

Comment l'ouverture du rail à la concurrence s'est faite en Europe

► Engagée en 1991, la libéralisation du rail dans l'UE a signifié quasiment partout la fin de l'emploi à vie des cheminots

C'était le 27 octobre 1992, vingt-six syndicats des douze pays de la Communauté économique européenne, plus l'Autriche et la Suisse, lançaient un mouvement de grève. En ligne de mire, la libéralisation de l'accès aux réseaux publics de chemin de fer promise par Bruxelles en 1991. Vingt-cinq ans plus tard, l'Union européenne a adopté

le quatrième «paquet ferroviaire» qui parachève la libéralisation du rail. Après l'ouverture à la concurrence du fret international en 2003, du fret national en 2007, du transport international de voyageurs en 2010, les Vingt-Huit se sont mis d'accord pour ouvrir le marché des transports passagers nationaux et régionaux.

En réorganisant en 2014 son système ferroviaire, la France a connu d'importantes grèves... Mais elle respecte plutôt le calendrier de réformes, que d'autres Etats membres ont même devancé, comme le Royaume-Uni, l'Allemagne, la Suède, la République tchèque ou l'Italie. La libéralisation a rimé quasiment partout avec la disparition d'un statut assu-

rant un emploi à vie. Dans ces pays, qui investissent toujours massivement dans le ferroviaire, le coût de production du train a baissé, et les passagers prennent à leur charge une plus grande part du prix de leur billet que les usagers français.

PHILIPPE JACQUÉ
AVEC NOS CORRESPONDANTS
LIRE LA SUITE PAGE 3

Nouvelle donne sur le marché allemand de l'énergie

Le secteur de l'énergie outre-Rhin est le théâtre d'un nouveau mouvement d'ampleur. Dans la nuit de samedi 10 à dimanche 11 mars, les deux groupes E.ON et RWE ont annoncé leur intention d'opérer un gigantesque échange d'activités pour un montant de 20 milliards d'euros.

E.ON devrait prendre le contrôle de l'une des filiales de son concurrent RWE, Innogy, valorisée 19 milliards d'euros en Bourse, avant de la démanteler. RWE, à la faveur de ce démantèlement, récupérera de nouvelles activités, notamment dans les énergies renouvelables, pour former l'un des plus gros énergéticiens d'Europe.

E.ON se concentrera essentiellement sur deux métiers : la commercialisation de l'énergie et la gestion des réseaux. RWE, de son côté, se focalisera sur la production d'électricité, en se renforçant dans les énergies vertes, avec, notamment, les actifs d'E.ON dans les centrales hydrauliques et les parcs éoliens.

RWE exploitera encore ses centrales conventionnelles, jugées nécessaires à long terme pour compenser le caractère intermittent des énergies renouvelables. Au terme de l'opération - qui doit être approuvée par les autorités de la concurrence -, RWE deviendra le premier actionnaire d'E.ON. ■

PAGE 4

La biométrie gagne le grand public

► Née des besoins de la sécurité publique et de la défense, la biométrie, qui permet d'identifier quelqu'un par ses caractéristiques physiques, se répand

► Fin janvier, Facebook a acheté Confirm, une application de vérification des pièces d'identité fondée sur cette technologie

► Le stockage et l'utilisation des informations par les géants du Net inquiètent l'Europe, où un règlement général sur la protection des données entrera en vigueur le 25 mai



Démonstration d'un logiciel de reconnaissance faciale par la compagnie chinoise LLVision, à Pékin, le 28 février.
THOMAS PETER/REUTERS

