Note de conjoncture

Biométrie : l'incontournable des paiements ?

Empreinte digitale, voix, visage, rétine de l'œil… Les moyens d'authentification biométriques se développent très fortement depuis plusieurs années, portés par un élan d'innovations technologiques sans précédent. Entre sécurisation des transactions et simplification des usages, la biométrie semble porteuse de nombreuses promesses sur le marché des paiements… au point de devenir incontournable ?

93% des consommateurs sont séduits et prêts à adopter la biométrie mobile ; 9 banques sur 10 déclarent vouloir adopter cette technologie [1]. Un véritable plébiscite confirmé par le nombre de paiements mobiles authentifiés via biométrie qui serait passé de 600 millions en 2016 à près de 2 milliards en 2017[2], soit une augmentation de +300%. A l'ère du *wallet* et du paiement P2P, la biométrie se démocratise progressivement, notamment grâce à l'avènement du smartphone.

L'innovation au cœur des paiements

Jusqu'alors très couteuse et souvent perfectible, la biométrie s'octroie une place de plus en plus grande dans la sphère des paiements à travers nos smartphones. Objet incontournable du quotidien, les acteurs du marché ont su tirer parti des possibilités offertes par le mobile, à l'image de :

- L'application **Cdiscount**, qui propose à ses utilisateurs de régler leurs achats via reconnaissance faciale,
- **ApplePay**, qui permet aux possesseurs d'iPhone de régler leurs achats via sa technologie de lecture d'empreinte digitale TouchID,
- **TalkToPay**, la solution de reconnaissance vocale de La Banque Postale disponible pour les paiements à distance.

> Actuellement 150 millions, on estime à 600 millions le nombre d'utilisateurs de la biométrie vocale d'ici à 2020[1]

Au-delà du smartphone, d'autres situations peuvent également appeler un facteur biométrique :

- La reconnaissance vocale **à la maison**, pour rembourser un ami par exemple (via une enceinte Google Home et Google Pay),
- La reconnaissance vocale **dans la voiture**, pour payer son plein d'essence sans même quitter son volant (via Android Auto),
- La reconnaissance faciale **au restaurant**, pour régler son déjeuner sans sortir son portefeuille : en Chine, Alipay propose ainsi aux clients des restaurants KFC de sourire afin de payer leur repas (« Smile to pay »),
- La reconnaissance d'empreinte digitale sur les cartes de paiement dotées de lecteurs (celles distribuées par la Société Générale par exemple), pour régler ses achats **en magasin** sans saisir son code PIN.

Visa et **Mastercard** ont aussi clairement fait le choix de la biométrie. Fin 2016, Visa s'est allié à BioConnect afin de développer une application d'authentification biométrique multi-facteurs (empreinte digitale, voix, iris…). De son côté, Mastercard ambitionne de faire de la biométrie « *le standard d'authentification des paiements*

[1] « *Guidelines for Deploying Mobile Biometrics in Financial Services* », Opus Research & Mastercard

[2] « *Mobile biometric payment volumes to triple in 2017 to nearly 2B* », Juniper Research

numériques d'ici la mi-2019 » grâce à son service MasterCard Security Check, déjà disponible dans 37 pays. D'autres acteurs proposent également leurs solutions biométriques, à l'image d'Idemia (ex OT-Morpho), Gemalto, Atos, Ingenico ou encore Nuance.

Innovant, le secteur des paiements a su trouver en la biométrie le moyen de dynamiser le processus de paiement… au détriment de la sécurité ?

La biométrie, une réponse aux exigences de la DSP2…

La nouvelle Directive sur les Services de Paiement (**DSP2**), fraîchement entrée en vigueur début 2018, rend obligatoire la mise en place d'un mécanisme d'authentification forte pour les paiements en ligne de plus de 30€. Une mesure supplémentaire du législateur visant à renforcer la sécurité des paiements. Ce système impose l'utilisation d'au moins deux éléments d'authentification (2FA ou Two Factors Authentication) pour vérifier l'identité du client :

- Un élément **connu** uniquement du client (« Ce que je sais »), tel un mot de passe par exemple
- Un élément **détenu** uniquement par le client (« Ce que je possède »), comme un smartphone
- Un élément **caractérisant** le client (« Ce que je suis »), telle une empreinte digitale
- Un élément **définissant** le client (« Ce que je fais »), à travers son comportement, ses habitudes (géolocalisation, fréquentation de sites, horaires de connexion…)

La Commission Européenne est même allée plus loin en demandant aux banques d'abandonner le système de validation des paiements en ligne par SMS d'ici septembre 2019, estimant celui-ci pas suffisamment sécurisé. Un objectif très (trop ?) ambitieux lorsque l'on sait que 85% des contrôles renforcés pour des achats online sont réalisés via SMS-OTP (« One Time Password »).

