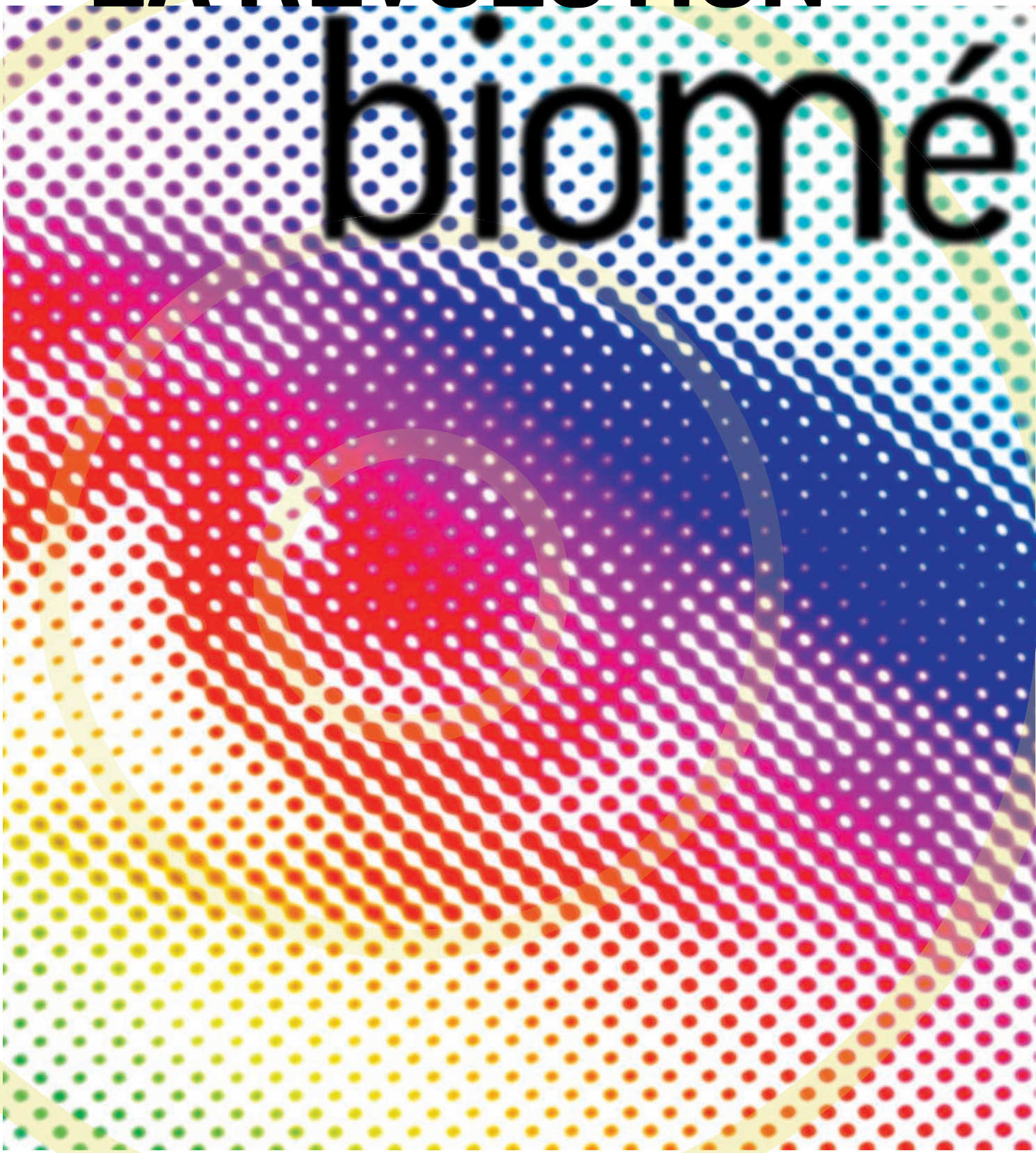
LA RÉVOLUTION biomé



VICTOR HABBICK VISIONS/SPL

trique

Dix ans après les attentats du 11 septembre 2001, l'industrie de la surveillance est en plein essor. Mais pour notre sécurité, va-t-on trop loin ?

