

Les acteurs actuels auront certainement des coûts liés à l'obtention des agréments. Lorsque les FinTech disposeront des agréments, elles auront la possibilité de vendre leur technologie en marque blanche à d'autres acteurs qui ne souhaitent pas développer ces technologies.

Les FinTech sont certes plus agiles lorsqu'il s'agit de faire évoluer leur système. Néanmoins, elles sont moins armées que les banques et ne disposent pas nécessairement de départements entiers étudiant la conformité réglementaire.

2.5.4.

Les e-commerçants

La DSP2 oblige les e-commerçants à une mise en conformité **pour intégrer l'authentification forte.**

Dans une interview, Michael Benisti, Head of Payment chez Vestiaire Collective, l'explique. La DSP2 oblige l'utilisation de l'authentification forte pour les paiements de plus de 30 €. Puisque Vestiaire Collective a un panier moyen de 400€, il leur faudra sécuriser la quasi-totalité de leurs transactions : utilisation du 3D Secure qui nécessite une navigation entre l'application de l'e-commerçant et l'application SMS. Vestiaire Collective s'inquiète de la fin du paiement en 1 click et des frictions pour l'expérience client. Ce dernier souhaite des dérogations pour les entreprises qui savent gérer la fraude autrement qu'avec l'usage de l'authentification forte (Big Data et machine learning donnant un indicateur de confiance élevé pour vérifier la fraude).

Les e-commerçants devront certainement **intégrer de nouveaux modes de paiement** rendus possibles avec les PISP et PIISP. Le service proposé par ces nouveaux acteurs apporte néanmoins de nombreux avantages. Le client est

protégé en cas de fraude. Les avantages pour l'e-commerçant sont :

- Des **commissions généralement plus faibles** car les transactions se font par virement ou prélèvement.
- Une solution **sans abonnement ni frais** de maintenance ou de support.
- Une **diminution du risque de fraude** monétique, avec la vérification de la solvabilité en temps réel.

Les e-commerçants auront également intérêt à ce que les banques déploient des solutions normalisées, avec le concours de la STET, pour éviter de multiplier des méthodes de paiement hétérogènes sur leurs plateformes.

2.5.5.
Les GAFAM

Même si l'UE veille à l'abus de position dominante des GAFAM en Europe (cf. Google et Android), les GAFAM constituent incontestablement la **menace la plus importante** pour l'ensemble des parties prenantes de par leur poids sur le marché :

- Une capitalisation boursière 30% supérieure à l'ensemble des entreprises du CAC 40 ;
- En cumulé, plus de 6 milliards de personnes utilisent les services proposés par les GAFAM ;

Les GAFAM ont toute l'agilité et les compétences technologiques pour proposer de nouveaux services. Elles auront l'opportunité de devenir une marketplace proposant des services financiers et non financiers dans un concept de « one stop shop ». De surcroît, par l'utilisation des services, elles améliorent encore la connaissance de leurs clients.

Plus de temps à perdre pour le secteur bancaire, les évolutions sur les services de paiement portées par la DSP2 sont structurantes et libèrent l'accès à toute la richesse des données qui ne sont plus pour très longtemps le monopole des banques. Cela implique pour elles, a minima, une adaptation de leur système d'informations et de leur organisation, et pourquoi pas une réorientation d'une partie de leur business model. **La DSP2 est en effet un premier pas vers l'Open Banking.** Elle permet aux banques, sous des obligations règlementaires, d' « API-ser » leur système d'information et à terme d'exposer d'autres API plus variées.

La menace que représentent ces GAFAM fait réagir de nombreux acteurs bancaires qui mettent en exergue l'inégalité règlementaire entre elles et les banques. En effet, les banques sont soumises à de nombreuses réglementations vis-à-vis de l'exploitation des données, des moyens de paiement et autres services financiers. Alors que de leur côté, les GAFAM ont une voie plus dégagée et sont contraintes à moins de réglementations.

FOCUS

FRANCISCO GONZALEZ,

Executive Chairman chez BBVA, dans le Financial Times (05/02/2018): Finance chiefs warn on Big Tech's shift to banking

Francisco Gonzalez, Executive Chairman chez BBVA s'est exprimé récemment sur l'inégalité croissante qui pénalise les banques vis-à-vis des GAFAM. Il demande une règlementation commune à tous les acteurs proposant des services financiers.

« Les autorités doivent ramener de l'ordre dans cet important changement [...] qui pourrait mettre en péril la stabilité financière. Si j'ai besoin d'avoir du capital pour prêter (de l'argent) alors les mêmes règles doivent être appliquées pour tout le monde – y compris les géants du web ».

3. … A L'OPEN BANKING : VERS DE NOUVEAUX MODELES BANCAIRES

3.1.
QU'EST-CE QUE L'OPEN BANKING ?

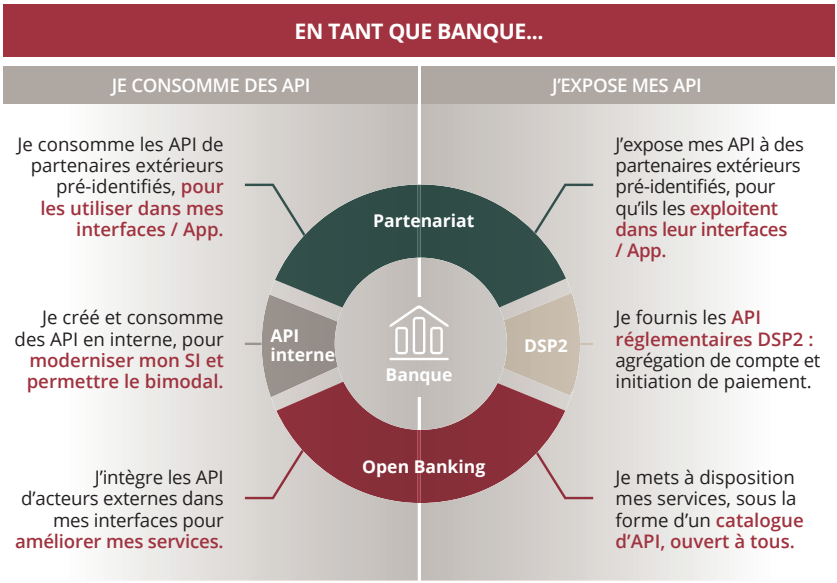
Au-delà des aspects réglementaires qui nécessitent des investissements lourds et obligatoires pour les banques, tant en termes d'organisation que de développement informatique, **la DSP2 mais aussi la RGPD, apportent des opportunités que les banques peuvent saisir,** à condition d'y prêter attention dès maintenant, sous risque de se faire dépasser par de nouveaux intermédiaires.

La DSP2 va transformer en profondeur le secteur bancaire et les services de paiement, favoriser l'arrivée de nouveaux acteurs et ouvrir la voie à des opportunités importantes de développement et d'innovation. Mal préparées et trop souvent moins agiles dans leurs processus et leurs systèmes d'information, les banques traditionnelles ont le plus à perdre de la révolution annoncée. **Elles détiennent pourtant une mine d'informations sur le comportement de leurs clients** mais elles sont davantage freinées quant à l'exploitation de ces données. Elles ne peuvent alors pas en faire bénéficier leurs clients. Cette tendance se confirme par la multitude de nouvelles offres 100% digitales et l'avènement des néobanques (Orange Bank, Compte Nickel, Carrefour Banque, N26, etc.).

L'enjeu de demain n'est plus simplement de détenir des informations clients mais surtout d'en **exploiter intelligemment toute la richesse** pour détenir une image complète et une vision prédictive des clients. Avec les technologies de screen scraping, l'accès aux données bancaires se fera de toute façon, avec ou sans les banques, avec pour elles **le risque majeur de voir se développer un écosystème indépendant.**

Pressées par la DSP2 et les exigences grandissantes des clients, les banques vont à minima devoir ouvrir leur système d'information. Pour se conformer à la nouvelle réglementation, elles auront jusqu'au troisième trimestre 2019, date d'entrée en vigueur des RTS. Elles doivent en parallèle en profiter pour revoir leur modèle bancaire basé sur leur stratégie d'API-sation.

