
Avec la reconnaissance faciale, la biométrie devient « grand public »

Description

Conçue des fins de sécurité ou de défense, cette technique d'authentification et d'identification par le corps trouve de nouveaux débouchés commerciaux. La reconnaissance digitale ou faciale remplace les mots de passe et les codes, simplifiant le verrouillage des terminaux, l'accès aux services et les modes de paiement.

Les empreintes digitales, les veines de la main, l'iris, le visage, la voix ou l'ADN deviennent des données d'identification et d'authentification comme les autres grâce au progrès de la numérisation. L'empreinte digitale remplace le badge d'entreprise, d'ordinaire elle se substitue au code PIN. À la pointe de l'expérience utilisateur, Apple, le premier, en 2013, a équipé son iPhone 5 de la fonction Touch ID permettant le verrouillage de l'appareil par la reconnaissance de l'empreinte digitale. Puis, en 2017, l'iPhone X sera équipé de la fonction Face ID, permettant l'identification du propriétaire de l'appareil par une image en 3D de son visage, même si l'on ajoute une paire de lunettes ou si l'on change de coupe de cheveux.

Authentification vs identification

La biométrie, ou « mesure du corps humain », sera ici peu la méthode la plus couramment employée pour identifier ou authentifier une personne à partir de ses caractéristiques biologiques uniques. Hier encore réservée aux missions de la police ou de l'armée, cette technologie, aujourd'hui moins onéreuse et moins complexe, devient « grand public » pour assurer la sécurité des transactions, des documents d'identité et des échanges sur internet. Dans le cadre d'une identification biométrique, il s'agit de répondre à la question : « Qui êtes-vous ? », comme on peut le lire sur le site de l'un des leaders mondiaux du secteur, Gemalto (filiale du groupe français Thales), en comparant une donnée biométrique d'une personne, comme la photo de visage, l'enregistrement de la voix ou l'image d'une empreinte digitale, avec les données d'autres personnes sauvegardées dans une base de données centralisée. L'authentification biométrique, quant à elle, consiste à vérifier une identité en établissant la ressemblance entre les caractéristiques biométriques d'une personne et un modèle de référence biométrique de cette même personne, enregistré sur un support autonome, comme une carte puce, et n'est donc pas obligatoirement consigné dans une base de données, afin de répondre à la question : « Êtes-vous bien Madame Z ? ».

La biométrie ne s'arrête pas aux mesures réalisées sur des données physiologiques, mais s'appuie également sur des données comportementales, annonce la société Gemalto.

Les données physiologiques sont celles liées à la morphologie : empreintes digitales ; forme du visage, de la main ou du doigt ; réseau veineux ; l'iris (iris et rétine) ou la biologie : ADN, sang, salive, urine qui peuvent servir dans le cadre d'une investigation criminelle ou un contrôle anti-dopage. Quant aux données comportementales, outre la reconnaissance de la voix, la biométrie parvient à analyser la dynamique des signatures (vitesse de déplacement du stylo, accélérations, pression exercée, inclinaison), la frappe sur le clavier d'un ordinateur, la démarche, le bruit des pas, la gestuelle. Ces caractéristiques permettent ainsi de savoir si un enfant, une femme ou un homme. Cependant, la biométrie ne parvient pas encore à garantir le même degré de fiabilité dans la mesure de ces diverses données. L'identification d'une personne à partir de ses données physiologiques : même si celles-ci changent au cours de l'existence reste ce jour plus performante que celle qui est liée à ses attitudes. Afin de réduire la marge d'erreur, liée aux « faux rejets » ou aux « fausses acceptations », la combinaison de plusieurs mesures (le visage et l'iris ou l'iris et les empreintes digitales) peut être effectuée : on parle alors de « biométrie multimodale ».