Par Marine Corniou

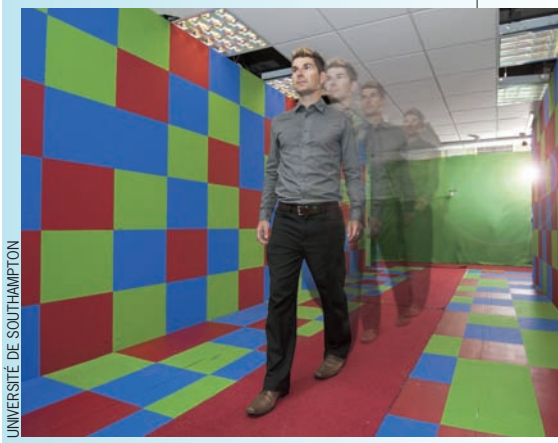
Au premier étage de l'aéroport Montréal-Trudeau, dans la salle des arrivées, les hommes d'affaires pressés savent désormais comment échapper à la longue file d'attente des douanes canadiennes. Il leur suffit de se présenter à une borne automatique Nexus. Cet appareil ultramoderne photographie l'iris de leurs yeux, identifiant ainsi l'individu qui peut entrer sans autre formalité sur le territoire canadien. Depuis sa mise en place, en 2007, le programme Nexus a permis à près de 400 000 voyageurs canadiens et états-uniens de gagner de précieuses minutes en faisant les yeux doux à ces machines. Mieux qu'un passeport, c'est le corps qui sert désormais de pièce d'identité.

« Cette technologie facilite le passage à la frontière de voyageurs considéré comme étant à faible risque. Avant d'être enregistrés dans le système Nexus, ils se sont prêtés à une entrevue, et on a vérifié qu'ils n'avaient pas d'antécédents judiciaires, explique Marie-Géralde Georges, surintendante des Services frontaliers du Canada à l'aéroport Trudeau. Cela nous permet de consacrer plus de temps aux passagers à risque. » Car ces technologies ont toutes le même but : s'assurer qu'un individu dangereux ne se fait pas passer pour un autre. Une borne Nexus est en effet difficile à duper. Si on peut mentir sur sa date de naissance ou sur son nom, les iris, eux, ne trompent pas. « La machine se base sur un algorithme qui utilise 244 points de référence dans chaque iris pour repérer l'individu dans une base de données, précise Ingrid Muzac, agente des Services frontaliers du Canada. Nous avons même deux vrais jumeaux inscrits au programme et la machine les distingue parfaitement. »

L'emploi des technologies « biométriques », qui permettent d'identifier une personne grâce à ses caractéristiques physiques ou biologiques, a littéralement explosé depuis les attentats du 11 septembre 2001. Ce jour-là, les États-Unis sont entrés en guerre contre le terrorisme et ont mobilisé le monde entier autour du même objectif :

Au pas !

Les mannequins le savent bien : leur démarche chaloupée est une véritable « signature ». Et si la démarche de monsieur Tout-le-Monde ne fait pas fantasmer les foules, elle n'en est pas moins unique. « La démarche n'est pas aussi distinctive que les empreintes digitales ou l'iris. Mais c'est la seule marque reconnaissable à distance, même lorsque la personne est de dos », explique Mark Nixon, de l'université de Southampton, au Royaume-Uni. D'où son idée de créer un **« tunnel »** de 4 m de long, utilisable dans les aéroports ou à l'entrée de certains bâtiments, pour enregistrer puis reconnaître la démarche des passants. Dans cet appareil expérimental, 10 caméras numériques collectent des informations sur la taille de l'individu, sa cadence, sa silhouette et ses mouvements, afin de recréer un modèle en 3 dimensions qui sera conservé dans la base de données. Pour l'instant, il



UNIVERSITÉ DE SOUTHAMPTON

faut cinq minutes pour « fabriquer » le modèle 3D, mais les chercheurs pensent que d'ici deux ans, le calcul ne prendra que quelques secondes. « Le problème majeur avec la biométrie comportementale, comme l'analyse de la démarche, c'est qu'elle est facilement modifiée par l'âge, un accident ou une prise de poids. Il faut donc qu'elle soit utilisée en combinaison avec d'autres indicateurs plus précis », avertit le chercheur. C'est la raison pour laquelle les caméras du tunnel « volent » au passage 90 photos des oreilles et du visage, histoire de combiner reconnaissance faciale et reconnaissance de la démarche. Les premiers tests sont encourageants : une centaine de participants s'y sont prêtés, et le système a confirmé leur identité dans 99 % des cas. Reste à prouver que la fiabilité sera la même si la base de données contient des milliers de « démarches » enregistrées. En Chine, des chercheurs de l'Institut des machines intelligentes, à Hefei, ont mis au point un « tapis » qui analyse discrètement la pression des pas et identifie le marcheur. Un système qui aurait fait ses preuves avec plus d'un millier de cobayes.

