Dossiers de préparation pour le groupe Radicalisation

Une réponse à la radicalisation : le développement de la reconnaissance faciale

Reconnaissance faciale : comment nos visages sont traqués

Par Frédéric Joignot

Publié le 22 mars 2018 à 17h00 - Mis à jour le 23 mars 2018 à 11h12

ENQUÊTE

Dans la rue, dans les commerces, sur Internet, des algorithmes peuvent à tout moment nous identifier. Ces nouveaux outils, auxquels s'intéressent professionnels du marketing et forces de l'ordre, posent d'importantes questions éthiques.

Notre visage est la source de l'éthique du fait qu'il est nu, expressif, doué de la parole humaine et semble nous dire : *« Tu ne me défigureras pas »*ou, plus profondément : *« Tu ne tueras point »,* assure le philosophe Emmanuel Levinas (1906-1995). De son côté, l'anthropologue David Le Breton avance que le visage, auquel il a consacré plusieurs études,*« incarne la différence infinitésimale portée par chaque homme »,* mais aussi, étant changeant et mobile, *« donne vie à notre esprit »,* ce qui fait qu'*« on tombe amoureux d'un visage, ou le déteste parfois »*...

Aujourd'hui, nos traits sont devenus une donnée exploitable : les progrès de la numérisation en ont fait une marchandise convoitée par les géants du Web, les experts du marketing et les services de police. La publicité ciblée est en effet devenue le carburant de l'économie numérique. Avec le visage, le profilage systématique des internautes s'affine.

Prenez Facebook, ce grand « livre du visage », le réseau social aux 2 milliards d'utilisateurs actifs : il engage chaque jour les internautes à taguer les photos qu'ils publient avec les noms de leurs « amis ». Puis, grâce à DeepFace, son système de reconnaissance faciale, l'entreprise se constitue une gigantesque banque de visages identifiables. Du big data*« très précieux »* à l'heure du *« boom du marketing personnalisé »,* fait remarquer Benjamin Sobel, chercheur en droit et technologie à l'université Harvard (Massachusetts), préoccupé par la disparition de l'anonymat sur le Web et les réseaux sociaux.

Repérer les voleurs jusque sur le trottoir

Sans surprise, Google s'y intéresse aussi. L'algorithme de reconnaissance faciale FaceNet de Google Photos est capable d'identifier, de nommer, de classer et de localiser d'innombrables personnes présentes sur les albums des internautes. Si cette fonction a été désamorcée en Europe à la demande des défenseurs de la vie privée, elle reste utilisable par quiconque domicilie ses recherches depuis un autre pays.

L'identification de nos visages intéresse particulièrement les enseignes d'e-commerce, les banques, les grandes surfaces… En 2017, Amazon a lancé Rekognition, un service de reconnaissance d'images permettant d'identifier des personnes. L'entreprise affirme avoir stocké plusieurs*« dizaines de millions de visages »* et pouvoir les détecter – déjà, la police américaine utilise cette application dans plusieurs Etats. Quant à la société californienne FaceFirst, elle vend un système de reconnaissance faciale permettant aux grandes surfaces de reconnaître leurs clients fidèles et de repérer les voleurs jusque sur le trottoir.

L'intrusion brutale de ces technologies de détection dans notre vie quotidienne suscite déjà de lourdes oppositions. En juin 2015, aux Etats-Unis, neuf associations de défense des libertés civiles et des consommateurs ont rompu leurs discussions sur la légalité de la reconnaissance faciale avec des représentants du commerce. Elles ont déclaré : *« 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 leurs noms. »*

De l'importance de l'obscurité

Analysant l'échec de ces négociations, qui n'ont pas repris à ce jour, le professeur de droit Woodrow Hartzog, de l'université de Samford (Alabama), et le philosophe Evan Selinger, de l'Institut de technologie de Rochester (New York), ont défendu dans *The Christian Science Monitor* du 22 juin 2015 l'importance de l'*« obscurité »* dans la définition de la vie privée.

Nous exhibions sans peur notre visage en public ou sur Internet, rappellent-ils, parce que nous avions l'habitude d'y conserver un anonymat suffisant : dans la rue, nous ne pouvons pas identifier tous les passants ; nous y sommes plus ou moins incognito. Aujourd'hui, cette part d'obscurité est menacée par la vidéo : assistée par l'intelligence artificielle, elle développe une capacité mémorielle supérieure à celle des humains, tout en stockant visages et données personnelles.