L'ouverture bancaire est un concept regroupant à la fois la consommation et / ou l'exposition d'API. Le schéma ci-contre synthétise les possibilités pour les banques quant à ces deux flux :



Il incombe désormais aux banques de se positionner stratégiquement sur le degré d'ouverture qu'elles souhaitent mettre en place. Du développement en interne d'API à l'exposition totale des services, le spectre est large. Le schéma ci-dessous résume les différents choix stratégiques qui s'offrent aux banques.

Ces modèles permettent d'illustrer les **différents degrés d'ouverture bancaire. Choix aux banques de les moduler, de les mixer,** pour établir leur propre stratégie, conforme à leur vision.

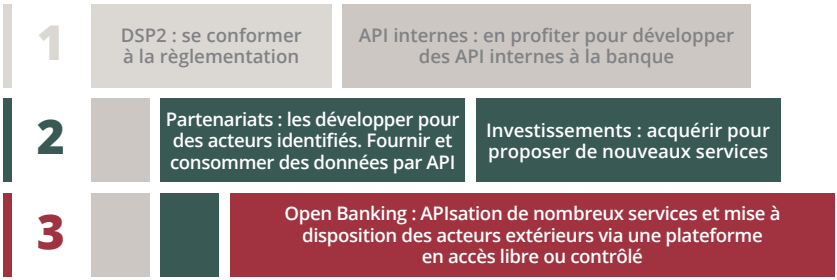
3.2.
MODÈLE 1 : SE CONFORMER À LA RÈGLEMENTATION DSP2 ET EN PROFITER POUR DÉVELOPPER DES API INTERNES À LA BANQUE

Pour répondre à **l'obligation DSP2** d'ouverture des données sur le compte courant, les banques créent leurs API et mettent peu à peu en place des **plateformes d'API management** afin de construire, gérer et suivre leurs API.

Cet investissement peut toutefois être rentabilisé s'il est également utilisé pour un usage interne. Au-delà de la DSP2, les banques peuvent mettre à disposition de l'ensemble des systèmes internes des API sur une plateforme commune et partagée, pour être consommées par l'ensemble des systèmes internes voire par l'ensemble des filiales de la banque. Les API qui ont été développées par la banque sont alors **uniquement à destination de ses systèmes internes.**

A des **fins d'innovation,** ces mêmes API peuvent être partagées avec leurs Labs, facilitant la sortie rapide des projets. La mutualisation des API, disponibles sur une plateforme d'API management,

Les modèles d'ouverture et les stratégies d'API-sation



permet de faciliter les développements. Comme c'est déjà le cas pour certaines entreprises, lors **d'Hackathon,** les développeurs peuvent alors laisser libre cours à leur imagination pour développer de nouveaux services qui consommeront les API existantes et déjà documentées. Côté métier, les analystes peuvent se concentrer sur les problèmes à résoudre plutôt que sur comment les résoudre, puisque le développement sera facilité et normé par les API. Face à la multiplication des FinTech et aux investissements consentis par les GAFAM dans le secteur bancaire, les API internes permettent **d'accélérer le rythme de lancement de services** plus novateurs et d'être plus agile.

Les API internes ne seront pas accessibles pour les autres acteurs externes. Cette solution défensive permet à la banque de rester l'unique interlocuteur avec les clients et d'éviter la désintermédiation pour des services dont les données de base ne seraient ni accessibles via Screen scraping, ni incluses dans la DSP2.

La mise en place de la plateforme d'API management est sans aucun doute **un accélérateur de la standardisation des services informatiques** et de la centralisation des données en un seul réceptacle (big data). Il est envisageable que ce dispositif facilite le respect de la RGPD lorsque le client souhaitera récupérer ou supprimer ses données puisque ses données seront centralisées, structurées et leur récupération facilitée. En effet, aujourd'hui, pour répondre à un client qui souhaite faire valoir ses droits, la banque se voit contrainte de gérer ses données dans une multitude de systèmes informatiques.

Si les API sont un prérequis à l'innovation, c'est bien **toute une organisation qu'il faut transformer** dans l'entreprise : nouveaux outils, nouveaux rôles, nouvelles fiches de poste, nouveaux départements. Les banques ne doivent pas se contenter de mettre en place des cellules d'innovation et espérer que l'innovation en découle. Il reste à **infuser un état d'esprit,** à faciliter les échanges entre les collaborateurs, pour les challenger et les accompagner dans le développement de leurs idées, pour leur laisser le droit à l'erreur. Les collaborateurs sont les plus proches

des problèmes à résoudre, ce sont donc eux les mieux placés pour trouver des solutions. La modernisation apportée par les API au système d'information existant permet un système bimodal. Le système bimodal consiste à conserver les services d'information existants, et à capitaliser sur ceux-ci en y intégrant au fur et à mesure des API. Cette démarche va permettre une meilleure transversalité entre les services, ce qui constitue un vecteur d'innovation interne important pour les banques.

3.3.
MODÈLE 2 : MODÈLE 1 + PARTENARIATS ET / OU INVESTISSEMENT

3.3.1.
Développer des partenariats pour des services identifiés et fournir les données via API

Les API, mises en place pour l'interne, peuvent être exploitées par des entreprises partenaires sélectionnées. Les données clients échangées peuvent être toutes les données hors DSP2 : informations sur les comptes d'épargne, les comptes titres des clients ou d'autres informations de la banque. Les partenaires sont alors engagés contractuellement et de manière spécifique avec la banque propriétaire des données pour l'accès à la plateforme d'API management (liste des API disponibles, documentation) et pour la consommation de ses API. L'exposition des API peut ainsi devenir une source de revenus pérenne pour la banque. De son côté, la banque consomme également les API des partenaires identifiés afin d'intégrer leurs services dans son offre. **La banque s'appuie sur l'écosystème des FinTech** pour faire émerger des services innovants via des partenariats. L'objectif est de pouvoir fournir le service identifié de la FinTech et de travailler rapidement (réduction du time to POC) et conjointement avec un nouveau partenaire. Cette mise à disposition du service de la FinTech par la banque est permise par un échange d'API (la banque fournit ses API / la banque consomme les API de la FinTech).

L'écosystème start-up est en pleine expansion : la France est le 1er pays en Europe en termes de création d'entreprise. Il devient de plus en plus difficile d'identifier les FinTech les plus prometteuses. Pour benchmarker les différentes start-up financières, la banque doit :

1. Être capable d'identifier les FinTech ayant du **succès auprès des clients**

FOCUS

LE CA STORE

Le Crédit Agricole tente une approche unique au regard du benchmark réalisé par Viatys auprès de 147 banques dans le monde : son CA store est la seule plateforme prête à rémunérer des développeurs pour leurs applications qui ont du succès. C'est un moyen d'attirer les meilleurs talents, d'assécher l'offre pour les concurrents et de les fidéliser sur le long terme, avant, peut-être, d'acquérir leur structure ou de racheter leur application.

de la banque, pour développer un partenariat afin d'offrir ce service à succès à ses clients. D'autres offres inédites pourront éventuellement être développées conjointement ;

2. Identifier les **idées les plus originales** portées par des start-up à la recherche de bases clientes importantes et ainsi sélectionner ses futurs partenaires.

Les partenariats ne sont pas circonscrits aux FinTech. A l'instar de l'initiative Wa ! avec Carrefour, des banques n'hésitent plus à s'allier à des retailers, petits ou grands, qui disposent aussi d'informations à valeur ajoutée contenues sur le ticket de caisse. Dans une même application, la banque fournit le moyen de paiement et le retailer les promotions avec des coupons de réduction. Il est en effet indispensable pour la banque d'être proactive et de se positionner cette fois-ci comme fournisseur de services, un partenaire de choix pour récupérer des données client, avant que le retailer ne le fasse par lui-même et monnaye ses données plus durement.

FOCUS

POURQUOI LES BANQUES DOIVENT DÉVELOPPER DES PARTENARIATS AVEC DES COMMERÇANTS ? PARCE QUE LES GAFAM SONT DÉJÀ DANS LA COURSE : L'EXEMPLE D'AMAZON PAY PLACES

L'application Amazon Pay est aujourd'hui installée sur 75% des smartphones américains, celle-ci permet pour l'instant de régler ses achats en ligne après avoir enregistré un moyen de paiement (carte bancaire).

