Le défi de l'innovation numérique pour les banques : la confiance

www.galitt.com

A propos de Galitt

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

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

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

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

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

Galitt est une société du groupe Sopra Steria. En 2017, elle a réalisé un chiffre d'affaires de 31,1 millions d'euros et employait 260 personnes.

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

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

A propos de ce document

Ce livre blanc s'adresse à l'ensemble des acteurs du secteur bancaire et financier. Afin d'appuyer notre analyse, en plus de l'apport de l'ensemble des compétences de l'équipe Payment Consulting, nous avons réalisé différents travaux de recherche :

- Des recherches règlementaires en nous penchant notamment sur les directives DSP2 et NIS, et règlements RGPD et eIDAS.
- Une veille continue de l'actualité du numérique dans le secteur bancaire et financier grâce, entre autres, à notre lettre de veille BUZZ PAIEMENT[1].
- Des recherches approfondies sur le thème de la confiance dans le numérique, avec notamment la réalisation d'une étude quantitative auprès de plus de 800 personnes représentatives de la population française et issues d'un panel Internet[2].
- De nombreuses interviews d'experts du numérique, de la banque et de la protection des données, permettant d'exposer les différentes opportunités qui sont offertes, que ce soit en termes de nouveaux services ou d'expérience client.

Ce document vise en particulier à :

- Analyser les enjeux de l'innovation numérique dans le secteur bancaire et financier et en proposer une synthèse
- Appréhender le cadre règlementaire européen qui régit le numérique et la protection des données
- Démontrer la position des banques comme acteurs légitimes de confiance
- Identifier l'appétence et les attentes des individus pour de nouveaux services bancaires et financiers
- En déduire des opportunités de services à valeur ajoutée
- L'objectif est de comprendre les défis apportés par l'innovation numérique au sein de l'Union Européenne pour le secteur bancaire et financier et de fournir un éclairage sur les opportunités qui en découlent.

1 Chroniques hebdomadaires de veille sur l'actualité et les innovations en matière de paiement, en 1000 mots réalisée par Galitt.

2 Etude réalisée en juillet 2018 via le Panel To Luna auprès d'un échantillon de 858 personnes représentatif de la population française

Sommaire

A propos de Galitt 2

A propos de ce document 3

Introduction 5

La confiance, un enjeu clé pour les banques 6

1.1. Une confiance entretenue par une relation de proximité au quotidien… 8

1.2. …Et une légitimité acquise par une expertise technique et des savoir-faire métier 11

1.3. Une relation de confiance qui peut être renforcée 13

Un marché en mutation, redéfinissant les tenants et les aboutissants de la confiance 15

2.1. L'identité numérique, nouvel enjeu clé de la confiance dans le monde numérique 16

2.2. Le Règlement Général sur la Protection des Données (RGPD), illustration d'un cadre règlementaire en transformation 19

Quelles opportunités, pour l'organisation et l'offre de service de banques ? 29

3.1. De nouvelles solutions pour la conduite de l'activité des banques, renforçant la sécurité et la protection des données 30

La blockchain, une technologie de mise en conformité RGPD ? 30

La biométrie, une solution pour sécuriser le KYC à distance ? 32

Le CIAM, une nouvelle approche pour une vision client unifiée et sécurisée ? 34

Les API, la « lingua franca » du monde bancaire à l'heure de l'open banking ? 35

3.2. De nouveaux services mettant l'accent sur la confiance 36

Conclusion 45

Introduction

L'ère du numérique confère aux données personnelles une valeur stratégique inédite. La collecte, l'analyse et l'exploitation de ces données, dont le volume a décollé avec l'usage de plus en plus intensif d'Internet, constituent les activités clés d'un marché juteux profitant aux « data brokers » et aux réseaux sociaux.

> Ce marché brille aussi par son opacité : les utilisateurs de ces réseaux, bien que conscients que leurs données soient exploitées, ne connaissent pas précisément les finalités ni l'ampleur de cette exploitation. La découverte, en avril 2018, de l'utilisation à des fins politiques de données de millions d'utilisateurs de Facebook par Cambridge Analytica[3], a mis en lumière le risque de voir ses données personnelles récupérées et exploitées à son insu.

Cette dérive souligne l'importance des sujets de consentement de l'utilisateur et de protection des données personnelles. Aujourd'hui, l'Union Européenne considère ces pratiques comme une violation des droits fondamentaux. Depuis le 25 mai 2018, elle a renforcé les sanctions liées à ce type d'activités avec l'application du **RGPD**[4] *(Règlement Général sur la Protection des Données)*. Dorénavant, les GAFA, et toute autre entreprise, ne pourront plus exploiter gratuitement les données des utilisateurs européens sans avoir obtenu au préalable leur consentement libre et explicite.

Ce règlement vise à restaurer la confiance des utilisateurs envers les services numériques par ailleurs mise à mal par de multiples et importantes failles de sécurité observées ces derniers temps[5]. En outre, la complexité des technologies et leurs usages non maîtrisés viennent accentuer cette défiance, jusqu'à générer un rejet d'une partie des utilisateurs.

L'adhésion aux services numériques par le grand public est donc conditionnée par la confiance que ce dernier leur accorde. Pour le secteur bancaire, la confiance, de par la spécificité des services qu'il délivre, constitue d'ores et déjà un enjeu central. Cet enjeu prend donc une dimension cruciale au regard de la transformation numérique de ce secteur, initiée il y a quelques années, à la fois par la modernisation de ses processus internes et par le renouvellement de son offre de service. Pour les banques, il s'agit désormais de conserver la relation de confiance des clients, tout en saisissant les opportunités des innovations numériques pour la renforcer.

---

3 *Les enquêtes du Guardian et du New York Times ont dévoilé que lors de la dernière campagne présidentielle américaine, le cabinet Cambridge Analytica est parvenu à récupérer le profil et les informations associés de millions de votants américains. Ces données ont été exploitées dans le but d'affiner la stratégie de campagne du candidat Donald Trump.*
Voir l'article du Monde : Comment une entreprise proche de Trump a siphonné les données de millions d'utilisateurs de Facebook

4 *EUR-Lex : règlement RGPD*

5 *Si le dernier cas médiatique concerne Facebook, d'autres très grosses entreprises ont aussi été touchées : Yahoo, MySpace, Ebay, Orange et bien d'autres. Voir l'article du Monde : Cinquante millions de comptes Facebook affectés par une faille de sécurité*

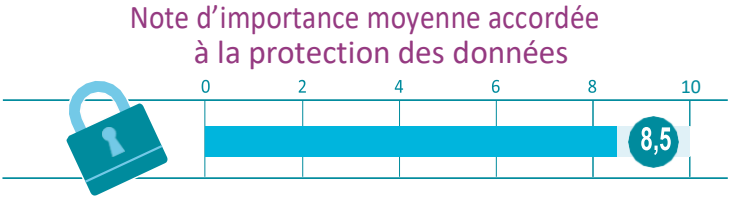
1

La confiance, un enjeu clé pour les banques

Les banques gèrent et protègent les fonds de leurs clients depuis des siècles, s'adaptant au fil du temps aux évolutions technologiques, règlementaires et opérationnelles. L'enjeu du secteur bancaire est à présent de ne pas pâtir du scepticisme ambiant et de la défiance des utilisateurs vis-à-vis des technologies numériques.

L'étude réalisée par Galitt auprès de 800 Français de 18 à 75 ans a permis de recueillir les perceptions des Français sur le monde bancaire, notamment sur des sujets relatifs à la confiance et à la protection des données.

Une grande importance est accordée à la protection et à la préservation des données personnelles avec une note moyenne de 8,5 /10.



Les Français s'avérant sensibles à la protection de leurs données personnelles, le choix de l'acteur chargé de leur protection est donc capital.

A cette question, les Français, toutes tranches d'âge confondues, répondent pour 63 % d'entre eux qu'ils confieraient leurs données personnelles à leur banque de détail. Une proportion deux fois plus importante que le taux de réponses désignant l'Etat français. La banque en ligne vient ensuite dans l'ordre des réponses apportées par les Français, assez loin derrière leurs ainées mais avec un taux intéressant au regard de leur part de marché en France. Notons enfin que 15 % des répondants ne souhaitent confier leurs données à aucun acteur parmi la liste proposée.

Certaines disparités apparaissent selon les tranches d'âges. Les plus jeunes semblent plus enclins à confier leurs données personnelles *(8% des 18-24 ans ne souhaitent pas confier leurs données aux acteurs listés)*, avec moins d'appréhension vis-à-vis des nouveaux acteurs *(17% confieraient leurs données aux néobanques, contre 5% en moyenne)*. Pour les plus âgés, ces logiques de réponse sont inversées.

Les banques de détail ainsi que l'Etat sont les deux acteurs bénéficiant du taux de réponse favorable le plus stable par comparaison des différentes tranches d'âge.

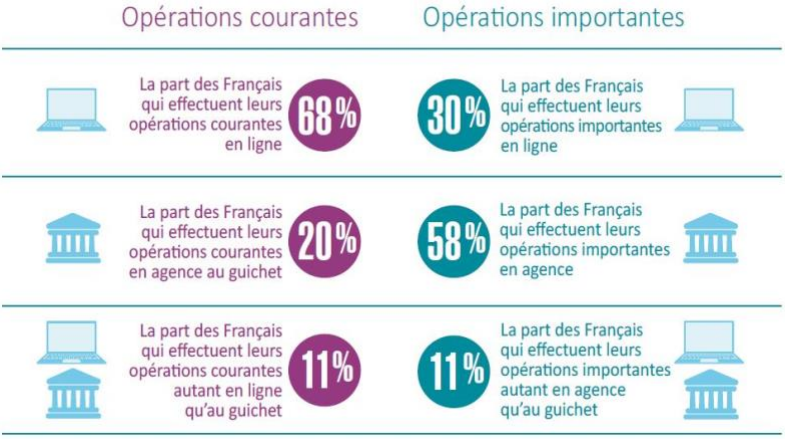
1.1. Une confiance entretenue par une relation de proximité au quotidien…

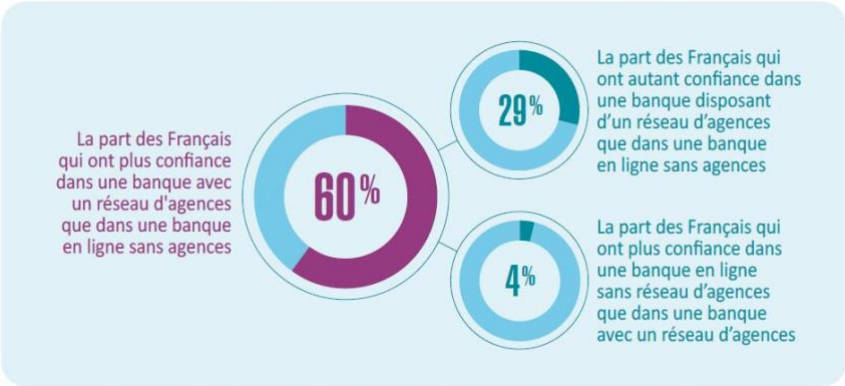
Les banques ont su gagner la confiance de leurs clients au fil des années en les **accompagnant au quotidien**. Elles sont leurs interlocutrices de prédilection lors des grandes étapes de la vie : la souscription d'un prêt étudiant, l'achat d'une voiture, ou l'acquisition d'un appartement ou d'une maison [6].