PAGES 6-7

19

MILLIARDS D'EUROS

C'EST LA VALORISATION BOURSIÈRE D'INNOCY, PRINCIPAL ACTIF ÉCHANGÉ ENTRE LES ALLEMANDS E.ON ET RWE

PERTES & PROFITS | E.ON-RWE

Après le tremblement de terre

Dans *Après le tremblement de terre* (2000), le romancier japonais Haruki Murakami raconte comment le séisme qui a détruit la ville de Kobe en 1995 a affecté le cœur et la destinée des survivants, révélant des failles intimes tout aussi ravageuses que celles du sous-sol de l'Archipel. Le séisme du 7 décembre 2011 qui a frappé le nord du Japon, provoquant un tsunami meurtrier et détruisant la centrale nucléaire de Fukushima, a eu le même effet. Rarement un accident industriel, dont on peine encore à établir le véritable bilan humain (aucun mort direct mais des milliers de déplacés et d'irradiés), n'a autant transformé une filière économique aussi stratégique, laissant remonter à la surface des mouvements tectoniques à l'œuvre depuis longtemps : méfiance envers le nucléaire, essor des énergies renouvelables, modification des équilibres économiques.

C'est à cette aune qu'il faut mesurer la spectaculaire opération capitaliste annoncée ce week-end en Allemagne. Un échange d'actifs entre les deux principaux électriciens du pays, E.ON et RWE, qui aboutit à spécialiser le premier dans les services et les réseaux et le second dans la pure production d'électricité, qu'elle soit à base de charbon, de gaz ou de renouvelable. Un peu comme si, en France, EDF se contentait de fabriquer de l'électricité pour le vendre à Engie, et d'autres se chargeraient de la commercialisation auprès des consommateurs.

C'est en effet l'accident de Fukushima qui a conduit le gouvernement allemand à décréter dès 2011 la sortie totale en dix ans du nucléaire,

qui représentait plus de 20 % de la production d'électricité. Une décision majeure qui, en doublant quasiment la part de l'électricité renouvelable, a détruit le modèle économique des producteurs. D'autant que le phénomène s'est répandu en Europe, après les décisions italienne, suisse, belge, autrichienne dans cette voie de sortie du nucléaire. L'apparition de ces nouvelles sources d'énergie, subventionnées, ainsi que le recours accru au charbon, au coût très faible, ont écrasé les prix et la rentabilité de tous les acteurs européens qui s'échangent de l'électricité en permanence.

Victime collatérale

Conséquence de ces bouleversements, tout investissement capitaliste devient hasardeux. Celui dans le nucléaire, plus encore. Les déboires d'Areva en Finlande et la facture de l'investissement d'EDF en Grande-Bretagne en attestent. De plus, le modèle de la vente à la quantité consommée est de moins en moins compatible avec la commercialisation de services de gestion et d'économie d'énergie. La solution allemande de séparer les métiers, avec d'un côté un producteur d'électricité dominant sur son marché et d'un autre des sociétés de services et de réseaux qui commercialisent, pourrait donner des idées à d'autres. Et notamment alimenter les réflexions en France sur une séparation des activités de production nucléaire d'EDF, lui aussi victime collatérale du séisme japonais du 11 mars 2011. ■

PHILIPPE ESCANDE

PORTRAIT L'AMÉRICAIN QUI LUTTE CONTRE LES PETITS BOULOTS AU ROYAUME-UNI

PAGE 2

MÉDIAS LE GROUPE LES ÉCHOS-LE PARISIEN CHANGE DE PATRON

PAGE 8

📊 CAC 40	5 295,64 PTS + 0,40 %
📊 DOW JONES	25 335,74 PTS + 1,77 %
📊 EURO-DOLLAR	1,2328
📊 PÉTROLE	65,24\$ LE BARIL
📊 TAUX FRANÇAIS À 10 ANS	0,894 %