L'objectif d'Amazon Pay Places est de s'étendre au commerce physique. Pour cela une notification permettra au consommateur de savoir que ce mode de paiement est accepté et se verra éventuellement proposé des offres dans le magasin. Le client et le commerçant n'utilisent plus de moyen de paiement physique, ce qui pour ce dernier peut être avantageux lorsqu'on connait le coût de location d'un TPE (entre 18 et 25 euros par mois) et les différentes commissions appliquées à chaque paiement.

Il est plus qu'envisageable qu'avec l'historique des achats, physiques et en ligne, cette application soit capable de pousser des offres ou des produits personnalisés à chaque client permettant aux petits et moyens commerces de bénéficier de publicités ciblées. Associé à un programme de récompenses basées sur la taille d'un panier ou un nombre de transactions passées, Amazon Pay Places pourra jouer sur les deux tableaux pour n'importe quel type de produit (alimentaire, multimédia, vestimentaire, mobilier etc).

Avec Alexa, assistant personnel intelligent, réagissant à la voix, Amazon pourra également notifier les clients, directement chez eux, des promotions en cours ou à venir et, bien entendu, offrir à l'utilisateur d'en profiter directement avec le Voice Payment.

Pour soutenir le commerce traditionnel, pourquoi ne pas s'unir à des FinTech, à l'image de BBVA qui a acquis la start-up FreeMonee. Cette FinTech regroupe la banque avec ses clients disposant d'un moyen de paiement et les commerçants utilisant le fichier client pour leur offrir des réductions et bonnes affaires. BBVA a permis de fidéliser ses clients qui utilisent ses cartes de paiement et offert aux distributeurs traditionnels un moyen de générer du trafic pertinent en boutique tout en permettant de satisfaire le besoin premier des clients : consommer avec de bonnes affaires. BBVA fait d'ailleurs figure de banque pionnière dans l'ouverture bancaire et dans la création de partenariats avec des FinTech. Un autre exemple avec la FinTech Dwolla à qui BBVA a délégué le service de virement inter-compte. Des initiatives françaises comme Lyf Pay (rapprochement des initiatives Wa ! du groupe BNP Paribas et Fivory du Crédit Mutuel) ou encore OrangeCash donnent accès à des réductions auprès d'enseignes partenaires.

3.3.2.

Et / ou réaliser des investissements pour proposer de nouveaux services

Depuis 2014, date du rachat de la start-up américaine Simple par BBVA, on constate une nette **augmentation d'entreprises bancaires investissant dans le capital des start-up financières.** Voici quelques exemples depuis ces deux dernières années :

- BCPE : Lepotcommun.fr, Depopass, e-cotiz, Fidor Bank ;
- Crédit Mutuel Arkéa : Leetchi, Linxo, Yomoni, Grisbee, Pumpkin, Apigee ;
- La Banque Postale : KissKissBankBank ;
- Bnp Paribas : Compte-Nickel, lancement d'un accélérateur de FinTech.

De nombreuses banques sont même allées **jusqu'à créer des fonds d'investissement de capital risque** (Venture Capital) comme Santader Group avec Santander InnoVentures ou BBVA avec BBVA Venture et Probel Venture (les fonds de BBVA sont estimés à 350 millions de dollars).

Ces « mariages » semblent de prime abord contre nature, tant les mentalités et les environnements qui caractérisent ces entreprises sont différents. **Les raisons motivant ces investissements sont pourtant réelles et avantageuses pour l'ensemble des parties.**

Pour les FinTech, l'enjeu principal est de ne pas perdre en agilité, en potentiel d'innovation et de création malgré l'arrivée d'investisseurs. Dans la majorité de cas, elles demeurent des entités indépendantes et conservent

FOCUS

ANA BOTÍN, GROUP EXECUTIVE CHAIRMAN OF BANCO SANTANDER 18 JUILLET 2016 :

" A deeper investment in our FinTech fund represents Santander's success in investing in disruptive new technologies that will help our transformation towards being the best bank for our customers - in the simple personal and fair way they expect and deserve today. "

leur pouvoir de décision. Elles gagnent en **sécurité financière** et peuvent se développer pour continuer à consacrer plus de temps à la recherche d'améliorations et de nouveaux services.

A l'heure où les GAFAM se tournent vers le secteur financier, l'investissement et la collaboration avec les start-up permettent aux banques de **rester dans la course digitale** et de booster leur innovation en acquérant des services déjà en place sur le marché et connus des utilisateurs. Les banques peuvent en profiter pour **absorber le savoir-faire spécifique : technologique et méthodologique.** Tout en élargissant son catalogue de services, la banque garde le contrôle des données qui sont exploitées. La banque gagne en agilité et peut observer les pratiques pour les appliquer à son contexte.

On peut aussi y voir un avantage concurrentiel si la banque acquiert en premier un service novateur. Elle peut revendiquer son dynamisme en étant la première à lancer ou fournir un service. Aussi, elle peut « fixer » un prix de rachat pour les start-up proposant des services similaires.

FOCUS

BBVA COMPASS, GABRIEL SANCHEZ -INIESTA, CHIEF INFORMATION OFFICER :

" API are nothing short of essential to banking's future. They are going to drastically change the way we do banking and banks will have to find their place in the new environment to really besom a winner. "

La banque véhicule une image qui reste en accord avec son temps en promouvant au passage ses partenaires. De même la sélection de nouveaux partenaires peut s'apparenter à la mise sur le marché d'un nouveau service qu'elle n'a pas développé **réduisant significativement son time to POC.**

3.4. MODÈLE 3 : MODÈLE 2 + DÉVELOPPEMENT DE L'OPEN BANKING JUSQU'AU MODÈLE BANK AS A SERVICE

3.4.1. Open Banking : APIsation de nombreux services et mise à disposition des acteurs extérieurs d'API via une plateforme en accès libre ou contrôlés.

La banque dispose de beaucoup plus de données que les FinTech : c'est sa force. Elle peut naturellement se positionner en tant que producteur de données dans un modèle « producteur / distributeur ».

Dans l'Open Banking, la banque détermine les API qu'elle souhaite exposer parmi l'ensemble des API, et donc des données et services dont elle dispose. La banque a alors un rôle clé à jouer dans la chaîne de valeur et devra tenter de garder le contrôle sur la distribution.

Le modèle économique est basé sur une offre de données avec des facturations associées. Les entreprises clientes viendront simplement récupérer les données nécessaires à leur fonctionnement. La banque agit alors comme un tiers de confiance et stocke de manière sécurisée les données du

client, à charge pour lui de déterminer à quelles entreprises il fournira les autorisations d'accès.

48 %
des banques disposent d'une plateforme d'API Open Banking
Benchmark Viatys réalisé sur 147 banques dans le monde

De nombreux établissements bancaires ont d'ores et déjà opté pour ce modèle (BBVA, DBS, Citibank, Crédit Agricole, ...) et ont construit un catalogue d'API en accès libre ou contrôlé. Ainsi, les acteurs extérieurs peuvent venir consommer ces API et les implanter sur leurs plateformes. Par ce modèle, les banques étendent de manière exponentielle leur réseau de distribution, leurs points d'entrée.

3.4.2.
Une ouverture bancaire poussée à l'extrême, un positionnement assumé vers le Bank As A Service

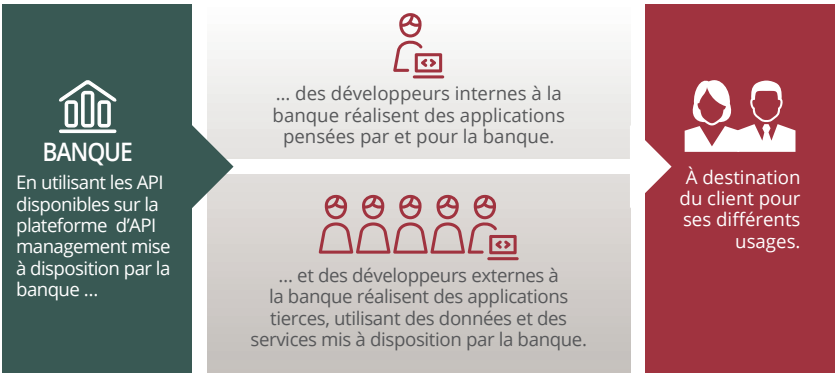
Certaines banques ont opté pour une ouverture totale de leurs données et assument un positionnement de back office. Cette solution est une nouvelle vision de la banque dite « Bank As A Service » qui fournit ses données via des API à toute entreprise souhaitant y accéder. Le modèle économique reste le même que pour l'Open Banking avec un spectre de données plus important.