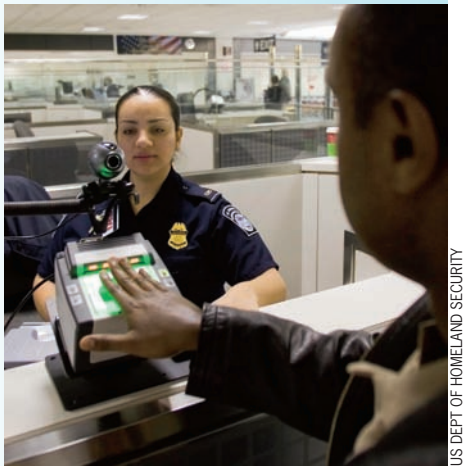
Au bout des doigts

Emblématique des films policiers, la prise des empreintes digitales est la plus ancienne mesure biométrique, et demeure encore la plus répandue. Les empreintes (ou dermatoglyphes) se forment avant la naissance, entre la dixième et la vingt-quatrième semaine de grossesse. Elles sont façonnées par les gènes, mais aussi par l'environnement dans lequel se développe le fœtus, notamment par les mouvements du liquide amniotique, les frottements des doigts entre eux ou contre les structures utérines. Si bien qu'elles dessinent un motif unique à chaque doigt et à chaque individu.

Fiable et peu coûteuse, la prise d'empreintes ne se fait plus en pressant son doigt sur un tampon imbibé d'encre, mais grâce à des capteurs optiques ou électroniques. En pratique, on pose le ou les doigts sur une surface de verre, et un appareil photo muni de diodes capture l'image en illuminant les crêtes et les sillons digitaux. L'image est numérisée puis un algorithme la «traduit» en code mathématique, en tenant compte des coordonnées d'une centaine de points (points de bifurcations des lignes, terminaisons, boucles, etc.). Pour comparer deux empreintes entre elles, il suffit ensuite de vérifier une quinzaine de points. Statistiquement, il est impossible de trouver deux individus – même des jumeaux – qui ont en commun 12 points caractéristiques.

Sauf que les lecteurs optiques traditionnels sont faciles à duper. Ils ne font pas la différence entre un vrai doigt et un doigt en résine ou en silicone, et les traces de doigts laissées par l'utilisateur précédent peuvent brouiller la lecture. De nouveaux types de capteur, les capteurs «capacitifs», permettent de minimiser les fraudes. Ils sont constitués de minuscules électrodes qui mesurent les variations de conductivité électrique entre les crêtes en contact avec le capteur et les sillons qui ne le touchent pas. Ils détectent le silicone, mais des doigts trop secs ou trop humides peuvent fausser les données. Les capteurs les plus sophistiqués sont ceux qui mesurent aussi la chaleur de la peau, voire le flux sanguin.

Au Québec, la police dispose de bornes qui permettent d'enregistrer l'empreinte des 10 doigts, mais aussi celle de la paume et du côté de la main. La raison? Si un criminel s'appuie contre un mur, sur une scène de crime, il le fait rarement avec l'index.



US DEPT OF HOMELAND SECURITY

La borne automatique Nexus à l'aéroport Montréal-Trudeau. Elle confirme l'identité du passager en photographiant son iris.

la sécurité. Plus de 80 pays ont déjà doté leurs citoyens d'un passeport biométrique, dont la puce électronique contient une photo et les empreintes numérisées des deux index. Certains pays, comme le Mexique, vont encore plus loin. En janvier 2011, le président y a déclaré que tous les jeunes de moins de 17 ans devraient désormais posséder des cartes d'identité biométriques (incluant les empreintes numériques des 10 doigts et de l'iris). Le Canada devrait lui aussi détenir ce genre de passeport très bientôt.

Cette gestion policière des citoyens est justifiée, selon les gouvernements, par le caractère aussi insaisissable qu'imprévisible du terrorisme. Dans cette lutte où l'ennemi est partout, la science apporte des moyens puissants de contrôle, de repérage et d'identification des personnes.

Empreintes digitales, iris, mais aussi forme des mains, des veines, du visage ou même du squelette, chaque parcelle de notre corps peut être scannérisée, photographiée, numérisée et stockée dans des bases de données pour servir ensuite à prouver notre identité.