L'entreprise Affectiva certifie posséder *« la plus grande base de données d'émotions faciales du monde : 6,3 millions de visages décryptés dans 87 pays ».*

L'obscurité ne signifie pas l'*« inaccessibilité totale »,* estime Woodrow Hartzog, mais le maintien d'une part d'ombre : pour cela, déjà, on renforce ses paramètres de confidentialité, on utilise des messageries cryptées, on enclenche la touche « Avion » de son portable. Cette *« obscurité pratique »,* estime-t-il, devrait être renforcée avec l'extension des nouvelles technologies biométriques, afin de *« favoriser l'autonomie, l'épanouissement personnel, la socialisation et la liberté face aux abus de pouvoir ».*

Las, l'inverse se passe. Non seulement des entreprises du numérique nous fichent puis revendent nos données et nos visages à des services de marketing – et parfois, nous le savons depuis les révélations d'Edward Snowden de 2013, les divulguent à la police –, mais elles entreprennent d'interpréter les sentiments qu'exprime notre visage afin de prévoir nos comportements. Afin surtout – c'est le nerf de la guerre commerciale – de devancer nos désirs. Ainsi, le service Amazon Rekognition assure pouvoir détecter *« l'état de bonheur, de tristesse ou de surprise à partir d'images faciales ».*

Quelques applications sociales ou médicales

D'autres sociétés américaines, Affectiva, Emotient, Realeyes, utilisent des logiciels de *« décryptage des émotions ».* Les logiciels d'Affectiva filment et*« numérisent en temps réel »* les visages, *« identifient les repères clés, comme les coins de vos sourcils ou de votre bouche »,* puis les algorithmes les décodent en s'appuyant sur une grille de lecture émotionnelle – l'entreprise certifie posséder *« la plus grande base de données d'émotions faciales du monde : 6,3 millions de visages décryptés dans 87 pays ».*

D'où provient cette grille d'analyse de nos sentiments les plus intimes ? La société a été créée par des chercheurs en « informatique affective »*(affective computing).* Fondé en 1995 par la chercheuse du Massachusetts Institute of Technology (MIT) Rosalind Picard, ce champ de recherche se situe au croisement de la morphopsychologie, de la biométrie et de l'informatique. Il s'inspire des travaux du psychologue américain Paul Ekman, qui a étudié dans les

années 1970 les *« micro-expressions faciales »* de milliers de personnes jusqu'à prétendre identifier les sept *« émotions primaires »* exprimées par notre visage, selon lui *« universelles »,* car léguées par l'évolution : la colère, le dégoût, la joie, le mépris, la peur, la tristesse, la surprise.

Pour l'informatique affective, ces expressions basiques peuvent être photographiées, numérisées, cartographiées, puis identifiées par des algorithmes d'intelligence artificielle. Un ordinateur ou un robot équipé d'un tel logiciel peut alors appréhender nos affects.

Si quelques-unes de ces recherches visent des applications sociales ou médicales – lunettes pour aider les enfants autistes à décrypter les expressions, capteurs pour repérer de façon anticipée et objective un état dépressif –, beaucoup d'entre elles ont trouvé des débouchés commerciaux. Aujourd'hui, Affectiva vend ses produits à des publicitaires et à des fabricants qui veulent tester en direct les réactions*« spontanées »* de clients à leurs produits : clip, jouet, habitacle de voiture…

Difficile de ne pas penser aux dystopies décrites par le roman *Le Cercle*, de Dave Eggers (2013, Gallimard, 2016) ou par la série britannique *Black Mirror* (2011-2018), un meilleur des mondes où nos visages et nos sentiments sont livrés en pâture aux algorithmes de décryptage qui nous traquent en tout lieu, prétendent nous connaître mieux que nous-mêmes – et juger nos comportements.

Un zèle décuplé

La grille émotionnelle des visages d'Ekman est très critiquée par les anthropologues et les ethnologues, pour qui les émotions faciales et leur signification – prenez le fait de pleurer ou de rire – varient considérablement d'un pays à l'autre : elles sont symboliques, liées à une culture, des habitus. Elles sont complexes, ambiguës, difficiles à cerner – et irréductibles à une lecture simpliste.

En septembre 2017, des chercheurs de l'université Stanford (Californie) ont annoncé avoir mis au point un dispositif de reconnaissance faciale capable de déterminer si une personne est homosexuelle avec une précision de 91 %.