Les possibilités offertes aux développeurs et aux start-up externes sur l'écosystème de la banque sont quasiment infinies. Elles peuvent favoriser la création de communautés d'experts externes plus larges, prêtes à développer spontanément des services basés sur ces API.

Si la banque devenait un back office, la contrainte majeure serait d'assurer et d'assumer ce rôle de tiers de confiance non seulement auprès des différents organismes de règlementation mais également auprès des clients. La moindre faille aurait alors des conséquences catastrophiques sur la confiance accordée par les utilisateurs.

D'aucuns souhaiteraient que ce modèle fasse de la banque un simple back office. Les banques seraient alors dépourvues de la relation avec le client, portée alors par les différentes FinTech.

L'écosystème de l'Open Banking



FOCUS

LA TRANSFORMATION DIGITALE DE BBVA

Entamée par une grande majorité des banques, BBVA semble être l'une des plus avancée dans son processus de transformation digitale. La prise de conscience date de 2006 et de la déclaration de Francisco Gonzalez dans laquelle il considère que **son principal concurrent est ... Google.**

Depuis **BBVA a constitué deux fonds d'investissement** de 100 millions de dollars en 2013 avec BBVA Venture et 250 millions de dollars en 2016 avec Propel Venture. La transformation digitale ne signifie pas uniquement l'investissement dans des projets novateurs mais consiste aussi à opérer une mutation en interne, ce pourquoi BBVA a investi près de 3 milliards d'euros pour y parvenir.

Plus récemment, le 24 mai 2017, BBVA a lancé **sa plateforme « Open Banking »** avec 8 API pour commercialiser ses données auprès d'entreprises tierces.

BBVA a su s'imprégner de ce nouveau modèle. Cette stratégie a eu le mérite de **faire connaitre sa marque bien au-delà de ses territoires** d'implantation en plus de lui apporter une **image innovante.**

Un cercle vertueux peut ainsi être mis en place : plus est véhiculée une image innovante, plus sont fournies des API performantes, **plus les développeurs du monde entier veulent concevoir des services avec les données disponibles.** Ces mêmes développeurs deviennent de facto de réels ambassadeurs de la marque et des utilisateurs captés. Les montants alloués à la promotion de la banque peuvent ainsi être investis dans le corporate funding. La stratégie du développeur, ambassadeur de la marque, n'est pas sans rappeler l'histoire d'Apple avec les applications mises à disposition sur l'IPhone.

La banque ne pourrait plus pousser ses offres directement au client et serait désintermédiée. C'est sans compter sur les besoins des clients, les capacités des banques à se conformer au réglementaire et à la richesse dont elle dispose : la donnée client. « Bank As A service » ne signifie pas qu'il faut nécessairement renoncer à la relation client.

3.4.3.
Jusqu'à imposer sa norme

Face à ces nouveaux challenges, l'attitude des banques britanniques vis-à-vis des calendriers DSP2 et RTS est notable. Keep Calm and Carry On (« Restez calme et continuez ») : plutôt que d'attendre la réglementation, un consortium, l'« Open Banking Working Group » a décidé d'aller au-delà de la DSP2. L'objectif du groupe est de proposer une norme commune pour les API, à l'image du W3C qui régit les normes pour Internet. Cette initiative n'est pas isolée. Plusieurs groupes de travail sont à l'œuvre pour construire des API bancaires et les proposer à d'autres.

Pourquoi ne pas devenir le chef de file de l'open banking : **définir la norme commune et diffuser les bonnes pratiques autour des API ?**

3.5.
QUEL MODÈLE DE RÉMUNÉRATION ?

Les API DSP2 sont mises à disposition gratuitement des AISP, PISP et PIISP. Pour rentabiliser ces coûts de conformité, la

banque peut utiliser le socle d'API pour des API en interne (modèle N°1). Elle pourra aussi réaliser des gains suite à l'utilisation par ses clients des nouveaux services réalisés avec les API.

Si elle s'inscrit dans l'ouverture vers l'extérieur (modèles n°2 et n°3), la banque devra définir le modèle de rémunération des API hors DSP2.

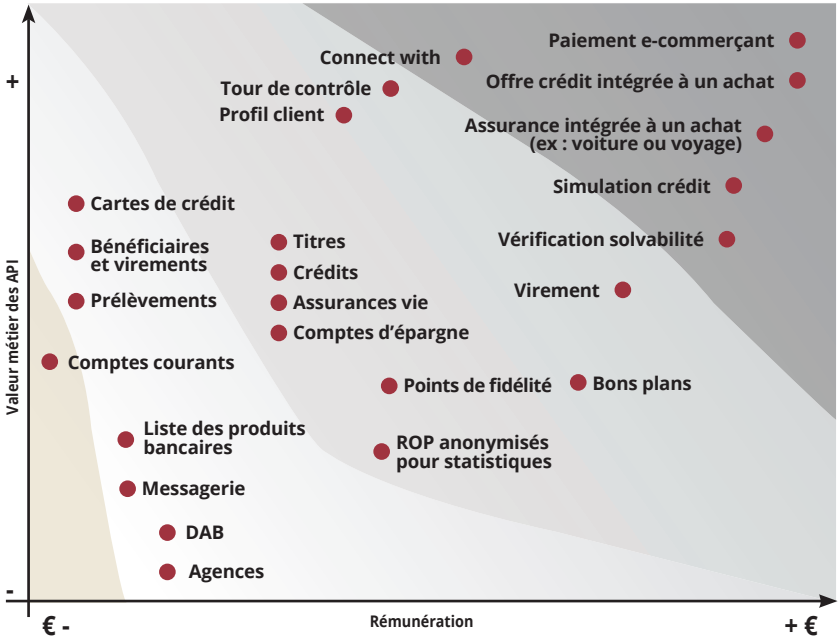
La première étape sera alors de **définir les API qui pourront faire l'objet d'une rémunération** selon la valeur métier qu'elles représentent. Une API sans réelle valeur ajoutée pourrait être mise à disposition de tous les acteurs sans nécessairement faire l'objet d'une rémunération. **Plus la valeur métier de l'API sera grande, plus la rémunération sera élevée.**

La rémunération est composée :

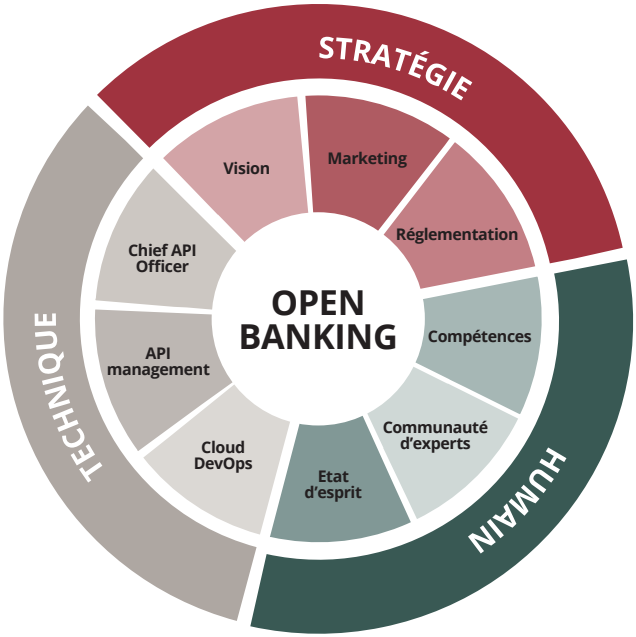
- **d'un montant fixe :** abonnement mensuel, sorte de droit à l'entrée, pour consulter la plateforme d'API management avec la liste des API et la documentation. Nombreux sont les acteurs qui aujourd'hui laisse cet accès gratuit. C'est d'ailleurs un moyen de donner aux développeurs l'envie de consommer les API.
- **d'une rémunération à la consommation d'API :** selon le nombre d'utilisateurs (inscrits ou actifs) ou alors selon le volume d'appels, avec des tarifs dégressifs.