Cette obsession sécuritaire est soutenue par des ordinateurs toujours plus performants, des techniques photographiques d'une grande précision, une analyse quasi instantanée des données et une baisse des coûts de la technologie. Si bien que la biométrie fleurit partout: dans les prisons, les écoles, les hôpitaux, les banques et les entreprises. Au Japon, 80 % des distributeurs automatiques de billets sont équipés d'un lecteur des veines de la main, permettant de s'assurer que la carte bancaire est utilisée par son propriétaire. Plusieurs pays, dont la France et les États-Unis, ont même installé des bornes de contrôle d'empreintes digitales dans les cafétérias scolaires, pour vérifier l'identité des jeunes clients. Il faut dire que la sécurité est un filon en or. En 2014, on prévoit que le marché mondial de la biométrie représentera 9,4 milliards de dollars : c'est trois fois plus qu'en 2009.

L'entreprise montréalaise Technologies Excellium surfe allègrement sur cette vague. Depuis sa fondation, en 2006, le nombre de ses clients n'a cessé d'augmenter. La PME fournit des produits et services biométriques aux gouvernements, à la police, aux aéroports, aux gestionnaires d'immeubles et aux en-

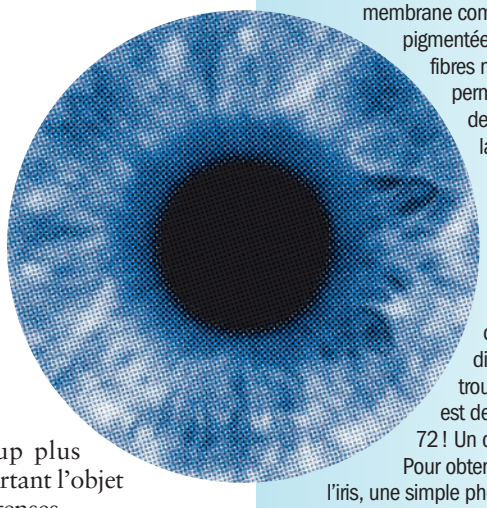
EXCELLIUM

La biométrie fleurit partout : dans les prisons, les écoles, les hôpitaux, les banques et les entreprises. En 2014, le marché mondial de cette industrie représentera 9, 4 milliards de dollars.

treprises commerciales. « Nous gérons aussi l'accréditation des participants à de grandes réunions, comme le G8 et le G20 à Toronto en 2010 », explique le président Jean-Claude Siew, au cours d'une visite pour le moins ludique. Car chez Excellium, chaque porte est dotée d'un « gadget » différent. L'homme affable présente son visage à un système de reconnaissance faciale, et la porte s'ouvre instantanément. Pour franchir les sas suivants, il lui suffit d'effleurer les bornes avec son doigt. Ses empreintes ou le dessin des veines de ses mains, préalablement enregistrés dans la banque de données, sont aussitôt reconnus. De quoi faciliter la vie de nombreux utilisateurs, affirme cet entrepreneur énergique. « Plutôt que de porter sur soi des cartes et des documents falsifiables, ou de mémoriser des dizaines de mots de passe, on n'a besoin que de soi-même pour s'identifier : c'est beaucoup plus pratique », soutient-il.

Mais la biométrie peut aussi se montrer sous un jour plus inquiétant. « Il existe deux usages bien différents de ces technologies : celui qui permet d'authentifier les gens, c'est-à-dire de s'assurer qu'ils sont bien qui ils disent être, et celui qui permet de repérer les criminels et de les surveiller à leur insu », souligne Jean-Claude Siew. Cet usage, beaucoup plus controversé, fait pourtant l'objet de recherches très intenses.