En cela, la biométrie peut ainsi jouer un rôle central dans la recherche d'un **compromis entre sécurité et facilité d'utilisation**, en phase avec la digitalisation croissante des modes de vie.

… et aux besoins des clients

Face aux risques de fraude et de cybercriminalité, la sécurité des transactions constitue plus que jamais un enjeu majeur vis-à-vis des clients dans le cadre de l'intégration de la biométrie au processus de paiement. La notion d'acceptabilité du client vis-à-vis de l'enregistrement de ses données biométriques sera d'autant plus forte que les solutions proposées seront adaptées aux besoins du client, qu'il s'agisse du consommateur, du commerçant ou de l'établissement bancaire.

> 79% des consommateurs français considèrent que « *les solutions biométriques offrent un moyen sûr d'authentification* »[3]

Les technologies proposées aujourd'hui permettent, notamment, de :

- **Fluidifier et accélérer le processus de paiement**, diminuant ainsi considérablement le taux d'abandon des achats en ligne,
- Adapter le **parcours client en fonction du contexte**, comme basculer d'une authentification vocale à une lecture d'empreinte digitale en présence d'un environnement trop bruyant par exemple,
- Améliorer la **détection de fraudes** grâce à la biométrie comportementale (profil du client), permettant la mise en place d'outils d'analyse en temps réel afin d'autoriser ou bloquer une transaction.

[3] « *Digital Payments Study* », 2017 - Visa

Vers un « standard biométrique » ?

Et si l'avenir de l'authentification passait par la définition d'un standard commun à l'ensemble du marché ? C'est l'objectif que s'est fixé l'Alliance FIDO[4] en lançant le « *Biometric Certification Component Program* », destiné à normaliser les techniques d'authentification biométrique sur une base interopérable.

A l'image des standards autour de l'agrégation de données bancaires (API / DSP2), la mise en place de normes communes d'authentification biométrique à l'ensemble du marché permettrait d'élever le niveau général de la qualité et de la fiabilité des équipements biométriques. Ceci en vue de fluidifier l'expérience et la mobilité client, simplifier la gestion des données et accélérer l'innovation autour de la biométrie.

Une ambition qui pourrait se révéler prometteuse, à la seule condition que la donnée recueillie soit suffisamment fiable et sécurisée.

La donnée biométrique, une donnée comme les autres ?

Exploitant des caractéristiques biologiques, voire comportementales, la biométrie interroge quant à la qualité de ces données. Par définition uniques et (pour la plupart) permanentes, elles sont presque impossibles à modifier, notamment si elles sont compromises : en cas de vol de son empreinte digitale, un consommateur ne pourra dès lors se contenter de la modifier comme il aurait changé un mot de passe. Alors même que les données biométriques assurent une fiabilité maximale, celles-ci apportent un paradoxe quant à leur sécurité !

Le RGPD (Règlement Général sur la Protection des Données) consacre d'ailleurs les données biométriques parmi les données sensibles, comme les données de santé ou celles relatives à l'orientation sexuelle.

Au regard de ces données très personnelles, une question demeure : la biométrie garantit-elle la confidentialité des données ? A l'heure où de nombreuses initiatives voient le jour, le paiement par authentification biométrique doit encore progresser afin de devenir véritablement incontournable dans la sphère des paiements.

Imane EL MANSOURI, Consultante senior
Nicolas BOISVILLIERS, Manager

[4] Alliance Fast IDentity Online (FIDO), consortium industriel regroupant + 260 membres, dont Amazon, PayPal, Gemalto, Visa, Idemia ou encore Alibaba

siltéa & Talan Consulting

Forte de son expertise reconnue des métiers de la banque, Siltéa accompagne ses clients dans la transformation de leurs filières & offres paiement.

À travers sa practice « Moyens de paiement et monétique » et ses profils experts, Siltéa associe les approches digitale, organisationnelle et innovante des moyens de paiement, tout en plaçant le « parcours client multicanal » au centre de sa démarche.

Nicolas BOISVILLIERS
Manager
+33 (0)6 24 18 17 83
nicolas.boisvilliers@siltea.com

Sophie DUMONT
Responsable communication
+33 (0)1 42 68 74 48
sophie.dumont@siltea.com