Pour ouvrir un compte bancaire

Au premier rang des nouveaux usages commerciaux de la biométrie, se trouvent les services proposés par le secteur bancaire, particulièrement sensibles au phénomène d'usurpation d'identité. Depuis février 2018, la banque Société Générale permet l'ouverture d'un compte à distance, une première en France, en utilisant la technologie de la reconnaissance faciale, après avoir reçu l'autorisation de la Cnil (Commission nationale de l'informatique et des libertés) pour déployer cette technologie « disruptive » dans le domaine commercial. Le recours à la reconnaissance biométrique faciale s'adresse particulièrement aux personnes n'ayant pas de compte bancaire : cette procédure se substitue à l'une des mesures de vigilance définies par le code monétaire et financier pour ouvrir un compte à distance, à savoir effectuer un premier versement depuis un compte ouvert à son nom dans une autre banque. À partir de l'application Société Générale, le futur client transmet à l'agence bancaire deux pièces d'identité numérisées et réalise un *selfie* dynamique : portrait filmé de face et des deux profils. La démarche s'achève par un entretien vidéo avec un conseiller. Après une signature électronique, le client recevra, dans les vingt-quatre heures, un relevé d'identité bancaire et une carte de paiement, sans avoir à se déplacer.

L'authentification d'une personne par l'application Société Générale repose sur un algorithme capable de comparer, en temps réel, la photo de la pièce d'identité aux diverses photos : profil, face, yeux ouverts ou fermés prises lors du selfie dynamique. Cette technique offre une fiabilité dix fois supérieure aux capacités de reconnaissance humaine. De la même façon, une seconde authentification est réalisée durant l'appel vidéo passé avec le conseiller. La banque précise que sont archivés les résultats des contrôles effectués à chaque reconnaissance biométrique, mais pas les données biométriques. Selon ses prévisions, près d'un tiers des ouvertures de comptes de la Société Générale devrait être effectuée de cette façon ici

En 2020, l'application Soci@t@ G@n@rale a @t@ d@velopp@e par le groupe fran@ais Idemia, autre leader mondial de ce qu'il nomme @ « l'identit@ augment@e », @ n@ du rachat en mai 2017 par Oberthur Technologies (fonds Advent) de Morpho (groupe Safran). @ l'automne 2017, Idemia a pr@sent@ une premi@re carte de paiement biom@trique, appel@e F.CODE Comfort, int@grant un lecteur d'empreinte digitale qui permet d'authentifier son porteur. En mars 2018, c'est au tour de la banque en ligne Boursorama, filiale de la Soci@t@ G@n@rale, de lancer une application permettant l'ouverture d'un compte, s@curis@e par un proc@d@ d'identification par reconnaissance faciale, d@velopp@ par l'entreprise isra@lienne Scanovate. @ la diff@rence de l'application choisie par sa maison m@re, Boursorama propose un proc@d@, appel@ @ « parcours flash », enti@rement automatis@.

S@curit@ civile

Dans la plupart des pays europ@ens, l'usage le plus r@pandu jusqu'alors concernait le passeport et la carte nationale d'identit@, portant les empreintes digitales du titulaire en plus de sa photo d'identit@. Bient@t, les sas automatiques de contr@le d'identit@ dans les a@roports parisiens seront @quip@s d'une nouvelle fonction de reconnaissance faciale, l'objectif @tant de r@duire les d@lais d'attente. Jusqu'ici, les sas Parafe (Passage automatis@ rapide des fronti@res ext@rieures) ne savaient reconna@tre que les empreintes digitales et @taient r@serv@s aux voyageurs fran@ais munis d'un passeport biom@trique. @ l'@t@ 2018, 80 sas Parafe fournis par l'entreprise Gemalto seront activ@s pour la reconnaissance digitale et faciale, @ leur nombre total sera port@ @ 95 @ l'automne. Une phase de tests pour la reconnaissance faciale a d@but@, en avril 2018, @ Roissy-Charles-de-Gaulle, et devrait d@boucher sur l'activation de cette fonction pour l'ensemble des sas, apr@s autorisation du minist@re de l'int@rieur. La majorit@ des passagers europ@ens sont concern@s par cette pratique qui reste, en France, circonscrite aux a@roports et @ certaines gares, @ conform@ment @ un avis de la Cnil qui s'oppose @ l'utilisation omnipr@sente d'un profilage en temps r@el ; @ autant plus que la technique de reconnaissance faciale automatique manque encore nettement de pr@cision. Selon le *Guardian*, le taux de @ « faux positifs » @ atteint 92 % @ sur les 2 470 @ personnes identifi@s par les cam@ras lors de la finale de la Ligue des champions de football @ Cardiff en 2017, quand la police invoque, de son c@t@, la pi@tre qualit@ des images stock@s dans sa base de donn@s de r@f@rence.