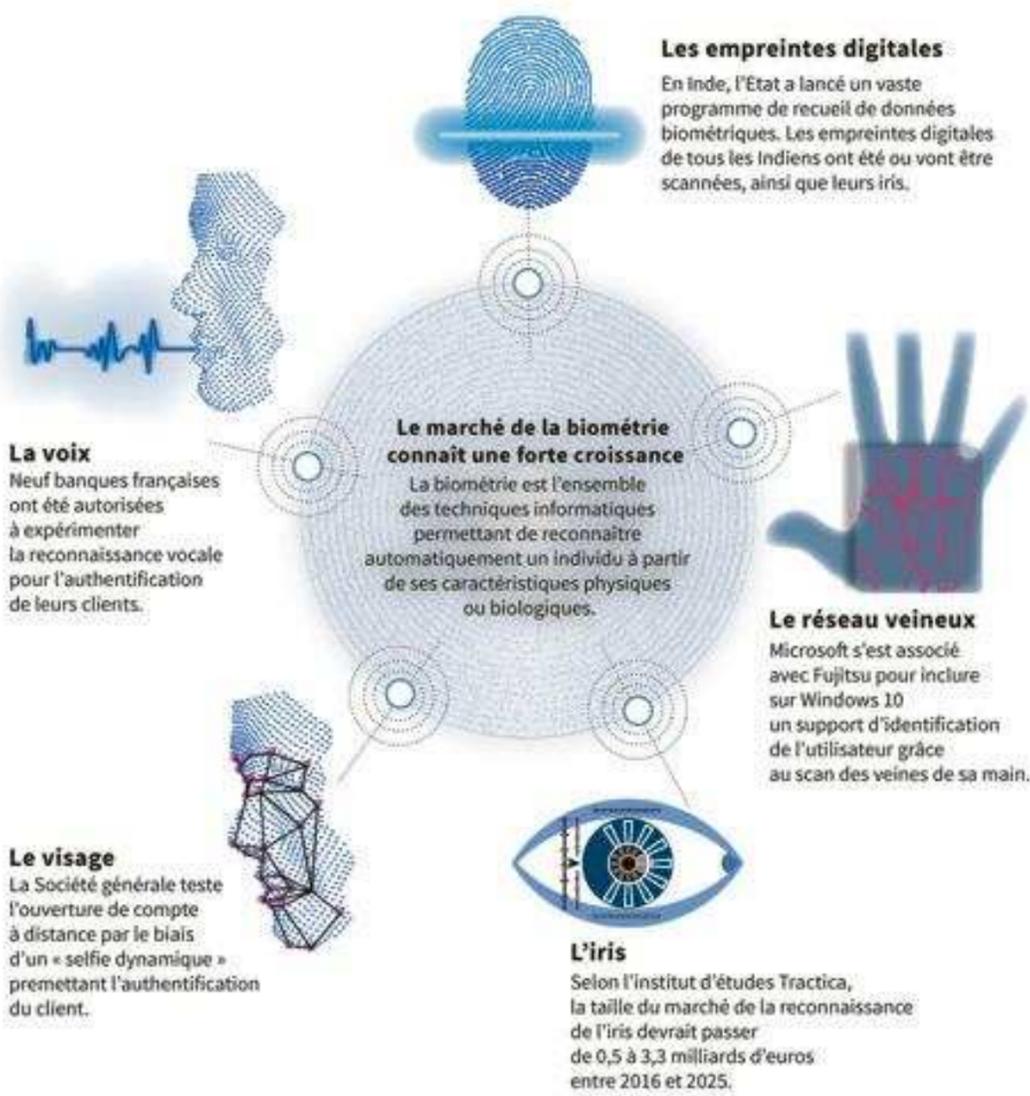
VALEURS AU 12 MARS À 9 H 30

Construire selon vos exigences environnementales, pour nous c'est (éco)logique

COUGNAUD
POUR LA VIE EN MOUVEMENT

À découvrir sur cognaud.com

Une technologie désormais omniprésente



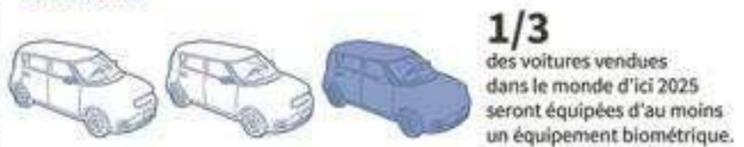
Trois secteurs particulièrement concernés