La plateforme API management permet de monitorer et de savoir précisément qui consomme les API et le volume de consommation. La plateforme d'API management est donc un prérequis indispensable pour la facturation.

Exemples de rémunération d'API selon la valeur métier



3.6.
LES POINTS D'ATTENTION POUR TRANSFORMER UNE BANQUE QUI SOUHAITE S'INSCRIRE DANS L'OPEN BANKING



Au choix de la stratégie s'adosse des **changements** pour transformer la banque.

LES CHANGEMENTS DE STRATÉGIE :

Vision

- Construire une vision concrète de la banque de demain à un horizon raisonnable et de sa place dans la chaine de valeur client - start-up.
- Définir le modèle de rémunération des API.
- Créer des **cellules de veille des start-ups et FinTech.**
- **Impliquer l'exécutif** pour permettre des partenariats et investissements rapides.

Marketing

- Développer le rôle du **marketing** dû à l'augmentation du rythme de lancement de nouveaux services et d'offres associées.
- Montrer l'exemple et lancer **ses propres applications** utilisant les API.
- Faire la **promotion des applications extérieures** qui utilisent les API pour inciter à rejoindre la communauté d'experts.

Réglementation

- **Veiller à la réglementation et à la mise en conformité.** L'Open banking rend le respect des contraintes règlementaires d'autant plus primordial

(RGPD, E-Privacy) sachant que la création de données engage la responsabilité de l'entreprise vis-à-vis de tous ces usages même s'il est fait par des tiers.

DES CHANGEMENTS DANS LA GESTION DE L'HUMAIN :

Compétences

- Développer les **compétences internes** des développeurs pour créer et gérer les API.
- Etre **à la pointe** des dernières technologies pour attirer les meilleurs talents issus des GAFAM et FinTech.

Communauté d'experts

- Créer une communauté d'experts avec des développeurs externes **promoteurs de vos API.**
- **Associer les collaborateurs** aux communautés d'experts.
- **Favoriser l'échange** entre interne et externe, autour d'évènements en présentiel sur des sujets challengeants, avec de vrais partages d'expertises.
- **Délivrer rapidement** des API pour améliorer leur fonctionnement et alimenter la communauté.

Etat d'esprit

- **Promotion interne de l'innovation** grâce au partage d'information via API.
- Mettre en place des **Labs ou autre incubateurs de projets** à booster (cf. BNP Paribas People's Lab pour créer des intrapreneurs).
- **Former les collaborateurs** aux nouvelles **méthodologies** comme le Lean, l'Agile, ou le Google design sprint (comment passer d'une idée à un MVP en 5 jours).
- **Acculturer les collaborateurs** au nouvel état d'esprit avec le « droit à l'erreur » induit dans le management de projets innovants.

DES CHANGEMENTS DANS LA GESTION DE LA TECHNIQUE :

Cloud et DevOps

- Moderniser le système d'information vers le Cloud pour optimiser les coûts.
- Opter pour des méthodologies DevOps pour le déploiement en continu des services.
- Revoir l'architecture pour assurer un niveau de **disponibilité** et de **performance** équivalent à celui proposé à ses propres clients. La banque doit être capable de fournir une réponse instantanée.

API management

- Mettre en place une **plateforme d'API management,** qui mettra à disposition les API et la documentation générale sur l'interface.
- La plateforme doit notamment être capable de suivre le cycle de vie de l'API, de contrôler les applications qui utilisent vos données et de suivre l'utilisation.
- Mettre en place une **équipe dédiée au suivi des API.**

Chief API Officer

- Désigner un Chief API Officer. Il sera notamment responsable de communiquer la **roadmap API.**
- Véritable chef d'orchestre, il aura la charge de **prioriser** l'ensemble des services à API-ser et d'en assurer la **cohérence** et la standardisation.

3.7.

OPEN BANKING : QUELLES SONT LES BANQUES LES PLUS AVANCÉES ?

Exemples de dix banques ayant entamé des transformations importantes en termes d'APIsation et d'ouverture bancaire :

BBVA
Multiples partenariats avec diverses FinTech et mise à disposition de nombreuses API.

THE BANCORP
Position de back office assumée. Ouverture totale par API.

DBS
Plus grosse digitalisation bancaire de ces dernières années. Catalogue d'API disponible (+150 API).

CRÉDIT AGRICOLE
Pionnier de l'ouverture bancaire en France avec son CA Store, API ouvertes aux développeurs. Nombreux services API-sés.

HSBC
Mise en place de nombreuses API et partenariats avec des FinTech.

STARLING BANK
Néobanque britannique. Catalogue d'API libre et gratuit. Stratégie d'ouverture bancaire totale par API.

FIDOR (GROUPE BPCE)
Néobanque proposant une place de marché de services libres et gratuits par API.

CITIBANK
Exposition de ses services (quasiment dans leur totalité) via API sur une plateforme ouverte aux développeurs.

SAXO BANQUE
Architecture ouverte auprès des FinTech, catalogue d'API ouvert et disponible.

AXA BANQUE
Mise en place d'une plateforme d'API ouverte dans la lignée de ce qu'a fait AXA assurances.

4. POUR QUELLE RELATION CLIENT ?

4.1.
LES API ET LE BIG DATA AU SERVICE DE L'INTELLIGENCE ARTIFICIELLE

On nous prédit de plus en plus d'intelligence non humaine basée sur des algorithmes de machine learning. **Ces intelligences consomment les données structurées (Big Data) et mises à disposition via des API.**

Par les analyses des données client avec des algorithmes poussés (« Analytics »), il est possible d'offrir des **services personnalisés** et des **offres parfaitement ciblées,** voire de **prédire** les comportements et donc les besoins des clients (machine learning).

De façon plus basique, les clients sont désormais habitués à recevoir des notifications, qui, grâce aux algorithmes seront de plus en plus personnalisées (PFM ou crédit personnalisés). DBS, par exemple, a lancé à Singapour sa plateforme de vente de véhicules d'occasion à laquelle elle a naturellement adossé des simulateurs pour connaître les capacités d'emprunt. S'il s'agit d'un MVP, la capacité d'emprunt est d'ores et déjà **mise à jour automatiquement** selon la navigation du client. Par la prédiction de votre comportement, des outils de PFM seront capables de vous proposer une gestion optimisée de votre épargne.

Pour leur **Service Client, des banques expérimentent déjà les assistants vocaux et autres Chatbots,** qui peuvent être considérés comme la partie émergée de l'intelligence artificielle. Wells Fargo a par exemple lancé son expérimentation en avril 2017 auprès de 5000 clients et collaborateurs. Cet agent conversationnel répond à des questions sur les comptes courants et les comptes carte et est capable de préciser la localisation des agences et des distributeurs. Il est aussi doté de capacités d'apprentissage (langage, contexte). **Il est indéniable que l'intelligence artificielle multiplie les interactions avec le client, en donnant au client un accès plus rapide à des informations.**

FOCUS

LLOYD BLANKFEIN, CEO DE GOLDMAN SACHS EN 2015 :

"You know, it's very ... when you ask about technology in our own industry, I'd like to point out that we're obviously a key player within our industry. We have something like 35,000 people in the firm; something over 9,000 of them are in technology. So when you ask me how is technology ... what might this technology be doing to disrupt the industry or our company, it's a little bit of a funny sentence. Because we are a technology company. So ..."

Pour faire évoluer leur modèle, **il appartient aux banques d'oser suivre les possibilités de l'intelligence artificielle :** exploiter tout le potentiel de la donnée structurée en Big data, tout en respectant le cadre réglementaire (RGPD). **Les banques auront fort à faire avec les nouvelles technologies.** Lloyd Blankfein, CEO de Goldman Sachs le précisait dès 2015 : « We are a technology company », car elle disposait déjà à cette époque de 9000 ingénieurs et développeurs, presque autant que le nombre d'employés Facebook la même année (10 000 en 2015).

