

Introduction de Frédéric Oudéa

Président de la Fédération bancaire française
15 octobre 2019 - FBF

-

« Risques cyber : où placer le curseur entre innovation et sécurité ? »

Bonjour à toutes, bonjour à tous,

Je suis extrêmement heureux, en tant que Président de la Fédération bancaire française, d'ouvrir cette matinée d'échanges autour d'un thème qui s'est imposé dans notre société, la cybersécurité. En quelques années seulement, nos modes de consommation et de communication traditionnels ont connu une véritable révolution, et internet s'est imposé comme un levier de transformation du fonctionnement de notre société. Etats, acteurs économiques, entreprises, citoyens, le monde entier a été bouleversé par les opportunités – et leurs pendents, les risques – offerts par la révolution digitale.

« Risques cyber : où placer le curseur entre innovation et sécurité ? ». La question est vaste, et les sujets qu'elle soulève, nombreux. Ce thème n'a pas de frontières ; les nouvelles technologies ont fait naître de nouveaux enjeux de souveraineté, la souveraineté numérique, et avec elle s'imposent les questions d'opportunités, d'enjeux humains et sécuritaires.

Quand on sait que la cybercriminalité coûte, chaque année, 3,6Md€¹ aux entreprises françaises, que 98% des attaques réussies le sont en moins d'une semaine, et qu'il faut 78 jours en moyenne pour les détecter, nous mesurons peut-être mieux le défi auquel nous faisons face. Et ces chiffres datent de 2016. Avec le développement de plus en plus rapide des technologies, et donc des risques qui y sont liés, ces chiffres n'auront de cesse que d'augmenter. Notre souveraineté est intimement liée à la puissance de nos outils technologiques.

¹ Enquête PWC 2016

Si l'enjeu de souveraineté numérique fut un temps une préoccupation uniquement pour le secteur des nouvelles technologies, aujourd'hui il touche toutes les industries. Cet événement est ainsi l'occasion de fédérer des acteurs de professions différentes, concernés par les métamorphoses digitales de notre société, et d'en faire connaître les enjeux auprès de chacun d'entre nous, auprès des citoyens, des pouvoirs publics, des entreprises.

Alors, où placer le curseur entre innovation et sécurité ?

C'est de l'industrie bancaire - celle que je connais le mieux et que je vois se transformer chaque jour, dont je vais vous parler. La banque est une industrie qui refuse de choisir entre innovation et sécurité, et dont l'un des enjeux est justement de maintenir cet équilibre. Les banques sont des acteurs dont l'activité dépend beaucoup de la technologie et qui ont dans leur ADN une culture de l'innovation permanente. Qui, ici, n'a pas son application bancaire² installée sur son smartphone ? Qui ne la consulte pas au moins une fois par jour ? Qui n'a jamais envie de pouvoir connaître, à l'instant T, et peu importe où il se trouve, l'état de son compte en banque ? Les Français ont constaté et approuvent largement ces innovations portées par les banques. 8 sur 10 jugent l'évolution proposée par les banques positive³. La banque est un service de proximité, qui fait de l'innovation un moyen de renforcer son modèle de banque relationnelle.

Notre industrie teste et utilise déjà les technologies innovantes : l'intelligence artificielle au service de la connaissance client, ou des sujets de conformité par exemple ; l'utilisation de la blockchain dans le trade finance, le développement des infrastructures cloud. Les banques investissent des milliards d'euros par an et ont lancé des projets de grande ampleur pour utiliser ces nouvelles technologies, avec un double but : proposer à leurs clients des services et solutions toujours plus innovantes, en temps réel, et gagner en efficacité et en sécurité.

Nous sommes une industrie de pointe et nous vivons une période de transformation de notre écosystème avec l'émergence de nouveaux acteurs qui participent aux mutations des codes et usages de nos clients. Avec les industriels, les fintechs, les

² Les applis bancaires parmi les trois applis mobiles les plus consultées, derrière la météo et les réseaux sociaux (sondage Opinion Way, mai 2016).