1.

CNIL : LES RÈGLES À RESPECTER EN MATIÈRE DE BIOMETRIE GRAND PUBLIC

2.

Justifier d'un besoin spécifique, comme l'accès à un lieu, une application ou un service, par la réalisation au préalable d'une étude d'impact sur la vie privée.

Laisser le libre choix à l'utilisateur, notamment d'opter pour un autre mode d'authentification classique comme un mot de passe.

Laisser à l'utilisateur le contrôle exclusif de ses données biométriques :

- soit parce qu'elles sont stockées uniquement sur un support autonome (passeport, téléphone portable) en sa possession,
- soit, si elles sont stockées dans une base de données, parce qu'elles peuvent être déchiffrées uniquement avec un code qu'il est seul à connaître.

Entrée en vigueur le 25 mai 2018, le RGPD ([voir La rem n°42-43, p.21](#)) consacre le caractère sensible des données liées au physique, à la biologie et aux comportements des personnes, au même titre que leurs données de santé ou celles relatives à l'orientation sexuelle.

Source :

– « Biométrie à disposition de particuliers : quels sont les principes à respecter ? », Cnil.fr, 10 avril 2018.

Au service des Gafa

En matière de reconnaissance faciale, les géants du Net, qui disposent déjà de considérables banques d'images, proposent évidemment chacun leur savoir-faire. À l'occasion du mariage

princier, qui s'est déroulé au Royaume-Uni en mai 2018, le service Rekognition d'Amazon appuyant sur sa filiale de *cloud computing* AWS (Amazon Web Service) a été utilisé par la chaîne de télévision Sky News pour lancer sur son site web et ses applications une fonction baptisée Who's Who, qui permettait aux internautes d'identifier en temps réel les 600 personnes invitées à la cérémonie. Amazon a déjà fait savoir qu'il disposait d'une importante banque d'images. Dans le même temps, aux États-Unis, une trentaine d'associations de défense des libertés civiles, dont Electronic Frontier Foundation et Human Rights Watch, ont adressé une lettre au patron d'Amazon, après que l'American Civil Liberties Union (ACLU) a révélé l'utilisation par la police de plusieurs États (notamment l'Oregon et la ville d'Orlando, ainsi que des négociations en cours avec la Floride et l'Arizona) de l'outil Rekognition, sans en avoir averti les citoyens, réclamant l'arrêt de cette surveillance qui emploie la technologie d'Amazon pour traiter des fichiers de la police. Pour les défenseurs des libertés civiles, cette pratique jugée abusive comporte notamment de nombreux biais et engendre des « faux positifs ».

Google, quant à lui, propose FaceNet, un algorithme sachant nommer et localiser n'importe quelle personne piochée dans les albums des internautes stockés dans Google Photos, fonction inactive en Europe. En avril 2018, Sundar Pichai, PDG de la maison mère Alphabet, a reçu lui aussi un courrier signé par plus de 3 100 employés, s'opposant à l'utilisation des technologies du groupe à des fins militaires, comme son outil TensorFlow loué au Pentagone dans le cadre du projet Maven, qui a recours à l'intelligence artificielle pour analyser les vidéos filmées par les drones militaires. Le 1^{er} juin 2018, Alphabet a finalement annoncé qu'il ne renouvellera pas ce contrat d'un montant s'élevant à quelque 15 millions de dollars qui court jusqu'en mars 2019.

Quant à Facebook, qui doit faire face à une class action lancée en avril 2018 dans l'Illinois pour collecte et conservation illégales des données personnelles à partir de son système de reconnaissance faciale, il ambitionne de lancer cette technologie en Europe. L'outil permettra de lutter contre l'usurpation d'identité, indique Facebook, en informant ses membres de la publication de photos sans leur consentement. La fonction de reconnaissance faciale est testée depuis mars 2018 auprès d'un petit nombre d'utilisateurs, y compris en France. Ces derniers garderont le choix de l'activer ou non, selon Facebook, et les données biométriques recueillies n'alimenteront pas leur profil publicitaire.