D'ici quelques années, la reconnaissance du visage, de l'iris ou du squelette permettra probablement de repérer un criminel recherché dans une foule anonyme. La façon dont une personne bouge, parle ou tape sur un clavier d'ordinateur – ce que l'on appelle la « biométrie comportementale » – peut aussi trahir son identité. Comme nombre de poseurs de bombes sont inconnus des services de police, on a tout intérêt à apprendre à dicerner les gens au comportement suspect ou faisant montre d'une nervosité inhabituelle. Dans ce domaine, les Israéliens ont pris une longueur d'avance. L'aéroport Ben-Gourion de Tel-Aviv, considéré comme l'un des plus sûrs au monde, est équipé de bornes d'enregistrement qui posent une série de questions au voyageur, et mesurent discrètement les variations de pouls, de température ou du rythme respiratoire. « Quand on dissimule quelque chose, notre corps réagit. Nos capteurs mesurent plus de 12 paramètres physiologiques à distance, les analysent en quelques secondes et peuvent repérer les personnes mal intentionnées », explique Ehud Givon, directeur général de l'entreprise qui a conçu les bornes, WeCU Technologies, située à Césarée, au nord de Tel-Aviv. Le système, affirme-t-il, est fiable à 97 % et parvient à différencier les terroristes des phobiques de l'avion. Au Canada, des chercheurs du ministère de la Défense nationale travaillent aussi sur le repérage des comportements hostiles. Pas moyen d'en savoir plus : le Ministère a décliné nos demandes répétées d'entrevue. Le sujet est sensible…



D'un seul regard

La reconnaissance de l'iris est considérée comme la technique biométrique la plus fiable. Seul organe interne visible de l'extérieur, il est très peu modifié par le vieillissement, et sa texture est unique. L'iris, qui est la partie colorée de l'œil, est une sorte de membrane composée de cellules pigmentées et de deux couches de fibres musculaires, qui lui permettent de se contracter ou de se dilater en fonction de la luminosité. Ces fibres, dont l'enchevêtrement résulte du hasard du développement embryonnaire, constituent un motif encore plus complexe que les empreintes digitales. La probabilité de trouver deux iris identiques est de 1 sur 10 à la puissance 72 ! Un chiffre inimaginable.

Pour obtenir une « empreinte » de l'iris, une simple photo suffit. On utilise en général l'infrarouge, car cette source d'éclairage n'éblouit pas et évite les reflets sur l'œil. Un logiciel extrait ensuite les caractéristiques de l'iris et les traduit en un code à barres unique. Outre sa grande précision, cette technique a l'avantage d'être difficile, voire impossible, à tromper. Les capteurs étudient la réaction de l'œil aux variations de la lumière, pour s'assurer qu'il ne s'agit pas d'un œil de verre, et détectent sans problème le dessin simpliste des lentilles colorées.

Seul inconvénient, la reconnaissance de l'iris demande une bonne coopération de l'utilisateur. La plupart des systèmes requièrent de se placer à 20 cm de la borne, de garder les yeux dans le même axe et de refaire la photo plusieurs fois si la première image est floue. Cependant, en 2010, la firme états-unienne Sarnoff a développé un appareil capable de capter l'image de l'iris de personnes en mouvement, jusqu'à une distance de 3 m, et de vérifier leur identité, au rythme de 30 personnes par minute !

Jusqu'aux os

Pas besoin d'être mort pour montrer son squelette. Les chercheurs du Wright State Research Institute, aux États-Unis, tentent de mettre au point un scanneur capable de révéler la structure osseuse d'une personne à 50 m de distance. C'est que chaque squelette est unique, de par sa densité, sa forme, ses anomalies et ses « cicatrices » (broches métalliques, anciennes fractures, etc.). Impossible pour un malfaiteur de mentir au scanner ou de « déguiser » ses 206 os… Cependant, il faut disposer d'une base de données de référence où les os des terroristes recherchés ont déjà été scannés une première fois. Or, faire accepter ce système par la population risque d'être délicat, car l'exposition répétée aux rayons X ou gamma, qui permettent de voir le squelette, peut augmenter le risque de cancer.