³ « Les Français, leur banque, leurs attentes », étude FBF menée avec l'IFOP, 2019

banques forment cet écosystème. Nous avons une ambition partagée, développer des services financiers simples et utiles aux clients, et c'est avec cet objectif que nous travaillons ensemble pour nous adapter et utiliser ces nouvelles technologies à leur service. La relation est réciproque, le cercle vertueux. Les banques bénéficient de l'agilité des fintechs. Mais l'inverse est tout aussi vrai, notamment en termes de sécurité et de puissance : les banques mettent à leur disposition des labs, des incubateurs, proposent des partenariats, financent leur développement. Prenez l'agrégation de comptes. Elle est née dans les fintechs, a grandi dans les banques, par des incubateurs qui ont permis le financement de ce qui n'était encore alors qu'un projet, et aujourd'hui les banques proposent ce service. Elles l'ont amélioré, standardisé et sécurisé afin de protéger les clients.

Alors, « Innovation et sécurité, où placer le curseur ? ». L'innovation est notre moteur, et nous sommes moteur de l'innovation. Nous participons à la transformation de l'écosystème, nous sommes des fers de lance de l'innovation technologique. Et nous avons conscience que cette innovation est aussi source de risques. Nos nouveaux modes de communication et de consommation – réseaux sociaux, mails, banque à distance, agrégation – resteront une opportunité tant qu'ils garantiront une protection maximale des clients. Jamais nous ne transigerons sur la sécurité de leurs fonds et de leurs données. Nous ne devrions d'ailleurs pas parler de « risque cyber », mais de « protection cyber ». C'est là qu'est le défi. L'innovation, tout comme la technologie n'est qu'un moyen de mieux servir nos clients. Cependant, elle doit être maîtrisée et nous nous devons partager les bonnes pratiques en termes de sécurité.

Les banques ont toujours été, et seront toujours intransigeantes sur la sécurité des fonds et des données de leurs clients. Cependant, l'approche de la confidentialité dans les mondes numérique et bancaire n'est pas du tout la même et nous nous devons d'accompagner les évolutions technologiques et numériques en continuant à préserver la sécurité des échanges et la confiance des clients. La cybersécurité est un enjeu fondamental du monde bancaire d'aujourd'hui. Ce devoir de sécurité est essentiel. Les données clients sont l'actif numéro 1 des banques et garantir la sécurité ces données est le socle de la relation de tiers de confiance établie avec tous leurs clients, entreprises comme particuliers. 98% des entreprises estiment que la transformation numérique a un impact sur la sécurité des systèmes d'information et

des données⁴ et 68% des Français ont confiance dans la sécurisation de leurs données personnelles par leur banque⁵. Nos efforts en matière de protection des données sont reconnus, et il nous est absolument indispensable de continuer à œuvrer en ce sens.

La révolution numérique a donné une immense valeur à la donnée. Nos données ont un prix et les protéger est un devoir pour les entreprises. Une entreprise qui ne respecterait pas la Réglementation européenne sur la protection des données à caractère personnel, la RGPD, s'expose d'ailleurs à une amende pouvant aller jusqu'à 20M€ ou 4% du CA (annuel mondial).

Les banques investissent massivement à la fois pour préserver les données personnelles des clients mais aussi l'intégrité du système financier, notamment des paiements. Prenons un exemple concret : La directive des services de paiement (DSP2) permet que soient accessibles, gratuitement, les données des comptes de paiement des clients, dans le cadre de l'agrégation et de l'initiation de paiement. Fidèles à leurs valeurs d'innovation dans la sécurité et d'accompagnement de leurs clients, les banques ont développé des API pour l'accès aux comptes de paiements des clients par ces agrégateurs et initiateurs de paiement. Ces interfaces, conformes à la DSP2 et aux normes de sécurité, garantissent la sécurité des données et des fonds des clients.