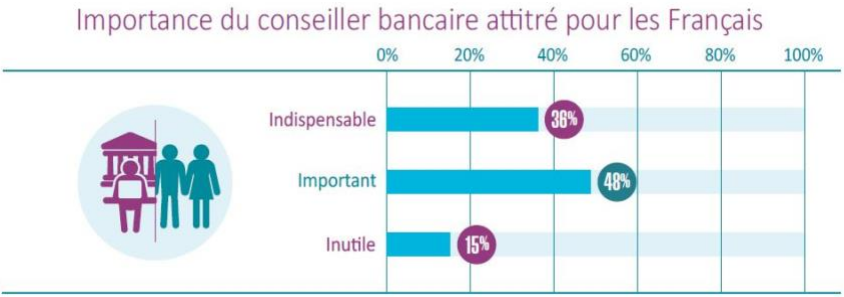
Si 68% des personnes interrogées effectuent leurs opérations courantes en ligne, 58 % effectuent en revanche leurs opérations bancaires importantes, comme la souscription d'un crédit, en agence. **La relation de proximité constitue donc un élément clé de cet accompagnement au quotidien. Il est donc important pour les**

6 *Pour plus de détails sur le cycle de vie du client bancaire, voir le livre blanc Galitt « Le secteur bancaire face au mythe des Millennials : décryptage d'une génération aux multiples facettes ».*

banques de détail de la préserver, d'autant que 60 % des répondants ont plus confiance dans une banque disposant d'un réseau d'agences que dans une banque en ligne sans agences. 84% des personnes interrogées estiment également qu'avoir un conseiller bancaire attitré est important voire indispensable.






Importance du conseiller bancaire attitré pour les Français
0%
20%
40%
60%
80%
100%
Indispensable
36%
Important
48%
Inutile
15%

1.2. ...Et une légitimité acquise par une expertise technique et des savoir-faire métier

La banque de détail possède une véritable expertise en termes de sécurité et de technologies financières. Elle s'est dotée d'infrastructures et de dispositifs technologiques devant permettre de protéger les fonds et les données de ses clients. Tout comme les données d'identité, les coordonnées bancaires sont considérées comme des données personnelles très confidentielles, ce qui, pour les clients, justifie le besoin de protection de ces données.

LES DONNÉES PERSONNELLES

Les données personnelles sont définies dans le Règlement Général sur la Protection des Données (RGP)[7] comme : « toute information se rapportant à une personne physique identifiée ou identifiable ; est réputée être une « personne physique identifiable » une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale ».

Les clients ont par ailleurs confiance dans les moyens de paiement mis à disposition par les banques. En particulier, la méthode OTP *(One Time Password)* SMS utilisée par le protocole d'authentification 3D-Secure, généralisée en 2007, est bien ancrée dans les usages comme une fonction de sécurisation des transactions de paiement e-commerce[8].
En particulier 68% des sondés estiment que la sécurité mise en place par les banques permet de réduire le risque de fraude, et 72% estiment que les mesures mises en place pour s'authentifier en ligne pour un paiement ou un accès à l'espace bancaire personnel sont sécurisées, dont 16% tout à fait sécurisées.

Les savoir-faire métier, en particulier la procédure de KYC *(« Know Your Customer »)* inhérente aux contraintes règlementaires et à la sensibilité des services délivrés, participent à sécuriser la relation avec le client et à légitimer la banque comme acteur de confiance.

LE KYC

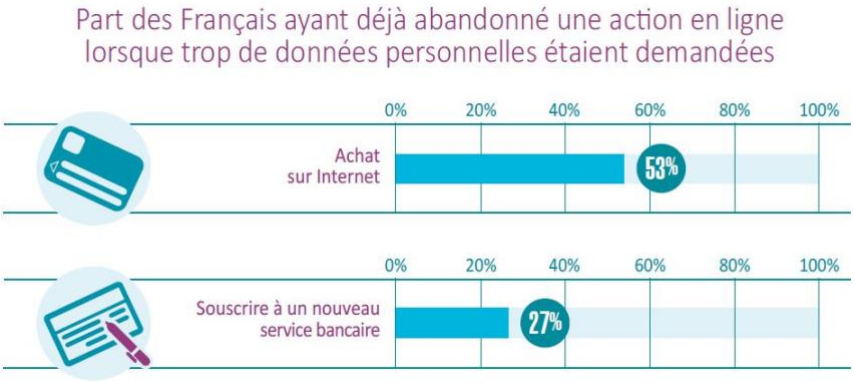
7 *Voir partie 2.2 pour plus de détails*

8 *Selon le Rapport Annuel de l'Observatoire des Moyens de Paiement publié le 1à juillet 2018, 41% du montant total des paiements en ligne sont authentifiés par 3D-Secure*

La transposition française de la directive AMLD4[9] spécifie les attentes en termes de procédure de KYC (« Know Your Customer ») pour les étapes d'identification et de vérification d'identité du client et du bénéficiaire. Le KYC est une procédure de vérification de l'identité consistant en la collecte, l'analyse et la vérification des données personnelles, ainsi qu'à l'évaluation des risques. Dans le cas d'une transaction, les banques doivent effectuer ce processus d'analyse via le KYC pour leur client, mais également pour le bénéficiaire de cette transaction. Certaines banques commencent à proposer des moyens d'identification à distance recourant à la biométrie pour permettre, dans le cadre de la procédure KYC, la vérification d'identité afin de diminuer le risque de fraude par usurpation d'identité. L'objectif est de conserver le même niveau de sécurité qu'une procédure KYC réalisée en face-à-face.

En conditionnant la contractualisation avec un client à une telle procédure, la banque s'assure de la fiabilité de l'identité déclinée par le client. Lors de chaque échange en ligne, celui-ci devra par ailleurs s'authentifier, permettant à la banque de s'assurer que le client est bien la personne qu'elle prétend être. De son côté, cette procédure d'authentification sur la base d'une identité vérifiée rassure le client : il sait que, grâce à cette procédure poussée, c'est lui et lui seul qui a accès à son compte bancaire.

D'après l'étude réalisée par Galitt, pour 69 % des Français, cette procédure poussée n'est pas une source d'abandon à l'ouverture d'un compte bancaire, même si les données demandées sont nombreuses. A l'inverse, 53 % des personnes interrogées ont déjà renoncé à un achat sur Internet car l'entreprise demandait trop de données personnelles.

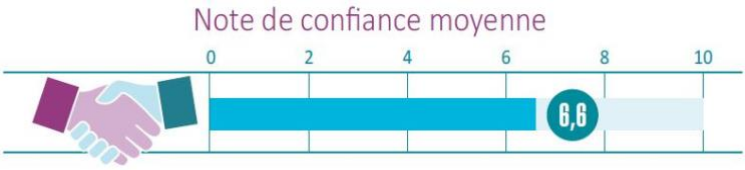


9 *Voir partie 2.2 pour plus d'éléments relatifs à AMLD4*

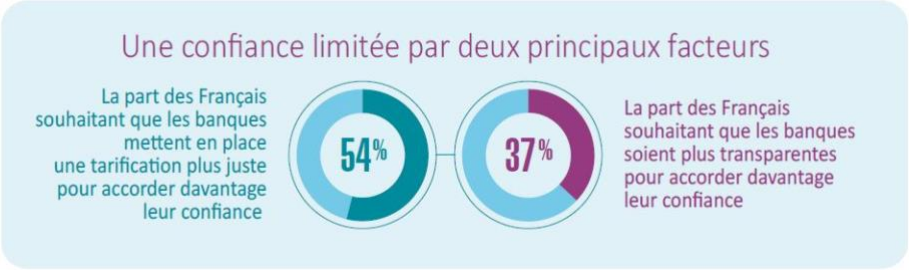
Les Français, dans le contexte d'un processus de souscription nécessitant de nombreuses données personnelles, accordent plus d'importance et ont plus confiance dans les banques que dans les acteurs du web en général. Cette méfiance des utilisateurs envers de nombreux services, notamment les réseaux sociaux, ou encore les opérateurs téléphoniques, est en partie imputable aux différents scandales de fuites et de reventes de données. Les banques, par leur relation de proximité avec leurs clients, leur savoir-faire ainsi que les technologies qu'elles mobilisent, se positionnent comme un interlocuteur de confiance et disposent d'un avantage concurrentiel fort vis-à-vis de la protection des données. Elles semblent donc posséder les atouts pour proposer des services supplémentaires sur ce segment

1.3. Une relation de confiance qui peut être renforcée

Si les banques sont bien perçues concernant leur capacité à protéger les données personnelles de leurs clients, la confiance accordée à celles-ci par les Français pourrait être renforcée, puisque la note de confiance globale attribuée est de 6,6.



Cette confiance est limitée par deux principaux facteurs : une tarification jugée pas toujours juste et un manque de transparence, notamment concernant les politiques de tarification et l'utilisation des données personnelles *(profilage et « scoring »)*.



Par exemple, un client ne comprend pas toujours pourquoi une demande de prêt lui est refusée suite à une action de profilage et de « scoring »[10]. Un ajustement pour une meilleure transparence, dans le respect du RGPD, contribuerait à améliorer la confiance intrinsèque *(ex. demande de consentement libre et éclairé au client sur les pratiques de l'établissement)*. Les banques pourraient ainsi faire usage du profilage et « scoring » comme d'outils non-discriminatoires voire positifs *(ex. lutte contre le surendettement)* dans l'intérêt commun de la banque et du client.

LE PROFILAGE

D'après le Règlement Général sur le Protection des Données (*RGPD*), le profilage correspond à « toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique ».

Notons que la sécurité est le troisième axe identifié susceptible d'améliorer la confiance des Français, ce qui démontre que, malgré une expertise reconnue dans la protection des données, ce sujet doit rester une priorité à l'heure de la digitalisation des activités bancaires.

Ces axes d'amélioration doivent être analysés à l'aune des mutations actuelles du marché, caractérisées par l'apparition de nouvelles problématiques, de nouvelles réglementations, de nouveaux acteurs et de nouvelles technologies.