La téléphonie

PART DES SMARTPHONES VENDUS DANS LE MONDE DOTÉS D'ÉQUIPEMENTS BIOMÉTRIQUES, EN %



L'automobile



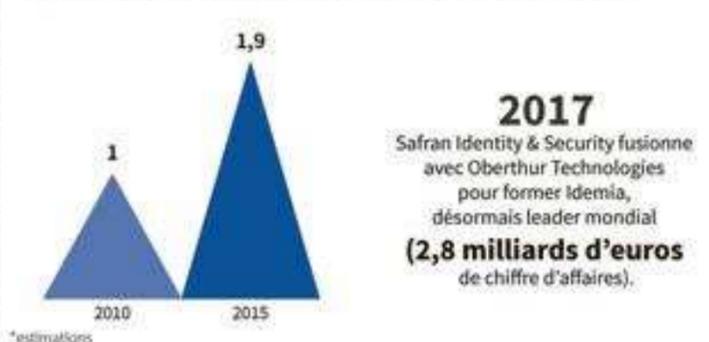
Le monde financier et bancaire

LIVRAISONS D'ÉQUIPEMENTS BIOMÉTRIQUES DANS LE MONDE, EN MILLIONS D'UNITÉS



Les entreprises françaises bien positionnées

CHIFFRE D'AFFAIRES DE SAFRAN IDENTITY & SECURITY, EN MILLIARDS D'EUROS



SOURCES : CMIL, TRACTICA, IDC, EMARKETER, FROST & SULLIVAN, TRANSPARENCYMARKETRESEARCH, ACUTY MARKET INTELLIGENCE, SAFRAN INFOGRAPHIE : PHILIPPE DA SILVA, MAXIME MAINGUET

Sous l'œil de la biométrie

Ce jeune homme debout, les mains dans les poches, qui sourit à un écran dans l'entrée d'un fast-food, ne patiente pas devant un vidéo en attendant ses morceaux de poulet grillé. Il est en train de payer d'un sourire le repas qu'il vient de commander. Les restaurants KFC de Hangzhou, dans la région de Shanghai, testent l'application Smile to Pay, du groupe chinois Alibaba, qui permet aux clients de payer leur achat par reconnaissance faciale.

Cette jeune femme, qui montre rapidement son smartphone à la borne d'entrée d'une supérette, remplit son cabas et sort sans payer, n'est ni distraite ni voleuse. Elle fait ses courses dans le magasin sans caisse Amazon Go de Seattle, sur la Côte ouest des États-Unis. Elle a été identifiée à l'entrée par le code-barres de son smartphone et dans tout le magasin par les caméras qui l'ont reconnue et suivie. Des capteurs ont enregistré ses achats, dont le montant est immédiatement prélevé sur son compte Amazon.

Née des besoins de la sécurité publique et de la défense, cette technique se répand dans tous les domaines. Le stockage et l'utilisation de ces informations par les géants de l'Internet inquiètent. En Europe, un règlement général sur la **protection des données** entrera en vigueur le 25 mai

Les technologies biométriques mises en œuvre dans ces applications sont à peu de chose près les mêmes que celles utilisées pour délivrer les documents d'identité électroniques (passport, carte d'identité...), pour lutter contre le crime et le terrorisme, ou pour la vidéosurveillance dans les lieux publics. La seule différence est que, dans les deux exemples cités, ce ne sont plus des États ni des gouvernements qui enregistrent les visages ou les empreintes digitales, mais de grandes entreprises privées, les Gafam

(Google, Apple, Facebook, Amazon, Microsoft) et les BATX (Baidu, Alibaba, Tencent, Xiaomi) en tête. Elles exploitent ces données pour identifier leurs clients dans leurs moindres activités, mieux les connaître pour leur vendre toujours plus en échange d'une « expérience utilisateur fluide et simple »!

