Banques, FinTech, AssurTech… L’union des données client fait-elle la force ?

Dans un contexte où la réglementation bancaire européenne s’intensifie et où les services compliance engagent des coûts financiers et humains de plus en plus importants, ne serait-il pas temps de créer un fichier commun de KYC, d’incidents AML et de fraudes, ouvert à toutes les banques, FinTech et assurances ?

---

12 février 2018

Depuis son entrée en vigueur en août 2015, la Loi Macron facilite la mobilité bancaire. Néanmoins, le premier pas vers un changement de banque est le passage obligé du KYC : le " Know Your Customer ", étape où le client justifie son identité auprès de l’établissement choisi. De quoi laisser penser qu'il serait temps de créer un fichier commun ouvert à tous les acteurs.

Entre digitalisation et réglementation

La digitalisation du secteur bancaire impacte l’ensemble des procédures administratives. Or, digitaliser le KYC peut constituer un frein pour les générations qui ne sont pas nées avec le numérique, et donc restreindre leur accès aux services bancaires. En impactant très fortement l'expérience client, le KYC complique l’entrée en relation avec les banques car les documents exigés sont de plus en plus nombreux. Il devient alors nécessaire de faciliter l’usage des services financiers digitaux pour s’assurer qu’ils restent accessibles à tous, donc en simplifiant et en fluidifiant l’inscription.

En parallèle, les directives européennes comme MiFID II, AML4 ou DSP2 annoncent le début d’une nouvelle ère qui va amplifier les vérifications, les analyses et la nécessité de croiser les informations pour mieux contrôler la fraude et les délits d’initié, mais également les financements du terrorisme et le blanchiment d’argent. Un vaste mouvement réglementaire est déjà amorcé et va avoir un fort impact sur l’expérience utilisateur et les procédures internes.

Dans ce contexte, alors que les établissements bancaires, FinTech et assureurs récoltent séparément les mêmes données personnelles des mêmes clients, ne serait-il pas judicieux de travailler de concert sur un fichier commun aux établissements régulés regroupant KYC, AML et fraudes au sens large ?

Mutualiser les données KYC pour réduire les coûts

Selon une étude menée par Thomson Reuters, les banques britanniques dépensent en moyenne 47,8 millions d'euros par an pour la conformité KYC. Un coût important qu'une base de KYC commune aux banques, assurances et Fintech permettrait de réduire.

Sans aller vers un modèle de Regtech qui consisterait à convaincre les utilisateurs de déposer leurs données puis de leur remettre une clé qui permettrait à n'importe quelle banque de les récupérer, l'idée serait de créer un Groupement d'Intérêt Économique (GIE) où tous les acteurs régulés déposeraient leurs données KYC pour mieux pouvoir les utiliser sans coût de traitement supplémentaire. La valeur de la data d'un client ne se trouve pas dans le KYC, mais dans l'étude de l'usage qu'il fait de son compte bancaire. En partageant les informations administratives et en mutualisant les coûts de traitement, les services compliances pourraient se focaliser sur des tâches à plus forte valeur ajoutée.

Vers une base KYC commune ?

Aujourd'hui un client qui souscrit à un compte bancaire et à un contrat d'assurance dans le même groupe doit fournir ses documents KYC à deux reprises. En effet, malgré une entité administrative unique, ce sont des branches juridiques distinctes qui contractualisent avec le client. En termes d'expérience utilisateur, cela n'a pas de sens. Centraliser les KYC et mutualiser les informations permettrait alors de mieux accompagner le client, de l'aider dans l'ouverture de services digitaux et donc de lui offrir une meilleure expérience.

De la même manière qu'un fichier FICP a été créé, mettre en place un fichier KYC commun permettrait de mieux appréhender les risques relatifs à l'inscription d'un nouveau client et à l'utilisation des services. En partageant ainsi les données collectées et en offrant la possibilité à chaque banque de déposer des incidents AML, la lutte contre la fraude serait à la fois plus effective et moins coûteuse.

Création d'un compte digital personnel

Un tel fichier doit être mis en place par l'impulsion de l'Etat ou bien par les banques, FinTech ou assureurs privés. Si l'Etat décide de prendre en charge ce projet, il s'inscrira sûrement dans la continuité de son chantier de digitalisation mais il faudra compter de nombreuses années avant qu'il ne voit le jour.

Au contraire, si le secteur privé était à l'origine de cette initiative, il serait plus facile de disposer rapidement d'une base KYC conséquente. Ainsi, chaque établissement – que ce soit des assureurs, des banques ou bien des FinTech – réunirait ses KYC, reliées en blockchain, sur une base commune. Un client qui souhaiterait alors changer de banque, souscrire à une nouvelle offre d'assurance, ouvrir un compte dans une néobanque, louer un appartement, souscrire un forfait mobile… n'aurait plus qu'à entrer son numéro de sécurité social et par un

système de token et de credentials, viendrait donner son accord et poser ses limites d'utilisation.

De nombreux philosophes, dont Gaspard Koenig, s'interrogent sur la valeur des données personnelles et la possibilité pour les citoyens de choisir celles qu'ils souhaitent vendre ou conserver. En construisant un premier socle concentré sur l'identité du citoyen (KYC), des acteurs du secteur bancaires, assureurs et FinTech, pourraient rendre ces idées tangibles, puis contrôler et préserver ce qu'elles ont de plus précieux, la data.

Avec l'explosion des néobanques, il n'est plus rare de voir un utilisateur à la fois client d'une banque et de différentes néobanques. Pour lutter contre l'usage possiblement frauduleux des comptes, les établissements ont ainsi tout intérêt à mutualiser les données clients. A partir d'un numéro de sécurité social, tous les acteurs autorisés pourraient alors obtenir les documents indispensables à l'ouverture d'un compte ou à la souscription d'un contrat d'assurance et récupérer un certain nombre d'incidents liés à des utilisateurs.

Article écrit par Iris Maignan