10 *Scoring : Notation des clients résultant d'un calcul d'analyse de risque issu du profilage*

2

Un marché en mutation, redéfinissant les tenants et les aboutissants de la confiance

Le marché bancaire est actuellement bouleversé par des facteurs d'ordres règlementaire, concurrentiel et technologique. Ces facteurs (parfois étroitement liés) pèsent sur les tenants et aboutissants de la confiance. En particulier, la protection des données personnelles a fait l'objet d'un règlement européen dédié, le RGPD. Ce nouveau contexte donne à l'identité numérique une dimension stratégique.

2.1. L'identité numérique, nouvel enjeu clé de la confiance dans le monde numérique

L'identité numérique est la représentation d'un individu dans le monde virtuel. Elle est constituée d'un ensemble de données rattachées à une personne physique ou morale existant sur Internet ou dans des systèmes d'information. En effet, l'identité numérique ne se limite pas aux données pivot[11] propres à l'identité régalienne d'une personne, et peut se définir comme une représentation numérique particulière de cette personne, plus ou moins anonyme selon le cas. Une personne possède une multitude de profils numériques constitutifs de son identité numérique. Typiquement un ensemble de données collectées sur Internet associées directement ou indirectement *(adresse mail, pseudonymes, adresse IP…)* à une personne peut permettre d'en établir un profil numérique.

L'identité numérique occupe une place centrale dans les processus d'enrôlement et de vérification d'identité, d'authentification, de signature et de consentement, dont les fonctions nécessitent l'utilisation de données personnelles des utilisateurs.

La fonction d'identification a pour but de répondre à la question « qui êtes-vous ? ». Elle consiste à collecter à l'enrôlement des données directement identifiantes *(un nom, un email, un numéro identifiant tel que le numéro de sécurité sociale)* de la personne ou indirectement identifiantes *(une adresse postale, son âge, son sexe…)* et à vérifier l'identité de la personne *(vérification de la validité, de l'authenticité, de l'intégrité et du lien univoque avec une personne réelle unique)*. Le processus d'identification permet donc de valider une identité vérifiée d'une personne pour lui donner légitimité à bénéficier d'un service.

La fonction d'authentification répond à la question : êtes-vous bien la personne que vous annoncez être ? Elle vise à autoriser l'accès à des services et/ou des droits rattachés à une personne, via une vérification formelle d'une ou de plusieurs informations, qualifiées de facteurs d'authentification[12].

Certains services (ex. accès à un réseau social, à son adresse email personnel) ne

11 *Données pivot en France : Le nom, le prénom, le sexe, la date de naissance, le pays de naissance ou la ville de naissance*

12 *Classés en trois catégories : Possession, Connaissance, Inhérence*

nécessitent pas d'authentification sur la base d'une identité au préalable vérifiée par une phase d'identification. Dans ce cas la personne peut utiliser pour un service en ligne un identifiant quelconque (ex. pseudonyme) pour accéder au service.

En revanche, pour d'autres services (ex. ouverture de compte bancaire), l'authentification se base sur une identité vérifiée à laquelle est associée un identifiant unique principal dans une base de données ou un registre. Dans ce cas l'authentification en ligne a pour but de confirmer l'appartenance de cet identifiant et donc du profil d'identité vérifiée associé à l'utilisateur qui le revendique. Typiquement, un processus d'enrôlement client pour l'ouverture d'un nouveau compte bancaire inclut une procédure de KYC nécessitant une identification *(incluant la vérification de pièces d'identité)* et une authentification du client *(vérification que la demande émane bien de la personne identifiée)*. En phase d'utilisation, l'authentification conditionne l'accès à un service auquel un identifiant donné a droit *(ex. moyen de paiement, via la saisie du code personnel de sa carte bancaire)*. Chaque service nécessitant son propre identifiant et un moyen d'authentification, l'utilisateur est confronté à la multiplicité des mots de passe et à l'usage de méthodes reposant sur des niveaux de sécurité différents. Par ailleurs, la DSP2 *(voir encart DSP2 ci-dessous pour plus de précisions)*, précisée par un règlement délégué RTS[13], généralise le recours à l'authentification forte pour les services de paiement. Cette authentification forte associe une authentification avec deux facteurs différents indépendants à une génération de code unique et aléatoire pour éviter les risques d'attaques à distance et de rejeu du code d'authentification[14].

DSP2

La directive DSP2[15] encadre tous les services de paiement. L'ordonnance française transposant cette directive est applicable depuis le 13 janvier 2018. Pour encourager le développement de l'innovation, la directive DSP2 permet l'accès ou le partage de certaines données bancaires, via des canaux sécurisés entre les Prestataires de Services de Paiement (PSP).

13 *RTS : RTS (Regulatory Technical Standards ou Standards Techniques) : ensemble des standards techniques préparés par l'Autorité Bancaire Européenne en collaboration avec la BCE (Banque Centrale Européenne) et les banques centrales nationales. Divers RTS sont prévus par la Directive DSP2 pour en harmoniser la mise en œuvre opérationnelle*

14 *Voir article 4-30 de la DSP2 pour une définition de l'authentification forte*

15 *DSP2 : Galitt est également l'auteur d'un livre blanc actualisé en 2018 consacré au thème de la DSP2 appliquée au secteur bancaire : « DSP2 & OPEN API : menaces et opportunités pour le secteur bancaire – En route vers l'Open-Banking ? ».*

Pour ce faire, la directive a notamment été précisée par des RTS pour spécifier les normes ouvertes, communes et sécurisées de ces canaux de communication. Ces normes CSC (Common and Secure Communication) permettent donc de décrire les mesures techniques et organisationnelles pour mettre en œuvre un nouveau droit, celui de faire accéder des tiers à ses données de paiement, qui doit être consenti explicitement par l'utilisateur conformément à la nouvelle réglementation RGPD. Ces RTS décrivent, outre la mise en œuvre d'interfaces sécurisées, les procédures relatives à l'authentification forte du client (Strong Customer Authentication - SCA), obligatoire lorsque le client souhaite accéder à son compte de paiement en ligne, initier une opération de paiement électronique, ou effectuer une action, à l'aide d'un moyen de communication à distance, susceptible de comporter un risque de fraude. L'authentification forte participe à la preuve de consentement explicite donné par l'utilisateur pour autoriser l'accès à ses données bancaires à un tiers PSP mais aussi pour initier par ce dernier une opération de paiement à partir d'un compte détenu chez l'établissement teneur de compte. Les exigences introduites par ces RTS devront toutes être appliquées à partir du le 14 septembre 2019.

Notons que ces deux fonctions *(identification et authentification)* peuvent être directement assurées par le fournisseur de service auquel souhaite accéder le client, qui assumera alors pour lui-même le rôle de fournisseur d'identité. Mais la tendance est aujourd'hui de confier ce rôle à un tiers, avec différentes architectures possibles : centralisée *(modèle single sign-on, par exemple Facebook Connect)*, décentralisée *(modèle de fédération d'identité, tel FranceConnect)*, et désormais distribuée, grâce à la technologie blockchain *(voir la partie 3.1 pour plus de détails à ce sujet)*.

LE PROGRAMME ACTION PUBLIQUE 2022

En France, le programme Action Publique 2022[16] déclare que la mise en place de solutions d'identité numérique sécurisée est une priorité. Il prévoit le déploiement d'un parcours d'identification numérique sécurisé pour l'Etat, et de moyens d'identification électronique eIDAS associés, permettant l'accès à ce parcours et à l'échange de données entre des fournisseurs d'identité agréés et des fournisseurs de services autorisés. Ces différentes actions seront effectuées sous le contrôle de l'utilisateur, avec la garantie que ses données personnelles seront protégées. Le

16 *Programme lancé le 13 octobre 2017 par le premier ministre, visant à accélérer la transformation publique alimenté en pistes de réformes par le Comité Action Publique 2022.*

programme prévoit également un principe de proportionnalité entre la force d'identification (données personnelles utilisées) et l'usage. Ce service devrait être accessible dès septembre 2019. D'autres moyens d'identification électronique matériels ou immatériels (par exemple une application sur son mobile) sont en cours de qualification par l'ANSSI et d'intégration par la DINSIC[17] dans « FranceConnect ».

Les fonctions associées à l'identité numérique, sont étroitement liées au nouveau règlement RGPD, qui adresse le sujet des données personnelles pour les banques, tant au niveau technique, règlementaire et organisationnel, que vis-à-vis de la confiance des clients.

2.2. Le Règlement Général sur la Protection des Données (RGPD), illustration d'un cadre règlementaire en transformation

Le **RGPD**, adopté en 2016 et applicable depuis le 25 mai 2018, définit un cadre d'obligations renforcées pour la protection des données personnelles des utilisateurs. Ce règlement s'inscrit dans la continuité de la directive de 1995[18] - restée faiblement appliquée en raison de sanctions peu dissuasives et hétérogènes entre les pays membres - et de fait s'applique directement à tous les pays membres de l'Union Européenne, sans transposition nationale. Le RGPD inverse le rapport à la conformité vis-à-vis de cette directive et introduit la notion d'« **accountability** » : tous les responsables de traitement[19] doivent être autonomes et compétents pour la gestion de la protection des données personnelles et garantir la conformité continue au règlement RGPD. Le contrôle peut être effectué à n'importe quel moment, alors que la directive de 1995 conduisait à une planification à date fixe du contrôle des mesures mises en œuvre.

Le RGPD définit pour l'utilisateur un **droit à la portabilité de ses données numériques**. Un client doit pouvoir récupérer ses données et les transférer de manière fluide vers un autre établissement s'il souhaite en changer. A défaut, il peut recourir à l'autorité de contrôle *(en France, la CNIL)* et au système judiciaire à titre individuel, ou par une action de groupe.

Le RGPD renforce la notion de **consentement explicite, libre et éclairé** pour la collecte

17 *DINSIC : Direction Interministérielle du Numérique et du Système d'Information et de Communication de l'Etat*

18 *Directive 95/46/CE (1995) relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (texte de référence avant le RGPD).*

19 *Responsables de traitement : les responsables de traitement sont définis de la manière suivante par la CNIL : « Le responsable d'un traitement de données à caractère personnel est, sauf désignation expresse par les dispositions législatives ou règlementaires relatives à ce traitement, la personne, l'autorité publique, le service ou l'organisme qui détermine ses finalités et ses moyens. En pratique et en général, il s'agit de la personne morale incarnée par son représentant légal. »*

et/ou le traitement des données personnelles, bien qu'il ne soit pas requis dans le cas d'exécution d'un contrat signé par la personne concernée ou dans le cas du traitement nécessaire au respect d'une obligation légale. Pour autant, les clients doivent toujours être informés de la collecte et du traitement de leurs données personnelles car ils en sont les uniques propriétaire

Le RGPD comprend différentes propositions de mesures, notamment le principe de **minimisation des données**. La mesure consiste à réduire toute demande de renseignement à caractère personnel à ce qui est strictement nécessaire pour effectuer la tâche concernée et cela dans le temps imparti pour celle-ci.