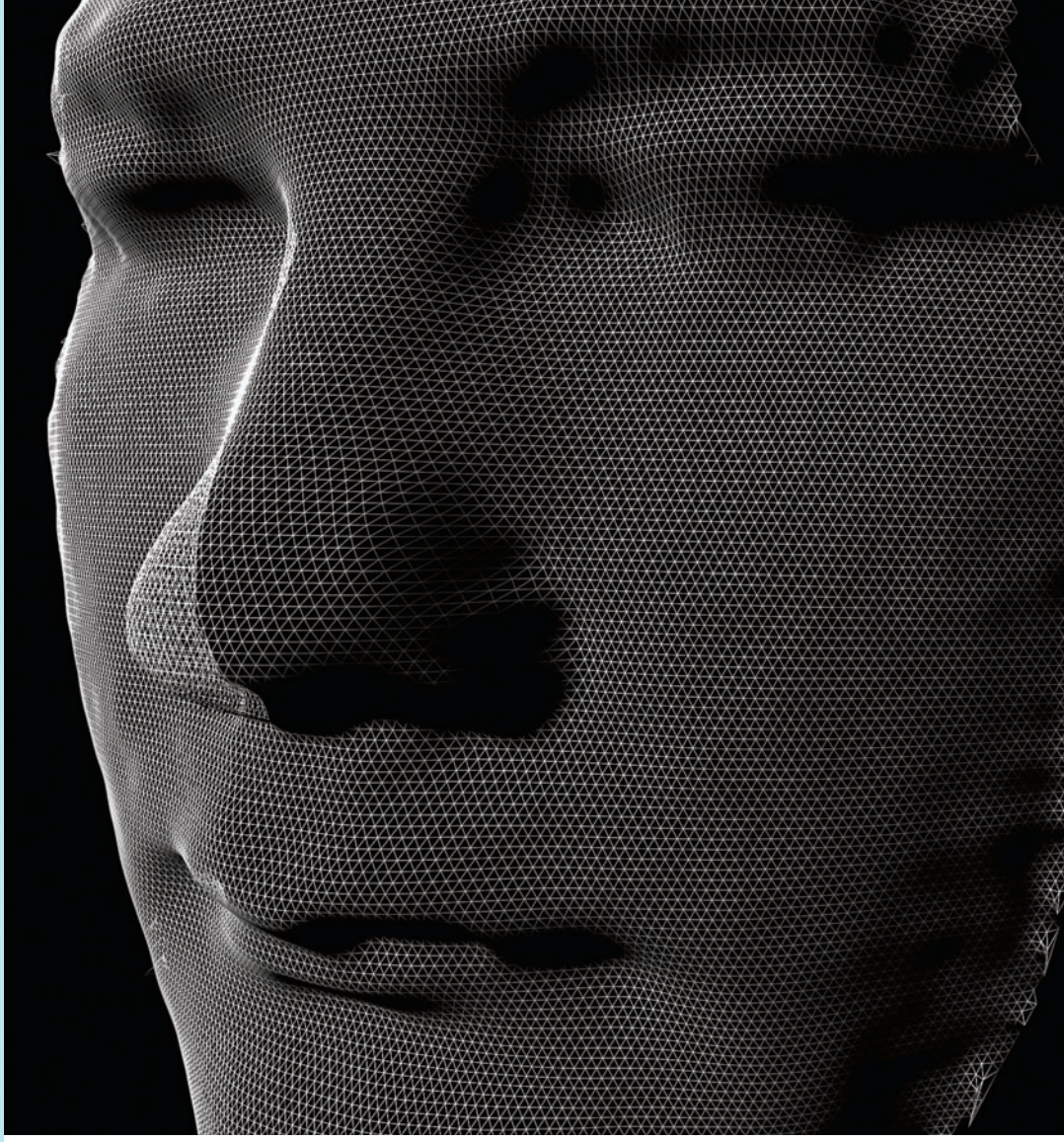
À visage découvert

Depuis des décennies, douaniers et policiers comparent les visages des gens à leur photo d'identité. D'où l'idée d'automatiser la « **reconnaissance faciale** ». En matière de surveillance, il n'y a pas plus prometteur. La reconnaissance du visage pourrait être utilisée à distance et permettre de repérer un criminel recherché dans une foule, à l'aide de caméras postées dans la rue ou les aéroports. La technique, encore expérimentale, n'est utilisée pour le moment qu'à des fins d'authentification, pour reconnaître une personne déjà enregistrée qui présente docilement son visage à la caméra. Un logiciel en extrait un ensemble de points peu susceptibles de varier dans le temps (écartement des yeux, distance nez-bouche, etc.), afin de créer un modèle graphique, en deux ou trois dimensions. Ce modèle peut dès lors être comparé à la photo du passeport biométrique, comme c'est le cas depuis 2007 dans les principaux aéroports d'Australie ou du Royaume-Uni.

Mais la technique est loin d'être parfaite. En février dernier, un homme a franchi les bornes de l'aéroport de Manchester, au Royaume-Uni, avec le passeport de sa femme. Le couple avait échangé par mégarde les deux passeports, et seule la femme s'est vu refuser le passage.