UNE TECHNOLOGIE FAILLIBLE

La biométrie consiste à identifier une personne à travers ses caractéristiques physiques : empreintes digitales, visage, iris, ré-

seau veineux, ADN... qui sont propres à chaque individu. La biométrie a longtemps été cantonnée au domaine de la sécurité civile et de l'accès à des sites critiques. La France se targue de compter deux des premiers acteurs mondiaux du domaine : Gemalto, racheté par Thales en décembre 2017, et Idemia, né de la fusion d'Oberthur Technologies et de Morpho, filiale de Safran Identity & Security.

L'utilisation de la biométrie gagne à présent le grand public. Le virage a eu lieu fin 2013 lorsque Apple a lancé l'iPhone 5, doté de la fonction de reconnaissance d'empreinte digitale Touch ID, permettant de déverrouiller l'appareil. Samsung a suivi. Apple a franchi une nouvelle étape fin 2017 en lançant Face ID, la reconnaissance faciale par caméra 3D, sur le modèle iPhone X. « Les composants électroniques nécessaires à la biométrie étaient quasiment réservés au domaine militaire du fait de leur coût et de leur complexité. La technologie est devenue plus abordable. Et l'innovation a suscité un nouvel usage rapidement adopté », explique Eric Boulay, directeur exécutif d'Accenture Security.

En matière d'identification et d'authentification, « il y a soit ce que l'on possède, un passeport, un badge ; soit ce que l'on sait, un mot de passe, un code PIN ; soit ce que l'on est, une empreinte, un iris... », poursuit M. Boulay. Un des principaux avantages de la biométrie est qu'elle dispense les usagers de mémoriser de nombreux mots de passe et de transporter plusieurs badges ou clés d'accès.

En simplifiant l'utilisation de services, la biométrie a su se faire mieux accepter par le grand public. Les citoyens n'hésitent pas à enregistrer leurs empreintes et leur photo pour passer plus facilement les frontières. Les consommateurs utilisent leur voix, leur visage ou leurs empreintes pour s'identifier et payer leurs achats en ligne ou consulter leur compte bancaire. La biométrie sécurise l'accès à des locaux, à des ordinateurs, à des documents confidentiels ou à des moyens de paiement. Elle enregistre le vote des électeurs. Elle contribue à la sécurité routière puisque de nombreux capteurs biométriques vont équiper de plus en plus les véhicules, qui mesurent le niveau de stress ou de fatigue du conducteur, après avoir vérifié son identité et reconnu son iris ou sa voix.

En Chine, les start-up surfent sur les besoins de l'Etat policier

LA PHOTO A FAIT LE TOUR des réseaux sociaux : une jeune policière en uniforme porte des lunettes noires, équipées d'une petite caméra. Au milieu de la gare de Zhengzhou, dans le Henan, une des provinces les plus peuplées de Chine, la jeune femme scanne la foule, grâce à un système de reconnaissance faciale. L'outil est connecté à la fois à un smartphone, dans les mains de l'agent de police, et à un écran dans le commissariat de la gare.

La scène futuriste aurait de quoi inquiéter des usagers français, mais en Chine, c'est la police locale elle-même qui a publié fièrement ces images juste avant le Nouvel An chinois. Grâce à cette technologie, elle aurait arrêté sept suspects recherchés et 26 personnes voyageant sous une fausse identité. Les lunettes ont été mises au point par LIVision, une entreprise ba-

sée à Pékin qui vend ces lunettes au grand public et a développé cette version équipée de la reconnaissance faciale en collaboration avec la police.

Contrôler les populations

En Chine, les start-up de la biométrie se développent main dans la main avec l'État policier. D'un côté, les autorités accueillent avec bienveillance, ou soutiennent, des technologies qui leur permettent de mieux contrôler les populations. De l'autre, des jeunes pousses peuvent se hisser à la pointe dans leur domaine grâce à des ressources en intelligence artificielle et un accès facile aux informations de près de 1,4 milliard d'habitants, profitant de la faible protection des données personnelles. Le résultat, ce sont des champions de la reconnaissance faciale, vocale, de la démarche, de la

lecture des veines de la main, etc., qui collaborent à la fois avec le privé et avec la sécurité publique.