LA MINIMISATION DES DONNEES

Exemple concret : le parcours de souscription à une assurance automobile requiert la fourniture de données personnelles qui devraient théoriquement se limiter strictement aux informations nécessaires (i.e. en lien avec le véhicule et à son usage et au permis de conduire du client). Ces données pourront être archivées pendant une durée n'excédant pas cinq ou dix ans, selon la nature du contrat, à compter de la fin de sa validité. L'assureur peut demander au client de fournir quelques données supplémentaires (non obligatoires pour l'obtention du service) pour lesquelles son consentement explicite et éclairé au regard de l'information fournie est nécessaire. Ex. : le statut marital et le nombre d'enfants de l'individu, permettant à l'assureur de réaliser une étude statistique et d'offrir des services additionnels non fournis dans le contrat. En revanche le nom, prénom, voire même l'âge des membres de la famille de l'assuré pourront être considérés comme non-légitimes au regard du principe de minimisation des données.

Un autre principe particulièrement pertinent du RGPD pour les banques est celui de « **privacy by design** », soit le respect de la vie privée dès la conception de la solution et tout au long de son cycle de vie. Cela signifie que chaque nouveau produit ou service utilisant des données personnelles des utilisateurs doit, dès sa conception, garantir le respect de la vie privée pendant toute sa durée d'utilisation.

PRIVACY BY DESIGN ET PRIVAY BY DEFAULT

Selon la CNPD (Commission Nationale du Luxembourg pour la Protection des Données), « le concept de « Privacy by Design » a pour objectif de garantir l'intégration de la protection de la vie privée dans les nouvelles applications technologiques et commerciales dès leur conception. Pour chaque nouvelle application, produit ou service ayant besoin de données à caractère personnel, les entités responsables du traitement devraient offrir aux utilisateurs le plus haut niveau possible de protection des données. Par exemple, un système « Privacy by Design » peut permettre, suite à une requête, l'accès à la valeur intéressante liée à une donnée, sans dévoiler la donnée exacte (par exemple permettre de savoir si l'individu est majeur, sans donner accès à son âge exact). Le concept de « Privacy by Design » est étroitement lié à celui « Privacy by Default », selon lequel chaque entreprise traitant des données personnelles doit mettre en place par défaut le plus haut niveau possible de protection des données, l'utilisateur gardant dans ce cas la main pour modifier ses paramètres.

Par ailleurs, les banques sont concernées par l'impact du RGPD sur le profilage et sur la décision automatique qui en découle. Exemple : lors d'une demande de crédit, la décision automatique consécutive à un résultat de profilage effectué par la banque doit être consentie clairement et librement par le client, qui doit également pouvoir s'y opposer s'il le souhaite et solliciter une intervention humaine. Le client peut demander à accéder à la valeur du « scoring », à la méthode de calcul et à la logique de la décision automatique.

LA DECISION AUTOMATIQUE

La décision entièrement automatique est définie par la CNIL dans le cadre du RGPD comme « une décision prise à l'égard d'une personne, par le biais d'algorithmes appliqués à ses données personnelles, sans qu'aucun être humain n'intervienne dans le processus. Elle peut intervenir dans de nombreux domaines d'activité (finance, fiscalité, marketing, etc.) et produire des effets juridiques ou des effets significatifs pour les personnes concernées. Par exemple, une décision de refus de crédit peut avoir pour seul fondement l'utilisation d'un algorithme qui applique automatiquement certains critères à la situation financière du demandeur, sans aucune intervention humaine.

Même vis-à-vis du risque de fraude, une décision 100 % automatique peut être interdite. La CNIL, le 13 juillet 2017[20], a défini qu'aucune décision produisant des effets juridiques à l'égard des personnes concernées par des données traitées dans le cadre de la lutte contre la fraude ne peut être prise sur le seul fondement de ces traitements automatisés. Dès lors, les alertes générées automatiquement doivent donner lieu à une analyse non automatisée par le personnel habilité, sous peine d'altérer la confiance des clients dans les banques, même si certaines décisions automatiques sont autorisées de façon très encadrée par les autorités de contrôle en charge de l'application du RGPD[21].

Dans le cadre du RGPD, d'autres définitions importantes sont rappelées, par exemple celle des **données sensibles**. En France, se rajoute le cas particulier du numéro de sécurité sociale appelé NIR, qui dispose d'un statut particulier, en tant que donnée personnelle sensible : un décret spécifique est requis pour autoriser la collecte, le traitement et l'archivage du NIR. Par exemple, pour la collecte et le stockage d'une feuille de paye sous forme papier ou numérique hors champ du décret, le NIR ne doit pas ou plus pas y figurer.

DONNEE SENSIBLE

Selon la CNIL, une donnée sensible correspond à « toute information concernant l'origine raciale ou ethnique, les opinions politiques, philosophiques ou religieuses, l'appartenance syndicale, la santé ou la vie sexuelle. En principe, les données sensibles ne peuvent être recueillies et exploitées qu'avec le consentement explicite des personnes ».

Les entreprises qui enfreignent volontairement le RGPD s'exposent à une **amende maximale équivalente à 4% de leur chiffre d'affaires mondial ou 20 millions d'euros** *(le montant le plus élevé s'applique)*.

Beaucoup de projets numériques peuvent répondre de facto à certains critères imposés par le RGPD *(contrôle, proportionnalité[22])*. Les banques doivent utiliser ces nouvelles règles comme une opportunité et non comme une contrainte.

Selon la CNIL, les entreprises peuvent en effet profiter de la mise en application du RGPD pour renforcer la confiance des utilisateurs, améliorer leur efficacité commerciale, mieux gérer leur entreprise, améliorer la sécurité de leurs données,

20 Délibération n° 2017-217 du 13 juillet 2017 portant autorisation unique de traitements de données à caractère personnel aux fins de la lutte contre la fraude externe dans le secteur bancaire et financier (AU-054) », apparu au journal officiel le 25 juillet 2017 (texte n°63).

21 Par exemple, en France, la CNIL a imposé à Boursorama un certain nombre de contraintes à respecter pour lui permettre d'instaurer un système de décision automatique dans ses procédures de KYC à distance.

22 Principe selon lequel les informations enregistrées doivent être pertinentes et strictement nécessaires au regard de la finalité du fichier constitué

rassurer leurs clients et leurs donneurs d'ordres et enfin créer de nouveaux services.

LE MARCHE DE LA CONFIANCE

« Aujourd'hui la culture change, les gens s'intéressent à la protection de leurs données. L'Europe adresse un grand message au reste du monde en termes de respect des individus. Le RGPD est une loi unique pour tous les pays de l'Union Européenne qui permet d'harmoniser la réglementation, une opportunité pour les entreprises de se positionner comme actrices crédibles et dignes de confiance, ainsi qu'un moyen d'égaliser les forces entre les entreprises européennes et étrangères, mais aussi entre de multiples acteurs. Le RGPD donne le choix aux individus. Il est à l'origine d'un nouveau marché : celui de la confiance. Des fonds d'investissement, par exemple, ont déjà décidé de faire de la conformité au RGPD un facteur décisif dans leurs choix d'investissements ».

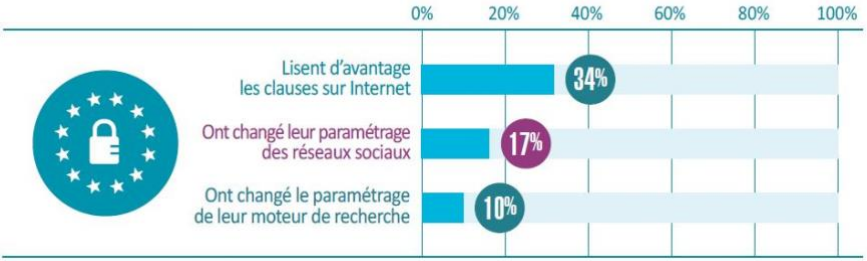
Isabelle Falque-Pierrotin
Directrice de la CNIL

Salon Viva Technology, 25 mai 2018 (jour d'entrée en vigueur du RGPD)

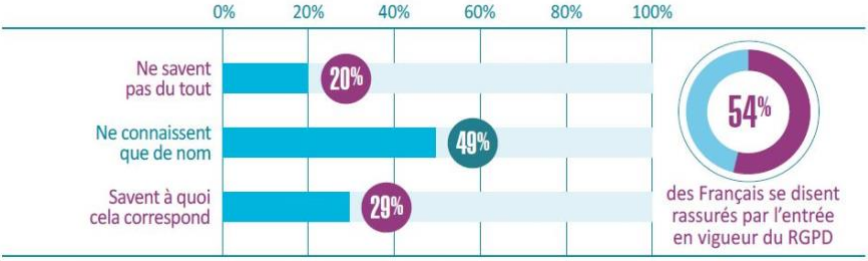
Le RGPD protège donc les utilisateurs d'une utilisation abusive de leurs données personnelles. Le RGPD apporte un cadre règlementaire uniforme pour tous les pays membres et permet une meilleure cohérence dans l'application de mesures de protection, ainsi que de sanctions, vis-à-vis des services numériques nécessitant l'utilisation de données personnelles.

L'entrée en vigueur du RGPD est bien perçu par les utilisateurs, bien qu'encore parfois méconnu *(voir infographie ci-dessous)* : la majorité des Français interrogés se disent rassurés par le RGPD, plus d'un tiers lit d'avantage les clauses sur Internet depuis l'entrée en vigueur du règlement, tandis que 17% ont changé le paramétrage de leurs réseaux sociaux et 10% le paramétrage de leur moteur de recherche.

Suite à l'entrée en vigueur du RGPD



Savez-vous à quoi correspond le RGPD ?



L'APPLICATION RGPD EN FRANCE

Selon En France, c'est la CNIL qui est chargée de faire respecter ce règlement. Dorénavant, elle sera encore plus vigilante vis-à-vis du respect des principes fondamentaux de la protection des données, même s'ils restent pour l'essentiel inchangés par rapport à la loi Informatiques et Libertés : loyauté du traitement, pertinence des données, durée de conservation, sécurité des données, etc. Les entreprises continueront donc à faire l'objet de vérifications rigoureuses par la CNIL et de possibles sanctions, comme l'autorise la loi depuis le 7 octobre 2016. À ce titre, diverses entreprises ont été sanctionnées pour des insuffisances de sécurité sur leur site Web relativement à l'accès aux données clients ou bénéficiaires.