L'anthropologue David Le Breton nous met en garde : *« La morphopsychologie confond le "visage", mobile, joueur, capable de simulation, et la "figure", au sens géométrique. Elle résume notre face à un ensemble de points, qu'elle prétend lire comme une carte représentant un territoire figé, alors que la contenance et l'équivoque sont le propre de l'humain, qui peut rire et pleurer à la fois ! La grille d'Ekman n'est que statistique, elle génère beaucoup d'erreurs d'interprétation qui révèlent souvent les préjugés des chercheurs. »*

De fait, en septembre 2017, des chercheurs de l'université Stanford (Californie) ont annoncé avoir mis au point un dispositif de reconnaissance faciale capable de déterminer si une personne est homosexuelle avec une précision de 91 %. Une avalanche de critiques a mis au jour leurs biais. David Le Breton ironise : *« Nous ne sommes pas loin de la physiognomonie du XIX^e^ siècle, la pseudoscience promue par le criminologue Cesare Lombroso qui prétendait définir le caractère et la dangerosité d'une personne au seul paramétrage de sa figure. »*

Non seulement nos traits et nos expressions intéressent les grandes entreprises, mais la traque du visage est aussi, bien sûr, la grande affaire des services de police – qui la pratiquent avec un zèle décuplé depuis la vague d'attentats terroristes. Elle est d'ores et déjà mise en œuvre à travers deux technologies : la reconnaissance faciale associée à la vidéosurveillance « intelligente » et la constitution de portraits-robots à partir d'échantillons d'ADN. Aux Etats-Unis, la première n'est soumise à aucune loi fédérale, si bien que le FBI et les shérifs des comtés l'utilisent massivement.

« Sans précédent et très problématique »

Une étude d'octobre 2016 du Center on Privacy & Technology de la prestigieuse université de droit de Georgetown (Washington DC), un think tank spécialisé sur la vie privée, dresse un état des lieux inquiétant : les visages de 117 millions d'adultes américains figurent à leur insu dans les fichiers fédéraux et locaux ; vingt-neuf Etats autorisent la police locale à chercher des visages dans les fichiers des permis de conduire, et dix-sept le permettent au

FBI, qui se construit ainsi un réseau biométrique d'*« Américains respectueux de la loi »* – une pratique*« sans précédent et très problématique »,* insiste Alvaro Bedoya, le directeur du centre.

Les juristes du Center on Privacy & Technology déplorent également que les services de police utilisent des algorithmes de reconnaissance *« pour scanner en temps réel les visages des piétons »,* notamment lors de manifestations : cela constitue à leurs yeux *« un risque réel* (…) *d'étouffer la liberté d'expression ».*

En France, la Commission nationale de l'informatique et des libertés (CNIL) s'oppose – pour l'instant avec succès – à l'utilisation systématique de la reconnaissance faciale (excepté dans les aéroports et certaines gares), mettant en garde contre le profilage *« à la volée de l'ensemble de la population »,* et contre une surveillance omniprésente qui porterait atteinte à *« la liberté d'aller et venir anonymement ».* Mais pour combien de temps ? Les avis de la CNIL, ne l'oublions pas, n'ont qu'une valeur consultative.

Reconstruction d'un visage à partir d'une bribe d'ADN

Autre grand dossier sur lequel les juristes américains et européens s'interrogent : le « portrait-robot génétique », c'est-à-dire la reconstitution d'un visage à partir de traces ADN.

Aux Etats-Unis, Parabon NanoLabs, une entreprise privée de Virginie, assure pouvoir fournir, à partir d'un échantillon d'ADN, un *« instantané détaillé »* comprenant *« la couleur des yeux, de la peau, des cheveux, la morphologie du visage et l'ascendance biogéographique détaillée »*. Sans surprise, elle travaille régulièrement avec les services de police aux Etats-Unis et au Canada. Pourtant, selon les spécialistes, la recherche est encore trop peu avancée pour reconstituer des visages fiables.

Le 17 mars 2016, critiquant un arrêt de la Cour de cassation, la Commission consultative des droits de l'homme s'est inquiétée, appelant à un encadrement légal strict du profilage génétique.