Oser suivre la technologie. C'est d'ailleurs le message porté par Peter Thiel, co-fondateur de PayPal, dans son ouvrage « Zero to One: Notes on Startups, or How to Build the Future ». Peter Thiel fait l'éloge du progrès vertical, qui consiste à faire un saut technologique, plutôt qu'un progrès horizontal, qui se limiterait finalement à copier la concurrence. Dans le progrès vertical, l'objectif est que la technologie créée soit une solution dix fois supérieure à son plus proche substitut.

La banque doit se tourner vers la technologie pour offrir plus et mieux à ses clients et ce n'est pas la seule transformation nécessaire.

4.2. LA NÉCESSAIRE TRANSFORMATION DES BANQUES POUR REVOIR L'EXPÉRIENCE CLIENT

Certaines banques font parfois un examen de conscience. C'est le cas de DBS à Singapour. DBS a étendu ses services pour accompagner le client au travers de sa vie et pas uniquement au travers de ses besoins financiers. **DBS a su s'inspirer des techniques des GAFAM avec son slogan « avec vous de A à Z » et est notamment réputée pour son expérience client et son service après-vente.** Alors consciente de ces lacunes, DBS a choisi de devenir un facilitateur et de ne pas freiner les nouveaux usages.

Chez DBS, les clients sont encouragés à utiliser des nouveaux services et la banque s'efforce de devenir invisible. La métrique portée par cette transformation digitale n'était plus le revenu moyen par client mais le « customer hour ». Plus DBS fait gagner du temps à ses clients, quelle que soit la démarche, bancaire ou non, plus DBS

gagne en satisfaction. En moins de 3 ans, DBS est passée de la banque la moins appréciée à la banque n°1 en termes de satisfaction client à Singapour.
C'en est fini des files d'attente au guichet DBS. Avant de se rendre à l'agence, le client envoie un SMS avec le message « Q », pour « Queue » (file d'attente). DBS lui demande le motif de sa venue. Selon la raison de sa venue, le client reçoit à la fois des indications pour procéder par lui-même (Selfcare) et son numéro d'attente dans la file pour être reçu en agence. Le SMS suivant lui indique même à quel numéro de guichet se rendre.
Afin de se transformer en profondeur, DBS a lancé un POC à taille réelle. A partir d'une feuille blanche, elle a ainsi créé une nouvelle filiale en Inde, avec un tout nouveau système d'information permettant de supporter la nouvelle expérience client souhaitée. Les tests concluants peuvent être déployés à la structure historique.
Pour remettre à plat leur modèle, les banques doivent dès à présent **analyser la relation client** et les points de contacts (**Touchpoints :** ensemble des moments où la banque et son client échangent des informations, fournissent et consomment un service ou manipulent des transactions). **Les points de frustration** des clients pourront alors être identifiés. En partant des problèmes rencontrés par les clients, et en définissant **des solutions à partir des problèmes,** les banques pourront alors inventer des services innovants. La banque devra revoir radicalement la manière de réaliser le projet pour être **plus centrée sur les besoins et les problèmes des utilisateurs à résoudre.**

FOCUS

FORRESTER, GLOBAL MOBILE BANKING BENCHMARK, 2017

" Become Customer-Obsessed And Mean It !

Many banks claim to be customer-obsessed, but just a handful are. Becoming customer-obsessed is not about focusing on adding new mobile banking functionality; it is about putting customers at the heart of what the bank does "

4.3. UN PARCOURS CLIENT VECTEUR DE NOUVEAUX SERVICES GRÂCE À L'API FIRST

4.3.1. Que signifie cette notion d'API First ?

Pour Viatys, quand nous évoquons le concept d'« API First », cela ne correspond pas à la technique de développement, mais bien à un nouvel usage, au même titre que le « Mobile First », cette fois-ci autour des API. Cela signifie que les entreprises doivent en priorité utiliser et créer des API.
L'idée est de fluidifier les échanges de données, qu'ils soient plus rapides et plus sécurisés, pour, in fine, enrichir les

parcours client. En effet, l'API a le grand avantage d'échanger ses informations en temps réel.

4.3.2.

Quels nouveaux services et quels avantages pour les banques et le client ?

Si l'on se place du côté de la banque, ce nouvel usage va permettre de proposer des services enrichis et personnalisés au client.

Par exemple, lorsqu'un client effectue un achat sur un site e-commerce, il pourrait lui être proposé de l'assurer avec telle mensualité et par tel assureur, en temps réel et directement sur le site e-commerce. Si plusieurs assureurs mettent à disposition des API, le client pourrait même comparer les prix des assurances.

Un autre exemple, toujours lors d'un achat sur une plateforme e-commerce, serait de présenter au client un plan de financement avec telle banque, toujours en temps réel, et directement sur le site e-commerce.

Ces exemples sont rendus possibles grâce à l'intégration d'API de banques ou d'assurance au sein de plateformes marchandes.

L'API First permet ainsi pour les banques d'accéder à deux nouveaux leviers de croissance :

- Un levier interne, avec la modernisation des systèmes d'information, parfois vieillissants des banques,
- D'un point de vue externe, l'usage croissant d'API peut décupler les opportunités business pour les banques. Le réseau de distribution d'une banque va croître à mesure que ces API seront exposées et consommées par des tiers.

La banque garde totalement la main sur la consommation de leurs API par les tiers. Ce contrôle les prémunit d'être dépossédées de leurs données puisque les tiers ne viennent que consommer les API ciblées des banques.

De son côté, le parcours client sera enrichi avec l'accès à des services, en temps réel, de la banque depuis des plateformes tierces. Ce parcours augmenté, rendu possible via les API, permettra de fournir des services personnalisés au client.

4.3.3.

Quels impacts sur la sécurité des données ?

Côté sécurité, le fonctionnement même d'une API augmente la sécurité quant à l'exploitation des données. Les données échangées sont ciblées dans une API, contrairement au screen scraping qui collecte des données plus massivement.

De plus, avec la nouvelle règlementation DSP2,le client devra donner son accord aux tiers utilisant ses données, avec un renouvellement de cet accord a minima tous les 90 jours.

4.4.

LE CLIENT DE DEMAIN, DIGITAL NATIVE, SOUHAITE LUI AUSSI PARLER À AUTRE CHOSE QU'UN ROBOT ET VEUT QU'ON L'ACCOMPAGNE AVEC UNE RELATION HUMAINE

4.4.1.

Le client a changé ?

Si la génération Y focalise autant l'attention, c'est qu'à l'échelle de la planète 50 % de la population a moins

LA GÉNÉRATION Y :

15,4 MILLONS

Nombre d'individus actuellement en France, nés entre 1980 et 2000, et donc appartenant à la Génération Y

50 %

Proportion de la génération Y dans le nombre d'actifs en France en 2025.

de 30 ans. Elle représente en France 15,4 millions d'individus, nés entre 1980 et 2000. En 2025, cette population représentera environ 50% des actifs en France. C'est dire si les entreprises doivent dès à présent en comprendre les particularités et leurs attentes en tant que clients, car ils vont devenir la norme. Cette génération est la première génération numérique, qui a une maitrise intuitive des appareils portables.

En tant que client, le Y est :

- **Renseigné** et exigeant ;
- Adepte de **l'économie collaborative**, du commerce social ;
- Rompu à **l'instantané** : il est adepte du chat, plus encore que du click to call ;
- A la recherche de **plaisir immédiat** : il souhaite trouver immédiatement les informations qu'il cherche ;
- Habitué à la **gratuité** ;
- Promoteur / **Ambassadeur des marques** sur les réseaux sociaux.

Comme pour les autres générations, celles que certains appellent les « Digital Naïves », ne deviendront pas clientes d'une banque uniquement pour une offre débloquée à l'ouverture d'un compte mais bien parce que le service sera à la hauteur de leurs attentes. Leurs attentes sont fortement inspirées

FOCUS

EN FRANCE ON PARLE DE « DIGITAL NAÏVE ».