Le règlement RGPD n'est qu'une première étape dans l'encadrement des nouvelles pratiques numériques. Le futur règlement ePrivacy[23] devrait entrer en vigueur prochainement pour le compléter afin d'élargir la libre circulation des données aux communications électroniques dans l'Union Européenne tout en fixant des règles respectueuses de la Charte Européenne des Droits de l'Homme. Il apportera un niveau de protection équivalent entre des personnes physiques et morales assurant la protection en confidentialité des communications électroniques *(contenu et métadonnées)*, ainsi que la protection en intégrité des équipements des personnes physiques et morales. Le règlement ePrivacy autorisera les communications marketing directes de façon encadrée et respectueuse des droits des utilisateurs.

En résumé, les banques doivent se mettre en capacité d'intégrer dans leurs processus les contraintes de l'arsenal règlementaire en cours de déploiement. En contrepartie, elles bénéficieront de l'opportunité d'offrir de nouveaux services sécurisés basés sur la libre circulation des données et l'interopérabilité en Europe.

23 *EUR-Lex : proposition de règlement concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques.*

Focus sur le cadre règlementaire

Les banques doivent respecter de nombreuses réglementations pour protéger les clients des risques auxquels ils peuvent être exposés. La réglementation bancaire est régie par les standards internationaux du Comité de Bâle. Le Code Monétaire et Financier (*CMF*), qui intègre à présent les règlements et directives européens, dresse le cadre règlementaire applicable aux banques françaises. L'ACPR - Autorité de Contrôle Prudentiel et de Résolution - dépendant de la Banque de France, est en charge de la surveillance des institutions bancaires sur le sol français. Les activités des banques sont également encadrées par des règlements et directives spécifiques.

La directive européenne AMLD4 (*« Anti-Money Laundering Directive 4 »*), en application depuis janvier 2018, donne des instructions aux banques et à tous les prestataires de services financiers, de paiement, et d'assurance, pour lutter contre le blanchiment d'argent et le financement du terrorisme. Son actualisation, AMLD5 (*« Anti-Money Laundering Directive 5 »*), vient étendre son champ d'action au marché de la crypto monnaie, durcit les exigences vis-à-vis des cartes prépayées, ou encore facilite l'accès au Registre de Transparence Européen[24]. Cette directive devrait être mise en œuvre d'ici le 10 janvier 2020.

La directive NIS, applicable depuis mai 2018, régit la cybersécurité au niveau européen et définit la notion d'OSE (*Opérateurs de Services Essentiels*) et de services de confiance numérique. Elle a été transposée en droit français en 2018, pour préciser les attentes générales relatives à la sécurité des réseaux et des systèmes d'information. L'ANSSI (*Agence Nationale de la Sécurité des Systèmes d'Information*) en définit les règles applicables et pilote les actions de mise en conformité règlementaire. Les pratiques prescrites par la directive européenne NIS sont en grande partie déjà en place en France. En effet, elles sont une juste continuité de la loi de programmation militaire (*LPM*), qui caractérise les grandes institutions bancaires comme des OIV (*Opérateurs d'Importance Vitale*) et de ce fait les soumet à des obligations fortes en termes de cybersécurité, en particulier de protection des infrastructures vitales dont elles disposent : une attaque sur le système d'information d'une OIV mettrait en risque toute l'économie du pays. La

24 Registre de Transparence Européen : Selon la Commission Européenne, c'est une base de données répertoriant les organisations qui cherchent à influencer le processus législatif et de mise en œuvre des politiques des institutions européennes.

directive NIS pourrait pousser l'ANSSI à notifier tous les prestataires de services de paiement comme des OSE et ainsi les contraindre à appliquer les règles de gouvernance, de protection, de défense, de résilience, de reporting de tout incident de sécurité et d'audit (vérification annuelle du SI).

Les banques doivent également respecter le règlement eIDAS dont l'objet du 1er volet est de créer un socle commun européen d'interopérabilité et de reconnaissance mutuelle transfrontalière de l'identité numérique pour les accès en ligne aux services publics. eIDAS spécifie trois niveaux de garantie[25]: faible, substantiel et élevé[26].

Le décret modifiant le CMF et visant à renforcer le dispositif français de lutte contre le blanchiment de capitaux et le financement du terrorisme, propose que la procédure de KYC des clients et des bénéficiaires ait recours à des moyens d'identification électronique définis par eIDAS au niveau élevé, ou substantiel s'ils sont complétés par une autre mesure. Sur ce point, ce décret devance et complète la nouvelle directive AMLD5, qui évoque simplement la possibilité du recours à des moyens d'identification électronique eIDAS sans en spécifier le niveau d'exigence.

Le 2ème volet d'eIDAS réglemente l'interopérabilité et la valeur juridique des cinq services de confiance numérique[27] pour les usages des services publics et privés. De nombreuses banques ont déjà mis en place la signature électronique pour simplifier les démarches dans un contexte de dématérialisation. Elles peuvent aussi tirer profit de solutions fournies par des prestataires de services qualifiés eIDAS, afin d'assurer une validité juridique très forte. Selon le texte eIDAS : « L'effet juridique d'une signature électronique qualifiée est équivalent à celui d'une signature manuscrite ». En d'autres termes, seule la signature électronique qualifiée est interopérable dans toute l'Europe et peut faire foi sans avoir besoin d'en démontrer la preuve dans un cadre juridique (*renversement de la charge de la preuve à la partie adverse*).

25 *D'après l'Annexe au Règlement d'exécution (UE) 2015/1502 de la Commission du 8 Sept. 2015.*

26 *eIDAS spécifie des exigences propres à chaque processus (enrôlement, identification électronique, authentification et management et organisation).*

27 *Services de délivrance de certificats qualifiés de signature électronique, de cachet électronique et d'authentification de site internet, services de validation qualifiée et services de conservation qualifiée des signatures électroniques qualifiées et des cachets électroniques qualifiés, services d'horodatage électronique qualifié, et services d'envoi de recommandé électronique qualifié.*

3

Quelles opportunités, pour l'organisation et l'offre de service de banques ?

L'acteur bancaire, aussi bien concernant ses processus internes que son offre de service, possède des atouts évidents pour saisir les opportunités issues des mutations du marché bancaire.

3.1. De nouvelles solutions pour la conduite de l'activité des banques, renforçant la sécurité et la protection des données

De nouvelles solutions, s'appuyant sur des technologies plus ou moins éprouvées, visent à faciliter, fluidifier, sécuriser la gestion et le traitement des données par les banques. De l'enrôlement du client, au partage sécurisé avec des tiers, en passant par la gestion des données personnelles, les pistes sont multiples, et permettent d'être en conformité avec la législation européenne. Par ailleurs, l'accès aux données personnelles étant de plus en plus facilité avec la transformation numérique, les banques peuvent mettre en place, en plus des mesures techniques et organisationnelles requises, des mesures intrinsèquement adaptées à la protection des données personnelles et au respect des droits des utilisateurs. En faisant cela, les banques sont conformes au principe de « privacy by default » prescrit par le Règlement Général sur la Protection des Données.

La blockchain, une technologie de mise en conformité RGPD ?

Dévoilée au grand public à la faveur du phénomène Bitcoin, la blockchain fait depuis l'objet de multiples investigations et expérimentations se traduisant parfois par le lancement de nouveaux services, notamment dans le secteur financier. L'un des sujets récurrents, qui n'est pas propre au secteur financier, porte sur l'apport potentiel de la blockchain sur la gestion et la protection des données personnelles. Pourtant, son adéquation avec les principes fondateurs du RGPD pose question puisque par nature, cette technologie ne permet pas d'appliquer le droit à l'effacement ou à la rectification des données. Une mise en conformité au RGPD est toutefois envisageable via une adaptation de la technologie blockchain appliquée en consortium privé. Selon la CNIL, le principe de blockchain privée permet « à une autorité désignée de garder la main sur les transactions et potentiellement de les contrôler et de les rectifier ».

BLOCKCHAIN

D'après la CNIL, « La blockchain est une technologie de stockage et de transmission

d'informations, transparente, sécurisée, et fonctionnant sans organe central de contrôle. Elle constitue une base de données sécurisée et distribuée qui contient l'historique de tous les échanges effectués entre ses utilisateurs depuis sa création : elle est partagée par ses différents utilisateurs, sans intermédiaire, ce qui permet à chacun de vérifier la validité de la chaîne. Il existe des blockchains publiques, ouvertes à tous, et des blockchains privées, dont l'accès et l'utilisation sont limités à un certain nombre d'acteurs. Une blockchain publique peut donc être assimilée à un grand livre comptable public, anonyme et infalsifiable. La technologie blockchain, et plus généralement la technologie de registre distribué, se déploie sur divers cas d'usages et dans de nombreux secteurs, parmi lesquels l'environnement, le transport, la logistique, l'éducation, la santé et la finance[28] ».

Vis-à-vis du RGPD, la blockchain présente l'intérêt d'offrir un historique infalsifiable grâce à l'horodatage des blocs et à une intégrité résiliente des transactions enregistrées sur la chaine de blocs. Cela ouvre des possibilités en termes de traçabilité des consentements clients, des transactions ou des modifications de données personnelles, permettant aux entreprises de respecter le principe « d'accountability » auprès des autorités de contrôle du RGPD et de respecter le droit des utilisateurs (*droit d'accès, de modification*) de façon transparente.

En revanche, si les blockchains de consortiums privés restreignent les accès aux informations stockées aux acteurs bénéficiant des droits d'accès, celles-ci ne résolvent pas pour autant les problématiques de droit à l'oubli (suppression de la donnée), ni de confidentialité des données, chaque acteur bénéficiant de l'accès à la blockchain ayant un droit de lecture sur l'intégralité de la chaîne de blocs. C'est pourquoi la technologie blockchain devrait être utilisé pour sa fonction première de livre de compte : un registre distribué sécurisé de preuves horodatées de transactions et surtout pas comme une base de données personnelles distribuée.

Outre sa fonction de registre de preuves, la technologie blockchain peut être combinée avec l'usage de smart contracts « privacy by design » permettant d'assurer l'exécution logicielle automatique de transactions en respectant les fondamentaux du RGPD.

Le protocole Ethereum a ainsi permis en 2017 l'utilisation d'une nouvelle brique cryptographique, le « zero knowledge proof » (***ZKP***)[29], visant à offrir confirmation d'une information sans en dévoiler le contenu. ING s'est inspiré de ce concept pour développer ses propres solutions. La dernière en date, le Zero-Knowledge Set Membership, permet, lors d'une procédure KYC, à un client de prouver qu'il est, par exemple, bien citoyen de l'Union Européenne, sans dévoiler son pays d'origine[30].

---

28 Pour des illustrations de cas d'application, voir notamment le projet de résolution européenne sur les technologies de registres distribués (TRD) et les chaînes de blocs pour renforcer la confiance par la désintermédiation, publié le 24 septembre 2018.

29 Traduit en français par preuve à divulgation nulle de connaissance, ce terme désigne un protocole sécurisé dans lequel un fournisseur de preuves garantit à un vérificateur l'exactitude d'une proposition relative à un secret, sans pour autant dévoiler autre chose concernant ce secret (au-delà de l'exactitude de la proposition).