Si la fiabilité de la reconnaissance faciale laisse à désirer, c'est parce que de nombreux facteurs peuvent modifier l'aspect d'un visage : les conditions d'éclairage, l'angle de présentation à la caméra, les expressions (un sourire, par exemple), mais aussi le maquillage, le vieillissement, des lunettes, une barbe, etc. Ainsi, la même personne photographiée dans des conditions différentes peut être impossible à reconnaître, même pour un œil humain. C'est pourquoi les systèmes actuels ne sont réellement efficaces qu'avec la coopération du sujet, dans de bonnes conditions d'éclairage. « Il y a une grande différence entre comparer deux photos statiques et analyser un visage qui se déplace sur une séquence vidéo », explique Éric Granger, professeur au département de génie de la production automatisée à l'École de technologie supérieure de Montréal. Son équipe a toutefois réussi à développer un logiciel capable de « poursuivre » un visage en mouvement, qui devrait être testé l'année prochaine par les services frontaliers canadiens.

Reza Shoja Ghiass, du laboratoire de vision et systèmes numériques de l'Université Laval, a quant à lui misé sur une approche inédite : la reconnaissance faciale entièrement basée sur l'image infrarouge. « Mon système permettra de discerner le réseau veineux du visage, qui est très peu altéré par le vieillissement et par les expressions. C'est une technologie qui permet de reconnaître un visage déguisé ou maquillé dans l'obscurité totale ! » explique-t-il. Il reste toutefois quelques problèmes à régler, notamment le fait que le verre des lunettes bloque les infrarouges et fait perdre beaucoup d'information.



Les logiciels de reconnaissance faciale traduisent le visage en un modèle graphique en deux ou trois dimensions.

Cela ne surprend pas René Provost. Selon ce professeur de droit et fondateur du Centre sur les droits de la personne et le pluralisme juridique de l'Université McGill, « le contrôle des frontières est devenu le point névralgique de la réflexion sur les droits de la personne. Lorsqu'on se présente aux frontières, on doit, dans une certaine mesure, renoncer à la protection de nos droits fondamentaux, affirme-t-il. Depuis le 11 septembre 2001, les intérêts généraux de la société priment sur les droits de la personne. »

Ainsi, en 2008, le Royaume-Uni a été condamné par la Cour européenne des droits de l'homme pour avoir constitué une base de données contenant le profil ADN de 5 millions de personnes, dont 100 000 n'avaient été impliquées dans aucun crime ou délit ! Quant aux militaires états-uniens, ils ont ramené d'Irak des milliers de données biométriques de civils (empreintes digitales ou iriennes, photographies) collectées arbitrairement.

L'ensemble de la société est en fait aux prises avec une redéfinition de la « sphère privée ». Au Royaume-Uni, par exemple, il est difficile de se promener incognito dans la rue. Deux millions de caméras scrutent la population en continu, si bien que chaque citoyen peut être filmé 70 fois par jour ! Et la grande majorité de ces caméras appartiennent à des sociétés privées, qui gèrent les données comme elles l'entendent. Car la technologie a avancé plus vite que les lois, et le développement fulgurant de la biométrie s'est fait sans garde-fous juridiques.

Or, il y a des problèmes. Les machines ont beau être très perfectionnées, chaque technique peut conduire à de faux rejets ou à de fausses acceptations.

« Jusqu'à quel point peut-on tolérer les erreurs ? s'interroge Stéphane Leman-Langlois, chercheur en criminologie à l'Université Laval et titulaire de la Chaire

de recherche du Canada en surveillance et construction sociale du risque. Dans un casino privé, si le droit d'entrée est refusé à tort, les conséquences sont minimes. En revanche, dans le service public, une erreur est bien plus grave, car elle peut bafouer les droits des citoyens. » Et que se passera-t-il, par exemple, si une personne est reconnue à tort comme faisant partie d'une liste de criminels recherchés? Bénéficiera-t-elle de la présomption d'innocence? « Il y a des risques de dérapage, c'est sûr, surtout dans des pays où les droits de la personne sont bafoués, comme la Chine. Ce qui est important, c'est que la biométrie demeure un outil. Les machines ne doivent en aucun cas prendre la décision finale », avertit René Provost.

Quant à savoir si la biométrie tiendra ses promesses de lutte contre le terrorisme, rien n'est moins sûr. D'une part, le lien entre le contrôle des frontières et la prévention des attaques terroristes est loin d'être établi; d'autre part, « les événements terroristes étant objectivement rares, on ne dispose pas de suffisamment de données statistiques pour évaluer l'efficacité de ces mesures », souligne Stéphane Leman-Langlois.