Si la reconnaissance faciale est plus impressionnante quand elle est installée sur des lunettes, elle équipe déjà largement les 176 millions de caméras de surveillance installées en Chine. Les entreprises SenseTime (Hongkong) et Megvii (Pékin) sont devenues des « licornes » en 2017, dépassant le milliard de dollars de valorisation. Ces spécialistes de la reconnaissance faciale collaborent à la fois avec des fabricants de smartphones comme Huawei, Oppo ou Xiaomi, avec Alibaba, le géant du commerce en ligne, et avec les départements de la sécurité publique des provinces chinoises.

Autre champion, iFlytek est spécialisée dans la reconnaissance vocale. Sa technologie permet de reconnaître et

de différencier des conversations dans un lieu public ou d'identifier des voix dans une conversation téléphonique.

L'entreprise, valorisée à 13 milliards de dollars (10,5 milliards d'euros), a séduit une kyrielle d'entreprises – dans l'automobile (Volkswagen), la banque, Internet (Tencent et Alibaba), les smartphones –, mais aussi les autorités du Xinjiang. Cette région autonome de l'Ouest chinois est devenue une prison à ciel ouvert après une série d'émeutes et d'attentats. Les habitants, surtout les Ouïgours, membres de la minorité musulmane locale, sont contrôlés en permanence, pour entrer dans un bus, ou dans les centres commerciaux, dans les hôtels... Et ils doivent se soumettre à des tests ADN pour obtenir un passeport. ■

SIMON LEPLÂTRE
(SHANGHAÏ, CORRESPONDANCE)



Une enseignante utilise la reconnaissance faciale pour identifier une élève avant le passage d'un examen, à Handan, en Chine, en juin 2017. AFP

En Inde, elle protège les enfants en enregistrant les vaccins qu'ils ont reçus dans une puce qui identifie par la biométrie la mère et l'enfant. Et depuis février, la reconnaissance faciale permet d'ouvrir un compte bancaire en ligne à la Société générale par simple « selfie dynamique », sans oublier l'envoi numérique des documents d'identité bien entendu !

La biométrie n'est pas infaillible pour autant. Les films d'espionnage regorgent de méchants qui se font passer pour des gentils à l'aide d'une lentille de contact ou de faux doigts. Chaque annonce de nouvelle technologie provoque des démonstrations de son détournement possible: un film collé sur le bout du doigt reproduisant l'empreinte digitale ou une photo appliquée sur un visage déverrouillent un smartphone ou donnent accès à un site protégé. « Il reste beaucoup de cas à étudier et à régler, comme le vieillissement d'un visage et la différence entre les jumeaux ou les membres d'une même famille, mais les technologies sont de plus en plus précises, explique Antitza Dantcheva, chercheuse à l'Institut national de recherche en informatique et en automatique-Sophia Antipolis. Les travaux de recherche portent, par exemple pour la reconnaissance d'empreinte, sur la prise en compte de la pression, de la température ou de l'humidité. Pour la reconnaissance faciale, on analyse les mouvements des paupières ou on fait une image 3D. Ce qui ne peut pas être fait avec une simple photo. »

DES RECHERCHES PORTENT SUR L'ODEUR

L'iris est la caractéristique la plus fiable. C'est cette membrane qui a permis d'identifier Sharbat Gula, dix-huit ans après que sa photo en couverture du *National Geographic* lui eut valu le surnom « d'Afghane aux yeux verts ». Mais pour plus de fiabilité, la tendance actuelle est au multimodal, c'est-à-dire à la combinaison de plusieurs facteurs biométriques, voire des paramètres qui peuvent y être associés. « On peut tricher sur une caractéristique, mais pas sur plusieurs ! », poursuit M^{me} Dantcheva. Le multimodal permet de créer une identité plus « sûre » en combinant des données biométriques entre elles et avec des données comportementales comme la voix ou la frappe sur un clavier.