30 Pour plus d'informations, voir le livre blanc d'ING sur le Zero-Knowledge Set Membership.

Pour certains services comme les services financiers, cette preuve doit avoir une valeur probante au sens juridique du terme. Dans ce cas, la technologie blockchain, registre de preuve associé ou non à des fonctions de smart contract, ne suffit pas : la valeur probante d'une donnée *(attribut)* personnelle doit être associée à un niveau de garantie délivré et certifié par un tiers de confiance pour une durée limitée dans le temps.

Les technologies de registre distribué et de blockchain pourraient prendre toute leur mesure pour la gestion de ces niveaux de garantie à valeur probante *(écriture, révocation, prolongation, accès)*. Ainsi un fournisseur de service qui souhaite s'assurer de la fiabilité d'un attribut personnel d'un client pourrait s'appuyer sur ce type de registre, alimenté ou géré par les tiers de confiance dans un écosystème de confiance ouvert et transparent.

En tant que tiers de confiance privés, les banques ont un rôle à jouer dans la mise en œuvre de fonctions de ces registres de valeurs probantes, ces derniers pouvant par ailleurs servir de fondations à l'instauration d'écosystèmes d'identité numérique. C'est la trajectoire que semble prendre le Canada, au travers d'une initiative de grande ampleur menée par le spécialiste de l'authentification et de la validation d'identité SecureKey, qui embarque plusieurs institutions financières canadiennes de premier plan. Cette initiative offre en outre des opportunités de fournir de nouveaux services aux clients bancaires *(voir partie 3.2 pour découvrir ces services)*.

La blockchain ouvre donc de nouveaux horizons en matière de gestion des données personnelles et de KYC, qui fait par ailleurs face à d'autres innovations.

La biométrie, une solution pour sécuriser le KYC à distance ?

En matière de KYC, l'heure est au déploiement de parcours totalement digitalisés. Pour la banque, le gain de temps apporté par une procédure eKYC dans le traitement d'un dossier client est indéniable : certaines banques réalisent désormais des ouvertures de comptes en 24 à 48h, contre une dizaine de jours pour une procédure standard. Côté client, le parcours de souscription est fluidifié, avec l'élimination d'un point de friction majeur, le rendez-vous physique en agence. En revanche, d'autres défis apparaissent : en sus des contraintes de connectivité de l'eKYC, plus de menaces pèsent sur la sécurité de la procédure, et en particulier sur l'identification du prospect. L'enjeu est en

fait double, il faut à la fois vérifier l'identité à distance en relation avec les preuves d'identité *(ex. un titre d'identité valide, un justificatif de domicile…)*, et être en mesure d'opérer une « détection de présence réelle » du prospect *(« liveliness detection »)*.

En Europe, certains régulateurs économiques ou du domaine bancaire se sont exprimés en faveur de ce type de procédé biométrique basé pour la plupart sur des solutions par vidéoconférence améliorées : l'Italie, l'Autriche, l'Espagne ou encore l'Estonie.

En France, l'ACPR ne s'est pas prononcée publiquement sur les systèmes d'identification par reconnaissance faciale des prospects lors d'une entrée en relation à distance. En revanche, la CNIL avait validé avant le RGPD les procédés de validation à distance mis en œuvre par la Société Générale[31] et par Boursorama[32] en termes de respect de mesures appropriées pour la protection des données personnelles particulièrement sensibles que sont les données biométriques.

Les deux procédés s'appuient sur la biométrie pour permettre une comparaison entre la photo du document d'identité du client et un selfie réalisé par le client avec son téléphone. En outre, dans le cas de Société Générale, la « liveliness detection » est réalisée via un entretien par vidéo entre un conseiller et le prospect. Lors de cet entretien, une nouvelle comparaison biométrique est effectuée entre la photographie figurant sur la pièce d'identité principale fournie et des photographies extraites de l'entretien par vidéo. Si nécessaire, la vérification d'identité peut être complétée par le conseiller via un questionnaire.

Boursorama fait valoir à l'inverse un procédé totalement automatisé sans intervention humaine : la reconnaissance faciale n'est utilisée par Boursorama que pour vérifier que la photo du titre d'identité correspond bien à la personne qui s'enrôle à l'aide d'un selfie. Il n'y pas de recours à d'autres procédés biométriques pour vérifier la présence réelle de la personne. Le processus automatisé comprend ensuite un processus de signature électronique du contrat de l'offre produit bancaire avec l'envoi d'un mail contenant une URL vers le nouvel espace client et son identifiant lui permettant d'y accéder.

Sur les procédures d'identification intégralement en ligne, notons le positionnement de l'ANSSI : dans le cadre de la qualification de moyens d'identification eiDAS substantiel ou élevé, la validation d'une identité à distance sans présence physique du demandeur sur le lieu de la vérification nécessite de démontrer l'équivalence avec une vérification d'identité en face à face physique. Cela passe par la mise en place de mesures techniques et organisationnelles permettant de lutter contre les risques de fraude avec une exigence de fiabilité au moins égale à la présentation physique du document d'identité et permettant de couvrir les risques liés à la manipulation par simulation d'une présence réelle de la personne.

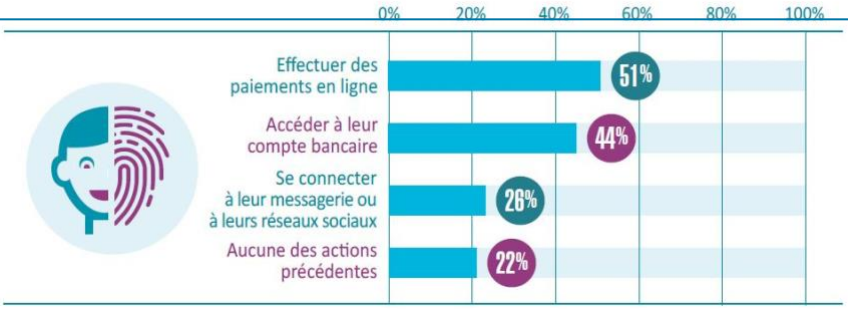
31 Legifrance : Délibération de la CNIL n°2017-251 du 14 septembre 2017 concernant Société Générale
32 Legifrance : Délibération de la CNIL n°2018-051 du 15 février 2018 concernant Boursorama

BIOMETRIE

Selon la CNIL, « La biométrie regroupe l'ensemble des techniques informatiques permettant de reconnaître automatiquement un individu à partir de ses caractéristiques physiques, biologiques, voire comportementales ». Le RGPD impose trois prérequis à l'usage de la biométrie :

- Une finalité légitime et licite : le dispositif ne sera validé que s'il répond à des besoins de sécurisation forte ;
- Le consentement préalable : il faut obtenir le consentement spécifique (pour l'usage en question), libre (une alternative doit être proposée), et éclairé (explicite) de l'utilisateur. Dans tous les cas, les personnes conservent le droit de ne pas y consentir ou de retirer leur consentement à tout moment du processus et d'opter pour des alternatives classiques ;
- Une étude d'impact vie privée (PIA) approuvée par la CNIL. La position de la CNIL est d'imposer le chiffrement obligatoire du gabarit biométrique.

L'usage de dispositifs s'appuyant sur la biométrie a augmenté de façon exponentielle en France ces dernières années : alors qu'entre 1978 et 2004, seuls 37 dispositifs avaient été examinés par la CNIL, 800 autorisations ont été accordées en 2017. Cette croissance trouve son reflet dans la perception des Français à l'égard des dispositifs biométriques, la méfiance historique pour ces technologies tendant ainsi à se dissiper.



Le CIAM, une nouvelle approche pour une vision client unifiée et sécurisée ?

Les solutions CIAM (Customer Identity and Access Management) visent à conjuguer expérience utilisateur et sécurité de façon optimale, par une réorganisation du système d'information des entreprises. En effet, ce type de solution permet aux entreprises de gérer de façon sécurisée le cycle de vie d'un utilisateur, tout en offrant une vision client unifiée en gérant les données personnelles dans un espace centralisé. Pour les banques, le CIAM est une occasion d'éliminer les silos, en regroupant les données personnelles des clients, quelle que soit leur utilisation *(gestion de comptes, crédits, assurance, etc.)* et leur canal *(agence, banque en ligne, application mobile, etc.)*. Cette approche CIAM peut donc permettre aux banques de proposer une gouvernance relation clients en conformité vis-à-vis du RGPD en satisfaisant le principe de « privacy by default » alors que la plupart des outils CRM du marché ne le peuvent pas.

Les API, la « lingua franca » du monde bancaire à l'heure de l'open banking ?

La protection des données bancaires fait face à de nouveaux défis avec l'éclosion de l'open banking. Ce phénomène transforme le paysage bancaire en introduisant de nouveaux acteurs, en instaurant de nouvelles règles du jeu et en modifiant les codes et usages relatifs aux données bancaires, jusqu'alors sanctuarisées. En effet, cette nouvelle stratégie bancaire se fonde sur la transparence et le partage des données entre acteurs de l'écosystème pour aboutir à un enrichissement des services proposés aux clients. La DSP2, qui donne un cadre règlementaire à cette tendance, impose l'usage d'interfaces de communication sécurisées pour partager ces données. Les banques sont désormais dans l'obligation de fournir ces interfaces pour permettre aux prestataires tiers de paiement d'accéder aux données de compte d'un client ou d'initier un paiement par exemple. La DSP2 impose de standardiser et de sécuriser les échanges entre acteurs, par l'intermédiaire d'API.

API

Une API (« Application Programming Interface » ou Interface de Programmation) est un ensemble normalisé de classes, de méthodes ou de fonctions mises en œuvre pour accéder à des services ou à des données. Ces interfaces doivent être évolutives, réutilisables et sécurisées, tout en offrant une facilité d'utilisation pour les développeurs informatiques.[33]

A l'heure actuelle, le mode de fonctionnement des prestataires tiers de service est basé sur le web scraping[34], une technique qui présente des risques pour la banque de voir son site en ligne ralenti voire à l'arrêt en cas de trop nombreuses requêtes. Par ailleurs, le web scraping ne garantit pas un usage proportionné des données clients ni le respect du principe de *minimisation* des données : lorsque le TPP obtient l'accès, certes consenti, au compte du client, il est en mesure de récupérer l'ensemble des informations disponibles sur les comptes, tels que les soldes, les virements, les prélèvements, ainsi que toutes les métadonnées associées *(lieu, date, heure, commerce, montant, montant du loyer, remboursements, emprunts, habitudes de consommation…)*. La mise en œuvre d'interfaces sécurisées cadrant l'accès aux données des clients est donc une mesure susceptible d'améliorer la confiance que portent les clients dans leur banque.