Ni pour mesurer les dérives de cette industrie florissante… QS

EXCELLIUM

« Il y a des risques de dérapage, c'est sûr, surtout dans des pays où les droits de la personne sont bafoués. Ce qui est important, c'est que la biométrie demeure un outil. Les machines ne doivent en aucun cas prendre la décision finale. »

Prêter l'oreille

Décollées, rondes, avec ou sans lobe, les oreilles aussi peuvent trahir notre identité. « Moins affectées par le vieillissement que le reste du visage, elles ont l'avantage d'être formées dès la naissance et de peu se modifier. Leur taille peut changer, mais leur structure reste la même. Les oreilles sont donc un excellent "outil" biométrique », souligne Mark Nixon, chercheur à l'université de Southampton, au Royaume-Uni. Pour le démontrer, son équipe a utilisé un logiciel qui permet de projeter des rayons lumineux virtuels sur une photo d'oreille et d'en déduire sa structure tridimensionnelle, même si elle est en partie cachée par des cheveux. En 2010, les chercheurs ont conduit des tests sur 252 photos d'oreilles, pour voir si le logiciel pouvait les apparier avec autant de photos de visages de profil. Résultat? Dans 99,6 % des cas, la machine a associé les oreilles à leur propriétaire.

Sous la peau

Le réseau des vaisseaux sanguins, et plus précisément celui des veines, dessine un motif unique et impossible à copier, et son authentification est simple : la paume de la main ou le doigt sont éclairés par des rayons infrarouges, qui sont absorbés par l'hémoglobine (le pigment rouge du sang). Les veines apparaissent donc en noir sur fond blanc, et leur cartographie est modélisée par un algorithme. Contrairement aux empreintes digitales, la biométrie du réseau veineux peut se faire sans contact. Au Japon, plus de 80 % des distributeurs automatiques de billets sont équipés de cette technologie ! De même, certaines voitures ne démarrent qu'après avoir reconnu le doigt du conducteur. Depuis 2009, Sony commercialise même un lecteur miniaturisé qui reconnaît les fines veines du bout du doigt, et peut être intégré à un téléphone cellulaire ou à un ordinateur. L'entreprise nippone Fujitsu, leader dans ce domaine, affirme que le taux de fausses acceptations (personnes reconnues par erreur) est inférieur à 0,00008 %. Quant aux probabilités de fraudes, elles sont négligeables. Même l'idée sordide de couper le doigt de quelqu'un et de s'en servir comme passe a été prise en considération par les fabricants. Les capteurs ne fonctionnent que s'ils détectent plusieurs signes vitaux, comme le pouls ou la saturation en oxygène.

La biométrie des gènes

Au royaume de la biométrie, l'identification par ADN devrait être reine. Impossible à berner et valable de la naissance à la mort, la signature génétique d'un individu est la plus fiable pour identifier un individu ! Mais cette technique présente d'importants défauts : elle coûte cher (600 $ à 1 500 $ par test), nécessite des analyses qui prennent plusieurs heures ainsi qu'un prélèvement de cellules (sang, salive, peau). Pour l'instant, elle est donc réservée à l'identification à partir de prélèvements effectués sur des scènes de crime. C'est notamment grâce au prélèvement « préventif » de l'ADN d'une sœur d'Oussama Ben Laden que le corps du chef d'Al-Qaïda a pu être identifié, le 2 mai dernier. Il a suffi de comparer l'ADN du cadavre à celui de sa sœur pour confirmer le lien. Cette technique est utilisée pour vérifier la parenté des réfugiés et des demandeurs d'asile, ou dans le cadre du regroupement familial.

Dans tous les sens

Voix douce ou aiguë, parfum fleuri ou musqué… on reconnaît nos proches sans les voir, au nez ou à l'oreille ! Des pistes également explorées par la biométrie. La reconnaissance vocale, cependant, est loin d'être fiable. Comme toutes les caractéristiques comportementales, la voix peut être modifiée volontairement, se transformer avec l'âge ou à la suite d'une maladie. Elle reste intéressante comme première approche de reconnaissance, notamment par téléphone.

Quant à l'odeur, les chiens le savent bien : chaque humain en a une qui lui est propre. Cette odeur est constituée de plusieurs substances chimiques volatiles, dont la combinaison est unique. Ces composés peuvent être capturés et analysés par des « nez électroniques ». Encore au stade expérimental, cette technique a l'avantage de pouvoir être utilisée à distance.

Le réseau des veines de la main est spécifique à chacun. Il peu donc servir à nous identifier.