D'autres travaux de recherche portent sur l'odeur, elle aussi propre à chaque individu. La start-up Caractère travaille avec l'université du Havre pour « capturer le portrait olfactif » d'un individu. Cela pourrait être fait sur le lieu d'un crime, lorsque l'on relève tous les indices. Problème, « l'identification d'une empreinte digitale peut être faite par un ordinateur, celle d'une odeur est faite par

un chien, et cela n'a pas encore de valeur auprès des tribunaux », regrette Florian Rabeau, le fondateur de Caractère.

La première vocation de la biométrie est de certifier l'identité des individus et de les protéger de l'usurpation de leur identité physique et numérique. Mais l'utilisation qui pourrait être faite de ces données inquiète. La réglementation sur le stockage et l'utilisation des informations biométriques diffère d'un pays à l'autre. En Europe, elle va devenir plus homogène avec le règlement général sur la protection des données (RGPD), qui entrera en vigueur le 25 mai. Ce texte impose aux entreprises de déclarer quelles données elles collectent auprès de leurs utilisateurs et quels usages elles en font. Toutes les sociétés actives en Europe y sont soumises. « Elles ne peuvent traiter les données biométriques que dans deux cas: soit elles obtiennent le consentement explicite de la personne pour une finalité spécifique, soit le traitement est nécessaire pour exercer une activité comme, par exemple, accéder à un lieu de travail », précise Jérémie Courtois, avocat au cabinet Cornet Vincent Segurel. Pour lui, « le vrai risque est le vol de données ». « Les conséquences sont déjà graves quand il s'agit de numéros de compte bancaire ou de carte de crédit, ce sera bien pire pour des données biométriques ! » D'autant que les caractéristiques biométriques sont irrévocables, c'est-à-dire que la personne ne peut pas changer d'empreintes digitales ou d'iris si ces données ont été volées ou compromises...

« FACEBOOK EST DEVENU LE GREFFIER DE PLUS DE 2 MILLIARDS D'INDIVIDUS, C'EST LUI QUI PEUT ATTESTER DE L'IDENTITÉ DE CES PERSONNES »

FRANCK GUIGAN
président de PopimsCode

Le sujet critique est celui du stockage, de la sécurisation et, surtout, de l'utilisation des données. « Le monde se divise en deux types d'acteurs: ceux qui protègent les données et la vie privée, quitte à faire payer leurs services, et ceux qui offrent des services gratuits et qui se rémunèrent en monétisant les informations de leurs clients », affirme Christophe Remillet, fondateur et PDG de la start-up One Visage, qui a développé une technologie de reconnaissance faciale 3D pour les appareils mobiles. « Nous sommes l'anti-Facebook, notre technologie permet aux utilisateurs de services numériques de protéger leur identité. »

CIBLER PLUS PRÉCISÉMENT LES CLIENTS

La technologie de One Visage fonctionne sur tous les modèles de téléphones munis d'une caméra et commercialisés depuis 2015. Le visage de l'utilisateur est modélisé en 3D et stocké dans le portable. Selon l'application, il peut aussi l'être sous forme de modèle de référence (pattern) dans un serveur. L'intérêt de la solution est qu'elle est ouverte à tous, peu onéreuse et aisée à déployer.

« Ce qui fait peur, c'est la méga base de données qui contrôlerait tout », remarque Eric Boulay, d'Accenture. Et cette peur est fondée ! Les multinationales associent les informations qu'elles recueillent, biométriques ou non, elles les croisent avec des données telles que le numéro de téléphone, de Sécurité sociale ou de carte de crédit, l'adresse, l'âge, la consommation, les pratiques sportives ou

religieuses, les lieux fréquentés, etc. Et elles analysent ces données, les revendent et les échangent contre des données détenues par d'autres entreprises pour mieux connaître leurs clients et les cibler plus précisément.