3.2. De nouveaux services mettant l'accent sur la confiance

En premier lieu, citons les services d'identité numérique, pierre angulaire de la confiance dans le monde numérique. Avec la multiplication des mots de passe à retenir pour les clients et les processus d'enrôlement laborieux, les solutions d'identité numériques visent à améliorer l'expérience utilisateur en permettant aux fournisseurs de services (les commerçants) de bénéficier d'un enrôlement préalablement réalisé par un fournisseur d'identité. Aujourd'hui différentes solutions de ce type coexistent, avec des niveaux de garantie associés disparates.

En s'appuyant notamment sur l'enrôlement sécurisé de leurs clients via les procédures de KYC, les banques sont en mesure de fournir des services d'identité numérique dotés d'un niveau de garantie significatif.

Leur légitimité s'appuie en outre sur deux autres piliers :

- La forte inclusion bancaire en France permet au secteur bancaire de couvrir une large partie de la population française. Cette large couverture

33 *API : définition issue du livre blanc "DSP2 & OPEN API : menaces et opportunités pour le secteur bancaire, en route vers l'Open-Banking ?", réalisé par Galitt en partenariat avec le cabinet DS Avocats.*

34 *Le web scraping est une technique consistant à extraire le contenu de sites web, via un script ou un programme qui va lire le code html, dans le but de le transformer pour permettre son utilisation dans un autre contexte.*

favorise logiquement l'adhésion d'un nombre conséquent d'utilisateurs au lancement d'un potentiel service d'identité numérique. Dans le cas d'un nombre d'adhésions important, les fournisseurs de service seraient incités à s'appuyer sur ce service pour enrôler leurs utilisateurs ;

- La fréquence de connexion des clients à leur espace bancaire en ligne prouve que ceux-ci sont accoutumés à s'authentifier auprès de leur banque. Ce constat laisse à penser que les clients adhéreraient à un moyen d'identification électronique fourni par la banque pour permettre l'accès à d'autres usages.

En se positionnant comme fournisseurs d'identité *(assurant les 3 processus suivants : processus d'identification, de délivrance du moyen d'identification électronique, et de vérification de l'authentification)*, les banques pourraient renforcer leur positionnement comme acteur du quotidien de confiance dans la vie des individus et ainsi conforter leur image de tiers de confiance, tout en leur permettant de fournir d'autres services numériques associés *(messagerie sécurisée, coffre-fort électronique, signature électronique…)*. A l'inverse, ne pas se positionner sur ce créneau comprend le risque de voir d'autres acteurs se positionner comme référence dans la fourniture d'identité numérique, jusqu'à venir empiéter sur la relation client des banques, voire rentrer en concurrence avec les banques dans la fourniture de services associés.

Etre fournisseur d'identité pour une banque est un choix stratégique, car elle est au cœur de la relation client. Cela peut être également un choix rémunérateur selon le business model mis en place. La banque peut choisir d'offrir un moyen d'identification électronique pour ses propres clients ou pour des partenaires clés *(cadre d'une offre single sign-on)* et cela sans adhérer à un écosystème de fédération d'identité.

L'intégration dans une fédération d'identité peut constituer un atout majeur dans le cas où la plateforme d'identité est un nœud européen eiDAS déclaré par un Etat, car alors l'acteur fournisseur d'identité peut adresser son offre à l'échelle européenne. Le fournisseur de service *(qui ne connaît pas le fournisseur d'identité que l'utilisateur a choisi)* peut payer l'écosystème pour bénéficier de la solution puis payer à chacune des connexions sur son site *(coût à l'usage)*. Cette solution de fédération d'identité permet aussi à la banque de mutualiser ses coûts sur des solutions d'identification et d'authentification conformes eIDAS, DSP2 et AMLD4, auxquelles elle doit se conformer. Enfin, en intégrant ce type d'écosystème, elle renforce son positionnement d'acteur légitime de confiance.

Notons qu'adopter la posture inverse, c'est-à-dire délaisser le terrain de l'identité numérique, peut aussi résulter d'un calcul économique qui devra être analysé. Déléguer la gestion des données personnelles à un tiers aurait l'avantage pour les banques d'abaisser leurs dépenses liées au coût de traitement sécurisé des données personnelles de leurs clients *(collecte, vérification, stockage…)* et aux charges induites par la mise en conformité au RGPD. Mais ce calcul économique court-termiste pourrait à plus long terme être dangereux au regard de la concurrence internationale très vive et à une évolution des usages et technologies numériques très rapide.

MODELE ECONOMIQUE DES SCHEMAS D'IDENTIFICATION ELECTRONIQUE, L'EXEMPLE ITALIEN SPID

Le règlement européen eIDAS prévoit la notification de schémas d'identification électronique nationaux à l'échelle européenne afin de renforcer la confiance des utilisateurs et d'étendre le périmètre d'utilisation des solutions en permettant la reconnaissance mutuelle des pays membres des moyens d'identification relatifs aux schémas notifiés. Parmi les états qui ont notifié auprès de la Commission Européenne un schéma d'identification électronique figure l'Italie, avec l'introduction de SPID[35]. Via SPID, le fournisseur de service peut notamment obtenir les données pivots nécessaires à l'authentification de ses utilisateurs, sur la base d'une identité vérifiée par le schéma italien. Pour l'authentification, le modèle de facturation proposé par les fournisseurs d'identité opérant dans le cadre du schéma SPID est décrit dans le tableau ci-dessous.[36]

Offre	Nombre d'utilisateurs inclus dans l'offre	Coût fixe (par utilisateur)	Coût par utilisateur supplémentaire
A l'unité	0	0 €	1,2 €
Small	50 K	50 K € (1,0 €)	1,2 €
Medium	250 K	200 K € (0,8 €)	1,0 €
Large	500 K	300 K € (0,6 €)	0,8 €
Extra Large	illimité	800 K €	n.a.

En Europe, plusieurs acteurs fournissent ou participent à la fourniture d'une solution d'identité numérique. Le cabinet de conseil Asquared les a recensés en février 2018[37].

35 *Le site du schéma d'identification électronique italien, disponible en italien et en allemand.*

36 *Ces tarifs, proposés en septembre 2017 par les fournisseurs d'identité, ont pu depuis évoluer.*

37 *Asquared, E-Identity Solutions in Europe – An european overview, 15 février 2018*

36 *Le site du schéma d'identification électronique italien, disponible en italien et en allemand.*

Parmi ces acteurs figurent de nombreuses banques. Certaines d'entre ellesproposent notamment des services dits de « Mobile ID », offrant :

- Des solutions d'identification sur mobile (eKYC), l'alternative à cette nouvelle étape d'identification pouvant être une dématérialisation sur mobile d'un titre d'identité (le cycle de vie de l'identité sur mobile est alors étroitement lié à celle du titre physique d'identité et est géré par le même fournisseur d'identité que celui du titre physique) ;
- Et/ou des solutions d'authentification par mobile.

Un exemple d'une solution de « mobile ID » créée par de grandes banques est celui du consortium itsme® en Belgique.

INTERVIEW

John Van Der Heyden

Responsable commercial et banque particulier chez BNP Paribas Fortis Belgique

En quoi consiste la solution itsme® ?

En Belgique, les opérateurs téléphoniques et les banques se sont associés pour créer la référence dans le domaine de l'identification mobile et du respect de la vie privée dans le monde numérique : **itsme®**. Grâce à cette application mobile, chaque citoyen belge est capable de s'**identifier** de manière non équivoque quand il se connecte à des applications numériques, de **confirmer** des transactions *(de paiement)* et même de signer des documents officiels.

L'application itsme® est universelle et permet de n'avoir qu'un seul mot de passe pour s'authentifier. Le client peut ainsi gérer ses informations et opérations bancaires d'une façon simple. Il lui suffit d'installer l'application, de créer son compte itsme® *(son identité numérique)*, puis de choisir un code à cinq chiffres. Pour certaines opérations, il lui est même possible d'utiliser la biométrie selon son modèle de Smartphone.

Les possibilités d'utilisation d'itsme® sont légion : s'enregistrer facilement comme nouveau client auprès d'une banque ou d'un commerçant, introduire une demande de document auprès de la commune, consulter les données de son assurance en ligne, signer des transactions de paiement dans « Easybanking » et pourquoi pas, dans le futur, sécuriser son domicile ou allumer son chauffage à distance *(Internet des objets)*, etc. L'application d'identité mobile itsme® est, depuis janvier 2018, officiellement **reconnue par le gouvernement**. Les retours de l'application sont extrêmement positifs. En un peu plus d'un an, plus de 500 000 Belges l'ont déjà adoptée.

Comment avez-vous réussi à la combiner avec les services de votre banque ?

Fortis n'oblige pas ses clients à utiliser itsme®. Ils peuvent également avoir recours aux processus déjà mis en place par la banque. Ceux-ci restent inchangés. Il n'y a donc pas d'interférence entre l'utilisation d'itsme® par les clients et les activités de la banque. C'est simplement un service additionnel.

Quels sont les avantages que votre banque tire de ce partenariat ?

Fortis a deux relations avec itsme®. Elle est membre de l'écosystème en tant que fournisseur d'identité et utilisateur des moyens d'authentification proposés par itsme®. Grâce au processus d'identification de ses clients *(KYC)* que la banque est légalement obligée de mettre en place, la banque possède aujourd'hui les identités vérifiées de tous ses clients. Lorsqu'un utilisateur souhaite créer son identité numérique itsme®, il peut le faire à partir de son identité vérifiée par la banque.

Aujourd'hui, presque toutes les banques proposent de s'authentifier et de signer via leur application mobile. Le service en lui-même n'est pas très différenciant à ce niveau et est difficile à rentabiliser. Cependant, créer un moyen d'authentification unique à toutes les banques permet de faire évoluer ses services plus rapidement et de faire une économie d'échelle. Le projet itsme® transforme un coût en une économie, et potentiellement deviendra une source de revenus dans les années à venir.

Comment gérez-vous les conséquences en termes de sécurité que l'utilisation d'une telle solution innovante peut engendrer ?

L'application offre **une triple sécurité** : itsme® fonctionne uniquement avec la combinaison adéquate entre Smartphone, carte SIM et code itsme® personnel. itsme® applique non seulement le Règlement européen pour l'identification électronique *(eIDAS)* et le Règlement général pour la protection des données *(RGPD)*, mais également les règles d'authentification forte *(SCA)* déterminées par la DSP2.

De plus, les données personnelles des utilisateurs sont dans une sorte de « coffre-fort » stocké par itsme®, certifié ISO 27001.

Quelle est votre stratégie pour les cinq ans à venir ? Quelles améliorations apporteriez-vous à l'application itsme® ?