La question de la protection des données et des fonds représente un enjeu qui dépasse largement les frontières de la France et de l'Europe. Nous devons réfléchir ensemble au modèle économique que nous souhaitons, notamment au sujet de la donnée. L'apparition dans le secteur financier des grands acteurs numériques extra-européens, américains et chinois notamment, pose la triple question de la souveraineté, de l'indépendance et de la protection des données. Nous sommes face à des choix de société, à des choix politiques. L'Europe ne doit pas se condamner à devenir une colonie du monde numérique financier.

Il nous paraît ainsi indispensable que tous les acteurs partageant un même segment d'activité, proposant des services semblables, travaillent dans un même sens. Et cela passe aussi par une uniformisation des règles, des exigences et des contrôles.

⁴ Opinionway pour le CESIN (Club des Experts de la Sécurité de l'Information et du Numérique)

⁵ « Les Français, leur banque, leurs attentes », étude FBF menée avec l'IFOP, 2019

L'industrie française, au sens large, doit apprendre à travailler ensemble. Nous ne pouvons plus envisager la régulation a posteriori.

Anticiper les enjeux sécuritaires permettrait de réduire le risque cyber, pour ne faire des nouvelles technologies qu'un outil puissant, capable d'assurer la sécurisation de l'accès aux données des clients, de protéger les systèmes d'information, de sécuriser les moyens de paiements et l'accès à la banque en ligne, de lutter, au sens large, contre la fraude. Les nouvelles technologies présentent une opportunité mais aussi des risques, alors que la Banque s'ouvre pour mieux innover. Or, le facteur humain est très souvent responsable des incidents de cybersécurité – tous secteurs confondus, 35% des incidents de cybersécurité ont été générés, malgré eux, par des collaborateurs⁶. Nous mesurons à quel point il est primordial de sensibiliser les salariés. Aujourd'hui, encore 50% des PME reconnaissent ainsi ne pas former leurs employés⁷. Pourtant, la formation est stratégique pour les entreprises. Elle permet de faire évoluer les compétences, et si l'entreprise est certes le moteur de l'économie, sans l'humain, elle n'est rien. L'humain est central. Il est et sera toujours indispensable. Les banques consacrent 4,5% de leur masse salariale à la formation. Presque deux fois plus que la moyenne des entreprises françaises. Elles sensibilisent régulièrement leurs collaborateurs, mais aussi leurs clients, particuliers, PME/TPE, ETI, grandes entreprises, aux risques cyber. Les banques vivent et accompagnent les clients dans l'accélération digitale. Elles forment leurs collaborateurs afin qu'ils puissent répondre aux nouveaux usages des consommateurs, et travaillent main dans la main avec les nouveaux acteurs de l'écosystème

La dimension humaine est essentielle de la stratégie des établissements bancaires pour préparer et accompagner les transformations digitales et anticiper les risques. Les métiers vont évoluer en même temps que l'environnement, mais l'humain restera au centre des transformations. Il n'appartient qu'à nous de développer encore la coopération entre l'homme et la machine, et d'unir nos forces vers un but commun : la lutte contre les risques cyber.

⁶ Proofpoint, rapport 2017

⁷ Proofpoint, rapport 2017

La transformation numérique de notre industrie est un défi majeur. Mais un défi dont elle est aussi le moteur. Elle travaille en permanence à l'innovation de demain avec l'ensemble des acteurs de l'écosystème, envers lesquels elle n'a qu'une exigence : ne pas subir une distorsion de concurrence qui se symboliserait par une baisse de la sécurisation des fonds et des données. La révolution numérique est et doit rester une opportunité. Nous ne devons pas l'appréhender comme une menace. Notre vrai combat, celui qui doit déterminer nos choix, c'est la sécurité. L'innovation est une force, et un enjeu de souveraineté. De la donnée personnelle du particulier, aux données confidentielles de l'Etat, en passant par celles des entreprises, les enjeux cyber concernent chacun d'entre nous et sont stratégiques. Nous devons continuer à développer nos nouveaux projets et à promouvoir les enjeux de la souveraineté numérique en France et hors de nos frontières. Le défi est grand, et c'est ensemble que nous y arriverons. Je vous remercie sincèrement d'avoir accepté de partager avec nous cette matinée d'échanges.