Le géant chinois de l'Internet Alibaba compte quelque 450 millions d'utilisateurs de ses services. Combien d'entre eux lui ont-ils confié leurs données biométriques pour « payer en souriant » ? Et à quelles utilisations ces données pourraient-elles servir un jour ? Fin janvier, Facebook a racheté la start-up américaine Confirm. Celle-ci a développé une application de vérification des pièces d'identité en les comparant à des données biométriques, notamment la reconnaissance faciale... Le réseau social compte se servir de cette application – qui n'est plus disponible à l'achat – pour s'assurer de l'identité de ses utilisateurs mais aussi de ses annonceurs. Et éviter les faux comptes et les « fake news » ?

Et demain, qu'en fera-t-il ? « Avec ce rachat, Facebook est devenu le « registrar » [greffier] de plus de 2 milliards d'individus, c'est lui qui peut maintenant attester de l'identité de ces personnes ! », s'indigne Franck Guigan, président fondateur de PopimsCode, une solution d'identité numérique gérée par l'utilisateur à l'aide d'une clé optique. Personne ne sait si Mark Zuckerberg sera candidat à la présidentielle américaine en 2020, mais une chose est sûre, Facebook en sait plus sur ses utilisateurs que n'importe quel gouvernement. ■

SOPHY CAULIER

« L'identification des personnes pose des questions éthiques profondes »

PROFESSEUR EN SCIENCES DE L'INFORMATION et de la communication à Télécom ParisTech, Pierre Musso souligne l'ambivalence entre le désir des internautes d'exposer leur vie privée et leur souci de préserver leur liberté.

Que change le mariage de la biométrie et du numérique ?

Le développement de ces technologies nous place au cœur de l'ambivalence entre notre besoin de liberté et une demande de protection de plus en plus forte. Pour accéder à des services, nous acceptons de confier nos données les plus intimes. Parfois nous les mettons en scène sur les réseaux sociaux comme Facebook, pour gagner en réputation. C'est ce que le sociologue Serge Tisseron appelle « l'extimité ». Après cinquante ans d'un ré-

gime où la production est pilotée par le consommateur, à l'image de Zara qui reconfigure en permanence son offre textile en fonction des ventes, nous passons dans une économie de la contribution où l'utilisateur est actif et individualisé. Dans cet univers, la biométrie apporte la promesse d'une identification plus grande.

Au détriment de notre liberté ?

Cela touche en effet à cette liberté essentielle qu'est le respect de la vie privée. Il faut distinguer l'authentification, nécessaire pour valider une procédure, et l'identification des personnes qui pose des questions éthiques bien plus profondes. D'abord celle du consentement, mais aussi celle de la finalité de l'utilisation des données et enfin celle de la proportionnalité

entre l'étendue de la collecte et son usage. C'est si délicat que certains demandent l'interdiction de la pratique.

La porte ouverte à toutes les dictatures ?

Il serait tentant de penser que cette manipulation des données, poussée à l'extrême avec la biométrie, mène inévitablement vers la société de surveillance généralisée, dépassant celle décrite par Foucault avec l'image du panoptique qui permet à un seul individu de surveiller tous les autres. C'est une voie possible, mais ce n'est pas la seule. Car avec l'Internet, le sujet observé, l'internaute, peut aussi être celui qui observe. Une sorte de panoptique inversé où la périphérie surveille aussi le centre et la production de services. Ce peut donc être

aussi bien l'enfer de *big brother* que le paradis de la transparence pour satisfaire l'obsession de tout voir. Le numérique ne se substitue jamais à une réalité, que ce soit l'information, le transport ou la politique, mais l'augmente et l'élargit. Ce peut donc être tout autant le totalitarisme augmenté que la démocratie augmentée.

Nous avons déjà des outils juridiques pour gérer cela, comme la Commission nationale de l'informatique et des libertés et ses règlements, mais il me paraît essentiel d'aller plus loin en provoquant de vrais débats de société sur cette double dialectique entre privé et public et entre sécurité et liberté, dont les frontières sont aujourd'hui profondément remises en cause. ■

PROPOS RECUEILLIS PAR
PHILIPPE ESCANDE