Selon Emmanuelle Duez – The Boson project la génération Y est symptomatique du monde qui évolue autour d'elle:

C'est la 1ère génération post moderne, c'est-à-dire pour laquelle le futur est plus sombre que le passé. La génération Y a vu la génération de leurs parents souffrir du chômage. Le Y est **pragmatique, individualiste, court-termiste.** Il attend de son employeur de l'épanouissement professionnel (sens, transparence, engagement). Il reconnaît la légitimité mais pas le statut. Il cherche le sens. L'entreprise doit montrer ce qu'elle a à apporter pour que le collaborateur voie s'il a envie de s'engager.

- **C'est la 1ère génération mondialisée et interconnectée, la 1ère génération du numérique.** Le numérique est vu comme un propre langage et pas seulement comme un outil. C'est une génération **zappeuse et multitâche, impatiente et dans l'instantanéité.**
- C'est la prochaine **grande génération.** 50% de la génération mondiale a moins de 30 ans. Les comportements de la génération Y dans l'entreprise vont devenir la norme.
- C'est la **1ère génération omnisciente,** qui dispose d'un ensemble d'informations dans son smartphone, avec le savoir à portée de clic.
- Pour cette génération, c'est **l'agile qui mange l'inerte.**
- Elle sera porteuse d'un nouveau modèle de société.

de leurs habitudes digitales cultivées auprès des GAFAM.

Le client de demain, sera connecté et renseigné. Il aura choisi sa banque au travers d'un comparateur. Il ne souhaitera pas payer pour des services qu'il peut avoir gratuitement par ailleurs. Il ne comprendra pas qu'il n'est pas possible de chater avec le Service Client.

La génération Y est considérée comme difficile à fidéliser. Si sa banque ne le satisfait pas, il aura à sa disposition un facilitateur en la loi Macron portant sur la mobilité bancaire : cette loi permet depuis février 2017 de transférer automatiquement les virements et prélèvements en quelques semaines vers sa nouvelle banque. A cette possibilité s'ajoutera demain, avec la RGPD, la mobilité des données.

4.4.2.

Même le digital native souhaite parler à autre chose qu'un robot et veut être accompagné par une relation humaine

De plus en plus de services pourront être fournis par des « robots ». Mais **dans l'expérience utilisateur, la banque n'est pas un simple commerçant. Tout ne se digitalise pas,** même pour les la génération Y habituée au digital.

DBS l'a bien compris et a su s'adapter à son client. Dans l'exemple du SMS, DBS offre ainsi le choix au client d'évaluer s'il est capable de réaliser par lui-même des actions bancaires selon ses connaissances personnelles, ou s'il préfère être accompagné. **Le digital est en effet un canal essentiel pour optimiser le service bancaire mais il ne doit pas être le seul.** A certains moments de sa vie, un client même rodé au digital, peut ressentir le besoin de se faire accompagner (premier emprunt immobilier, premier investissement, décès d'un proche).

Des FinTech peuvent proposer du conseil en patrimoine, comme la Finbox par exemple. Mais si le client n'a jamais réalisé d'investissement, il se retournera invariablement vers son banquier, seul humain à sa disposition, qui **saura plus expliquer en face à face** les tenants et les aboutissants de son investissement.

Pour améliorer l'expérience client, BBVA pense qu'il faut **faciliter l'accès à un conseiller bancaire** pour ses clients. C'est dans cet esprit que BBVA a lancé sa fonctionnalité Click to call permettant d'accéder à son conseiller ou à son Service Client directement depuis son application Smartphone.

Si, aujourd'hui, le fait d'avoir un interlocuteur privilégié et identifiable en la personne du conseiller client, est un élément clé du climat de confiance, il n'en reste pas moins que les mentalités sur la relation humaine entre un client et son conseiller sont en cours d'évolution. On peut définir ainsi 4 enjeux :

1. **L'interactivité :** chaque client souhaite aujourd'hui être considéré comme un individu à part entière et ainsi se voir proposer des services personnalisés intervenant à des moments opportuns dans sa vie.
2. **La collaboration :** les utilisateurs fournissent volontairement de plus en plus de données et les entreprises disposent des moyens de les stocker mais surtout de les exploiter à l'aide du Big Data. Cette technologie doit aujourd'hui permettre d'analyser en temps réel les usages des clients

et pouvoir ainsi leur répondre rapidement.

3. **La prédictivité :** l'analyse de données récoltées doit permettre d'anticiper les futurs besoins et interrogations d'un client pour fournir des réponses adaptées à sa situation.
4. **L'immédiateté :** le conseiller doit être capable de répondre rapidement aux demandes du client. L'attente suite à des réclamations ou des souscriptions est de moins en moins tolérée par les clients bancaires. Pourquoi attendre quelques semaines pour l'ouverture d'un compte en ligne, alors que par ailleurs des néobanques offrent des moyens de paiement dès la souscription ?
5. **La continuité :** le client souhaite pouvoir poursuivre un achat ou une souscription à une offre en changeant de canal (smartphone, tablette, web, service client, agence).

Alors comment fidéliser ou conserver ses clients alors que ceux-ci sont de plus en plus nomades et que les nouvelles réglementations vont faciliter leurs velléités de départ ? Le constat de Paul Cobban, Chief Data and Transformation Officer de DBS est sans appel. Ce constat a été réalisé à la suite d'une expérience qui a consisté à mettre le Président de DBS au téléphone avec des clients mécontents, comme le fait le CEO d'Amazon, Jeff Bezos, chaque année.

Un client aspire à 3 éléments dans sa relation avec une banque :

1. **Gagner du temps**
2. **Pouvoir entreprendre facilement ses démarches bancaires**
3. **Être suivi et écouter par son conseiller bancaire**

Cette expérience donne une image plus humaine de l'entreprise et plus proche de ses clients. Cette approche plus humaine du digital se retrouve dans la campagne de publicité du Crédit Agricole pour qui **« le digital ne signifie pas la fin de l'humain »**.

Le nouveau modèle de DBS place le consommateur au centre des préoccupations, l'entreprise doit ainsi **faire preuve de compréhension et d'empathie** vis-à-vis de ses clients. Les notions de réseau, de collaboration, de communauté, et d'ouverture doivent être prises en compte dans la création de nouveaux services. Qui mieux que le conseiller pour faire preuve de qualité humaine ?

Il est à noter que la part de clients n'ayant qu'une banque 100% mobile (Hello Bank, Boursorama…) est relativement faible. Ces clients sont souvent multi bancarisés avec des banques traditionnelles pour relation principale.

4.5. LA BANQUE RESTE UN PARTENAIRE DE CONFIANCE PRIVILÉGIÉ

Une étude de novembre 2016 produite par CSA Research pour le compte de BNP Paribas rappelle que **2/3 des Français attendent un accompagnement** de leur banque et les **plébiscitent comme premier partenaire de leurs données.** En somme, les Français voient la banque comme interlocuteur de confiance, car les clients savent que, quoi qu'il arrive, les crises financières notamment, les banques persisteront et seront toujours là demain.

+ DE 2 TIERS

des Français plébiscitent les banques comme premier partenaire de confiance pour les accompagner dans la protection de leurs données bancaires (77%) et plus largement, de leurs données personnelles (63%).

Baromètre les Français et le digital : confiance et pratiques par CSA Research

C'est la position qu'adopte actuellement Wells Fargo aux USA en lançant une **« tour de contrôle »** pour les consommateurs de services disruptifs dont ceux des FinTech. Ce tableau de bord permet au client d'avoir, en un clin d'œil, **un état des lieux des services qui accèdent à ses données bancaires,** de savoir depuis quand, dans quel but et de modifier les autorisations d'accès pour chaque service. La banque se positionne tel un facilitateur, à l'image de DBS, tout en permettant une co-innovation à l'image de BBVA. Wells Fargo s'établit en tant que **tiers de confiance**. Par ailleurs, les banques disposent souvent d'une offre de coffre-fort électronique, d'un soutien juridique lorsqu'elles font aussi de l'assurance et d'autres services qui, réunis de manière ergonomique et centralisée, peuvent redonner **un rôle clef dans la chaine de valeur** entre client - start-up – et banque.

Les clients veulent du service digital mais avec une **sécurité**. Alors, pourquoi ne pas les accompagner et devenir tiers de confiance et développer des services innovants liés à l'activité bancaire, comme **une fonctionnalité de « login with »** qui permet de s'inscrire rapidement à un service avec ses identifiants bancaires ? Un moyen peu coûteux de pérenniser la relation client et d'obtenir des informations à 360°.