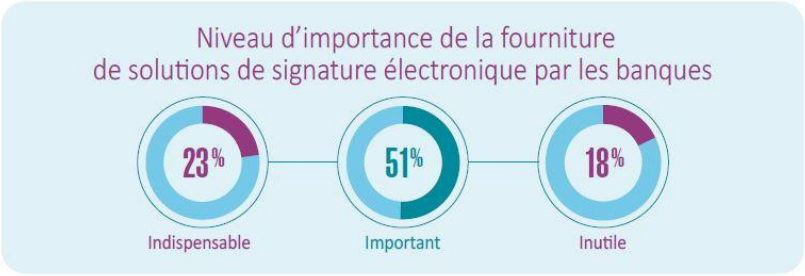
Dès son lancement, en mai 2017, itsme® proposait déjà 3 des 4 fonctionnalités que nous souhaitions mettre sur le marché : partager ses données d'identité vérifiées, se connecter et confirmer des paiements ou des ordres. La 4ème fonction est la signature électronique qualifiée. Nous travaillons pour le moment au développement de la solution et attendons la qualification de ce service au niveau européen.

D'ici au printemps 2019, la quasi-totalité du secteur bancaire adhérera à itsme®. D'autres secteurs ne restent pas inactifs non plus, tels que le secteur des assurances, les ventes aux enchères, l'immobilier, les mutualités...

Nous avons également des ambitions internationales : itsme® passe la frontière pour aller au Luxembourg. itsme® a bien démarré en Belgique, ce qui nous réjouit grandement, mais nous croyons que le produit a beaucoup plus de potentiel, y compris en dehors de nos frontières. C'est pourquoi, Belgian Mobile ID a conclu en mai 2018 un partenariat stratégique avec LuxTrust pour positionner itsme® sur le marché luxembourgeois.

La signature électronique

La signature électronique est une preuve électronique qu'une personne délivre pour affirmer son accord sur le contenu d'un document ou d'un ensemble de données lié à la signature. Elle consiste à garantir l'authenticité et l'intégrité du document dans le cadre d'une opération ou transaction entre deux parties, ainsi qu'à s'assurer de l'identité des signataires, à l'aide de certificats de signature électronique. La signature électronique peut être utilisée comme un procédé électronique de dématérialisation de la signature manuscrite avec une valeur probante plus ou moins forte selon le type de la signature et du certificat[38]. **Seule la signature qualifiée fournie par un prestataire de service qualifié a la même valeur qu'une signature manuscrite, avec une interopérabilité européenne**. Les autres niveaux de signatures simples et avancés bénéficient du principe de non-discrimination, mais à charge de la banque de démontrer la valeur de cette signature au niveau de la juridiction nationale du client[39]. La fourniture de ce service par les banques est jugée importante par une majorité de Français.



Le partage des données personnelles

Le fournisseur d'identité peut, au-delà des données nécessaires à l'identification et à l'authentification, récolter auprès de l'utilisateur des données personnelles annexes (feuille d'imposition par exemple dans le cadre d'une relation contrac- tuelle pour une offre de crédit amortissable de longue durée pour un bien immobilier), qu'il pourra transmettre par la suite à un fournisseur de données tiers, sous réserve du consentement explicite préalable de l'utilisateur et pour un intérêt légitime et proportionné. Pour l'utilisateur, l'intérêt est de faciliter la réalisation de démarches auprès du fournisseur de services nécessitant des données spécifiques.

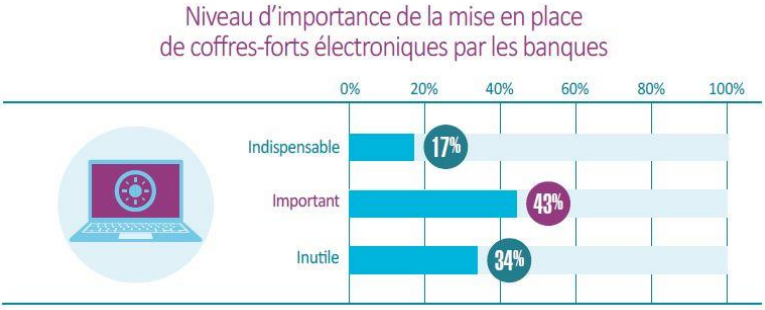
Le coffre-fort numérique

Une opportunité qui s'offre aux banques est également la création de

38 Pour plus d'informations, consulter la page du site de l'Union Européenne sur le sujet : What is an electronic signature ?
39 Pour plus d'éléments sur ces autres niveaux de signature, lire le guide archivage des preuves de signature électronique à la volée, par la FNTC.

coffres-forts numériques sécurisés *(et bientôt certifiés par l'ANSSI)* qu'elles mettent déjà à la disposition de leurs clients pour certaines. Les banques disposent de la technologie, du savoir-faire et de la légitimité nécessaire pour proposer ce type de service, de par la confiance que les Français leur accordent. Les banques françaises peuvent proposer de telles solutions depuis peu, car le décret sur les coffres-forts numériques a été signé en 2018[40]. Les coffres-forts numériques permettent aux banques de proposer à leurs clients un espace numérique de confiance, très sécurisé, pour stocker des éléments numérisés non nécessairement liés à des données bancaires *(factures, documents contractuels, diplômes, photos, etc.)*, en garantissant une protection en confidentialité et en intégrité et une disponibilité des informations.

Une part majoritaire des Français juge importante la mise en place de coffres-forts électroniques par les banques.



Certaines opportunités évoquées dans cette partie, doivent, pour libérer leur entière plus-value, être envisagées de manière combinée. C'est la stratégie adoptée par Docapost et Vialink, qui ont apporté leurs expertises respectives pour l'élaboration d'une plateforme de KYC à 360°, mêlant identité numérique, coffre-fort électronique, et machine learning41.

Ces différentes pistes, qu'elles traitent du fonctionnem bien de nouveaux services, démontrent donc que les d'alternatives pour se réinventer et renforcer la co encontre.

Conclusion

Le marché du paiement est en pleine évolution, en témoigne la vague de réglementations européennes qui vise à sécuriser le monde numérique, contraignant ainsi les banques à s'adapter. Mais plus qu'une contrainte, ce nouvel

40 *Legifrance : Décret n° 2018-418 du 30 mai 2018 relatif aux modalités de mise en oeuvre du service de coffre-fort numérique.*

41 *Communiqué de presse Docapost et Vialink sur la création d'une plateforme unique d'identification totale (KYC), 15 octobre 2018.*

arsenal règlementaire doit être perçu par les banques comme une occasion d'amorcer une réflexion sur leurs activités et sur la relation qu'elles entretiennent avec leurs clients. Ceux-ci sont désormais sensibles aux enjeux de sécurité liés aux usages numériques. En tant qu'acteur bénéficiant de la confiance de ses clients, la banque a un rôle à jouer pour renforcer la sécurité du monde numérique, en protégeant les données personnelles de ses clients. En réalité, adopter cette démarche permet au monde bancaire de se saisir d'une double opportunité, défensive et offensive : maintenir sa légitimité en tant qu'acteur de confiance et investiguer de nouveaux axes commerciaux.

Pour transformer avec succès cette opportunité, les banques ne devront pas perdre de vue les attentes de clients en termes d'autonomie, de fluidité et de personnalisation de service. A ce titre, adopter une démarche « customer in control » pour la mise en œuvre de services qui traitent de sujets aussi sensibles que la gestion des données personnelles prend ici tout son sens.

Laisser la main au client sur le paramétrage d'un service n'est pas une nouveauté pour les banques qui mettent en œuvre depuis quelques années maintenant des services dits de « selfcare » permettant à leurs clients de paramétrer les modalités d'utilisation de leurs produits bancaires via une application mobile ou sur leur espace bancaire en ligne. En revanche, étendre ce principe à l'identité numérique du client constitue une piste de réflexion dans cette quête de réinvention que les banques doivent initier. L'intérêt actuel des clients pour la protection des données personnelles est de nature à faciliter l'adoption d'un tel service. Au-delà des services de coffre-fort numérique, qui proposent de conserver de manière sécurisée des documents, les banques pourraient fournir une plateforme de service qui gérerait les droits des utilisateurs et les consentements accordés par les clients pour un usage limité ou non de leurs données personnelles.

Le client aurait la possibilité de configurer, au travers d'une application mobile, et après avoir accepté de confier la gestion de son identité numérique à un prestataire de services tiers, les accès à ses données personnelles, avec une capacité pour le client de configurer des autorisations d'accès ou des restrictions d'accès à certaines catégories de données personnelles.

Dans cette perspective, nous imaginons une initiative des acteurs bancaires pour élaborer une plateforme de ce type au travers d'une infrastructure mutualisée. La banque serait donc fournisseur d'identité et chargée de la gestion des données personnelles des clients.

Outre l'intérêt d'une telle démarche vis-à-vis des attentes clients et des enjeux du monde numérique, les banques doivent voir dans la mutation actuelle de leur secteur une occasion de devenir un acteur indispensable de l'expérience client dans la sphère digitale, tous domaines d'activité confondus.

A propos des auteurs

Nathalie Launay - *Consultante Règlementaire*

Après 15 ans chez les leaders de la carte et de l'identité, Nathalie a consolidé son expertise technique vers l'identité numérique avec des missions de consultant pour des PME et une start-up, tout en affûtant ses connaissances règlementaires transectorielles et sectorielles. En 2018, elle a rejoint Galitt pour accompagner les acteurs du paiement dans leurs nouveaux usages du numérique sur la base d'une identité numérique fiable et de services de confiance.

Cécile Rouhaud - *Practice Manager- Observatoires Benchmarks Veille*

Cécile est en charge de l'activité études quantitatives auprès des consommateurs et des professionnels. Elle intervient notamment dans la réalisation des Observatoires tels que l'Observatoire du PAiement Mobile et Sans COntact (OPAMSCO) et l'Observatoire des nouveaux MOdes D'Authentification (OMODA).

Gwendal Boëdec - *Payment Consultant*

Diplômé de Sciences Po Rennes et de l'Ecole de Guerre Economique (EGE), Gwendal est actuellement Consultant au sein de la Business Unit Payment Consulting de Galitt, travaillant principalement sur des sujets liés aux innovations et à la réglementation dans le secteur du paiement.

Oriane Perrachon - *Chargée d'études Marketing*

Principale contributrice de ce livre blanc, Oriane a réalisé son stage de fin d'études chez Galitt, dans le cadre de son Master 2 à l'ISIT Paris.

Plusieurs collaborateurs de Galitt sont intervenus sur le projet :

Emmanuel Caron : *Practice Manager*

Nathalie Gaudin : *Practice Manager*

Rémi Gitzinger : *Directeur Exécutif*

Alexandre Martin : *Practice Manager*

Isabelle Pujadas : *Directrice de la communication*

Rendre les paiements simples, efficaces et sûrs, dans la vie de tous les jours.

galitt
a Sopra Steria company

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