« Au minimum, les gens devraient pouvoir marcher dans la rue sans craindre que des entreprises dont ils n'ont jamais entendu parler enregistrent chacun de leurs mouvements et les identifient par leur nom ».

À s'insurgeaient déjà en 2015 des associations de défense des libertés civiles, ainsi que des associations de défense des consommateurs aux États-Unis contre le déploiement d'outils de détection dans la vie quotidienne, notamment le système FaceFirst, qu'une entreprise californienne propose aux supermarchés, pour suivre « y compris sur le trottoir » les bons clients comme les voleurs.

Ailleurs

C'est en Chine que le système de surveillance en direct est le plus abouti. Le pays comptera plus de 400 millions de caméras de surveillance en 2020. La technologie de reconnaissance faciale, reliée aux serveurs des services de l'État, équipe le réseau vidéo installé dans les grandes villes. Ce réseau permet, entre autres, d'afficher sur un écran géant l'identité et le visage d'un piéton contrevenant aux règles de la circulation.

Et, c'est en Inde qu'a été créée, en 2010, la plus grande base de données biométriques au monde, appelée Aadhaar. Concernant plus d'un milliard d'individus, soit près de 99 % de la population adulte, ce système biométrique enregistre de graves dysfonctionnements (voir *infra*). À New Delhi cependant, grâce à un logiciel de reconnaissance faciale fourni gracieusement dans un but humanitaire par une entreprise portugaise, la police est parvenue à retrouver, en 2018, en quatre jours seulement, l'identité de 3 000 enfants perdus, à partir d'un fichier de 45 000 mineurs.

Et demain ?

Grâce au progrès du phénotypage génétique, il sera possible de reconstituer un visage à partir de l'ADN. En Europe, huit pays, sous l'égide d'instituts universitaires, judiciaires et policiers – l'Institut national de police scientifique en France – ont lancé, en 2017, le projet Visage (Visible Attributes through Genomics), ayant pour objet de recherche l'aboutissement d'un portrait-robot génétique.

Sources :

- « Biométrie : authentification et identification (2018) », Gemalto.com, 5 février 2018.
- « Sociétale Générale révolutionne l'ouverture de compte à distance », communiqué de presse, Societegenerale.com, 15 février 2018.
- « Sociétale Générale va ouvrir des comptes grâce à la biométrie faciale », Sharon Wajsbrot, *Les Echos*, 16-17 février 2018.
- « Facebook va tester la reconnaissance faciale en Europe », Elisa Braun, *LeFigaro.fr*, 1^{er} mars 2018.
- « Aprés la Sociétale Générale, Boursorama se lance dans la reconnaissance faciale », Marc Rees, *Nextinact.com*, 5 mars 2018.
- « Sous l'égide de la biométrie », Sophy Caulier, *Le Monde*, 13 mars 2018.
- « Big data t face », Frédéric Joignot, *Le Monde*, 24 mars 2018.
- « Vers une class action » contre Facebook dans l'Illinois », Claude Fouquet, *Les Echos*, 18 avril 2018.
- « Les aéroports parisiens misent sur la reconnaissance faciale », Bruno Travidic, *Les Echos*, 24 avril 2018.

- « Inde : une application de reconnaissance faciale pour les enfants disparus », Sbastien Farcis, RFI.fr, 3 mai 2018.
- « La reconnaissance faciale testée par la police britannique fait des tas d’erreurs », Gabriel Hassan, Courrierinternational.com, 5 mai 2018.
- « Au mariage du Prince Harry et de Meghan Markle, une intelligence artificielle identifiera les invités », Marius François, LeFigaro.fr, 15 mai 2018.
- « Amazon exhorte ne plus fournir son outil de reconnaissance faciale à la police », AFP, tv5monde.com, 22 mai 2018.
- « La technologie de reconnaissance faciale d’Amazon utilisée par la police américaine », Elisa Braun, LeFigaro.fr, 23 mai 2018.
- « Sous la pression de ses employés, Google renonce à son projet controversé avec le Pentagone », Jérôme Marin, Silicon 2.0, blog.lemonde.fr., 2 juin 2018.

Categorie

1. Techniques

date créée

16 juillet 2018

Auteur

francoise