Le client adepte de ces nouveaux outils fournis par sa banque sera libre d'utiliser tout type de service mais **gardera une attache auprès de sa banque qui sera la garante de ses données, l'informateur de ses droits et le connecteur universel aux autres services.** On confie à la banque son patrimoine, on y dépose ses bijoux et alors que la data est perçue de plus en plus comme un élément de valeur, pourquoi ne pas les confier en garantie à sa banque ? Un client aura du mal à quitter sa banque s'il s'est inscrit avec son identifiant bancaire, au travers d'une API fourni par sa banque, à divers services. **Quitter sa banque reviendrait à quitter immédiatement l'ensemble des services auxquels il a souscrit.**

Amazon, Facebook, Google ont tous une API de type « login with ». Toutefois **les banques garderont toujours un avantage, celui de fournir des informations vérifiées et vérifiables** là où les GAFAM ne peuvent le faire. Il est difficile pour une FinTech d'accepter de s'inscrire avec le profil Facebook de son chat alors que le profil issu d'une banque identifie une personne physique. En faisant ainsi, la banque fournit un moyen de **simplifier encore plus le parcours client** mais se positionne aussi comme un partenaire indispensable à l'ensemble des acteurs.

4.6. CONFIANCE, FIABILITÉ, SÉCURITÉ : DES CHALLENGES AUSSI POUR LES FINTECH, MODÈLES DES PARCOURS CLIENT SANS COUTURE

Les FinTech sont souvent perçues comme les modèles pour les parcours

client réinventés. Elles sont présentées comme une menace pour les banques, pour qui oppose grande structure et structures plus agiles. Cependant, pour perdurer les FinTech doivent aussi faire face à des transformations. Trois challenges principaux qui les attendent :

1. **Confiance :** si les FinTech ont pour ambition de devenir les banques de demain, elles pourront obtenir les autorisations nécessaires. Il faudra néanmoins que le client ait suffisamment confiance pour placer l'intégralité de son argent dans ces nouvelles structures, qui peuvent sembler moins pérennes. La confiance est bien le pilier essentiel à un système monétaire, John Law de Lauriston qui a essayé d'introduire le papier-monnaie en France en 1716 ne nous contredira pas.
2. **Fiabilité de l'infrastructure :** l'infrastructure devra être optimisée pour supporter l'APIsation et être en adéquation avec le service client délivré.
3. **Sécurité des données personnelles :** l'utilisateur devra avoir suffisamment confiance en la FinTech comme garante de la sécurisation de ses données personnelles, et la FinTech devra fournir des moyens d'exercer leurs droits.

Les utilisations massives des réseaux sociaux et des services partagés ont désinhibé le consommateur vis-à-vis de ses données. Obligé d'accorder sa confiance à des services sous peine de ne pas pouvoir les utiliser, l'utilisateur de demain fournira ses données bancaires et personnelles à divers PSP et services.

Ces données seront exploitées pour rentabiliser le service – souvent gratuit – des FinTech ou d'autres start-ups. Cependant, ces entreprises se doivent de respecter la réglementation et notamment permettre de contacter directement la personne en charge de la RGPD (actuellement en charge de la CNIL) ou encore de donner accès facilement à l'ensemble des données d'un service pour les consulter, les modifier ou encore les télécharger pour, idéalement, les utiliser ailleurs.

L'humain reste au cœur du challenge des FinTech puisqu'il s'agira de confiance : sur les données, sur la fiabilité, sur la pérennité de l'entreprise à laquelle le client confie son argent. Ces challenges sont à l'heure actuelle les forces des banques. FinTech et banques ne peuvent s'opposer et doivent s'allier en vue de fournir à l'utilisateur des solutions pour résoudre ses problèmes.

5. COMMENT VIATYS PEUT ACCOMPAGNER SES CLIENTS ?

La DSP2 et l'open banking apportent de profonds changements dans le secteur bancaire, chez les commerçants, les néobanques et les prestataires des services bancaires. Ces évolutions ont de forts impacts opérationnels, organisationnels, technologiques dans les banques et doivent être anticipés et traités.

DIAGNOSTIC

- Décryptages réglementaires (DSP2, RGPD)
- Evaluation des impacts business et techniques de la DSP2 pour votre organisation
- Open Banking : sensibilisation
- Analyse des Touchpoints dans le parcours client et des points de frustration client
- Benchmark maturité Expérience Client
- Analyse Expérience Client des applications Web et Mobile

TARGET OPERATING MODEL

- Audit organisationnel
- Évaluation des ressources et des capacités
- Conception des processus métier (Lutte Anti-Fraude, gestion des réclamations, etc.)
- Change management
- Mobilisation des acteurs

EXPERTISES

- Paiement et monétique
- LAB
- Authentification forte
- API
- Big data

STRATEGIE ET INNOVATION

- Open Banking : stratégie marketing et offres
- Value Proposition Design
- Alternative Business Model
- Mise en œuvre de partenariat avec des FinTech
- Etudes et benchmarks

SCALE PMO

- Structuration de programme DSP2
- Mise en place de programmes Open Banking
- Formalisation de la stratégie du programme
- Définition des objectifs
- Déclinaison en portefeuilles de projets
- Gouvernance et pilotage de la mise en œuvre

LEXIQUE DES ABREVIATIONS

ACTEURS

GAFAM : Google, Apple, Facebook, Amazon, Microsoft

FinTech : start-up financière

OTT : Over The Top

EBA : European Banking Authority, Autorité bancaire européenne

FBF : Fédération Bancaire Française

CNIL : Commission Nationale de l'Informatique et des Libertés

UE : Union Européenne

CE : Commission Européenne

RÔLES

PSU : Payment Service User, Utilisateur de Service de Paiement

ASPSP : Account Servicing Payment Service Provider, Prestataire de Service de Paiement Gestionnaire de Compte

TPP : Third Party Provider, Prestataire Tiers

PSP : Payment Service Providers, Prestataires de Services de Paiement

AISP : Account Information Service Provider, Prestataire de Service de Paiement d'Information de Compte

PISP : Payment Initiation Service Provider, Prestataire de Service d'Initiation de Paiement

PIISP : Payment Instrument Issuer Service Provider, Prestataire de Services de Paiement Emetteur d'Instruments de Paiement

RÉGLEMENTATIONS ET NORMES

RGPD/ RGPD : General Data Protection Regulation

DSP2 : Directive de Services de Paiement n°2

RTS : Regulatory Technical Standards

SWIFT : Society for Worldwide Interbank Financial Telecommunication

CSP : Customer Security Program

NIS : Network and Information Security

AUTRES ABRÉVIATIONS

BAAS : Bank As A Service

API : Application Programming Interface

MVP : Minimum Viable Product

POC : Proof Of Concept

B2B : Business to business

B2C : Business to customer

CONTACTS

VIATYS

JULIEN BORDERIE
Directeur Associé
Mob. : +33 6 24 91 41 22
julien.borderie@viatys.com

VIATYS

AUDREY DHELLEMMES
Senior Manager
Mob. : +33 6 89 32 64 06
audrey.dhellemmes@viatys.com

A PROPOS DE VIATYS

VIATYS accompagne depuis plus de 10 ans les entreprises françaises et européennes, issues de tous les secteurs d'activité, dans leurs projets de transformation organisationnels, transactionnels et culturels en s'appuyant sur des méthodes d'innovation et sur un socle rigoureux de pilotage.
VIATYS se positionne comme un acteur différent et différenciant, maîtrisant tous les codes de rigueur, de méthode et d'engagement que l'on doit trouver dans le monde du conseil, mais souhaitant apporter également innovation, ambition et rupture.
Notre organisation est le fruit d'une aventure entrepreneuriale et humaine, basée sur un modèle managérial de proximité et un suivi permanent des équipes qui permet de garantir une motivation et une implication maximale de chacun au sein du cabinet.

VIATYS

173 avenue Achille Peretti - 92200 Neuilly-sur-Seine
tél. 01 46 40 36 00 - fax : 01 46 40 36 01 - www.viatys.com