Nonobstant, en 2014, l'équipe de Mark Shriver, professeur d'anthropologie génétique à l'université de Pennsylvanie, a recueilli auprès de 600 volontaires une numérisation en 3D de leurs visages ainsi que leurs données génétiques. Le but : identifier les marqueurs génétiques affectant la morphologie faciale – c'est le phénotypage génétique *(DNA phenotyping).* L'étude révèle que *« vingt gènes montrent des effets significatifs sur les traits faciaux » ;* une séquence de huit gènes donne une bonne idée de la couleur des yeux ; deux sont en relation avec la calvitie, un seul avec les taches de rousseur…

Bref, la reconstitution d'un visage à partir d'une bribe d'ADN ne fait que commencer. En Europe, le projet Visage (Visible Attributes through Genomics), un consortium de treize partenaires provenant d'institutions universitaires, policières et judiciaires de huit pays (en France, seul l'Institut national de police scientifique y participe), a été lancé début 2017 pour affiner ces recherches. Son objectif est clair : mettre au point*« une nouvelle boîte à outils » « pour produire des informations détaillées sur l'apparence, l'âge et l'ascendance biogéographique d'un donneur de traces inconnu, aussi vite que possible ».*

Boîte de Pandore

Assurément, la reconnaissance faciale comme le portrait-robot ADN soulèvent de lourds problèmes éthiques, juridiques et démocratiques. En France, le 25 juin 2014, la Cour de cassation a admis la légalité d'un phénotypage génétique dans le cadre d'une affaire de viols en série à Lyon. Un *« arrêt spectaculaire »,* d'après Etienne Vergès, professeur de droit à l'université de Grenoble, qui se demande s'il n'est pas contraire à l'article 8 de la Convention européenne des droits de l'homme sur les données personnelles.

N'a-t-on pas ouvert une boîte de Pandore avec cet arrêt ? Le 17 mars 2016, critiquant l'arrêt de la Cour de cassation, la Commission consultative des droits de l'homme s'est inquiétée, appelant à un encadrement légal strict du profilage génétique : seul un juge d'instruction devrait pouvoir l'ordonner, en veillant à ce qu'il soit limité *« aux seuls traits objectifs, extérieurs et pertinents pour l'identification ».*

La Commission consultative des droits de l'homme comme la CNIL ne s'inquiètent pas pour rien. En Chine, fin 2017, 170 millions de caméras de vidéosurveillance étaient déjà installées – 400 millions sont prévues d'ici à 2020. Dans les grandes villes, elles sont couplées avec des systèmes de reconnaissance faciale directement reliés aux fichiers des services d'identité et sociaux : le règne du big data global sur nos vies arrive.

Chine

Est-il possible d'échapper à la vidéosurveillance en Chine ?

Big Browser

La BBC a tenté l'expérience, qui n'a bien sûr pas duré longtemps dans un pays équipé de millions de caméras fonctionnant à l'intelligence artificielle, dont la reconnaissance faciale.
Dans la ville de Guiyang, à chaque feu rouge, les caméras scannent les visages des conducteurs. Damir Sagolj / REUTERS

En Chine, l'omniprésence des caméras CCTV – 170 millions à travers le pays, et 400 millions de plus prévues dans les trois ans –, ajoutée au développement de technologies de reconnaissance faciale et d'intelligence artificielle a abouti à ce que la BBC décrit comme *« le réseau le plus étendu et sophistiqué de vidéosurveillance au monde »*.

Le correspondant de la BBC en Chine, John Sudworth, a voulu illustrer le fonctionnement de ces caméras. Il a pu accéder aux locaux de la police de la ville de Guiyang, où les près de 3 millions de citoyens sont constamment sous l'œil des caméras installées par la municipalité, comme c'est le cas dans presque toutes les grandes villes chinoises.

How long can a BBC reporter stay hidden from CCTV cameras in China? @TheJohnSudworth has been given rare access to… https://t.co/vZB8T28rLW
— BBCWorld (@BBC News (World))

Avec la complicité des policiers de Guiyang, Sudworth accepte d'être un cobaye dans une expérience pour que chacun comprenne l'efficacité, et l'omniprésence, de la vidéosurveillance. Il se fait prendre en photo dans les locaux de la police et son visage est ajouté à la base de données où figurent ceux de tous les autres habitants de la ville. Pas besoin d'organiser de séances photo, ce sont celles de leurs cartes d'identité.

Combien de temps le journaliste pourra-t-il marcher dans la ville avant d'être repéré ? En descendant de sa voiture, près du centre-ville, il tente d'aller jusqu'à la station de bus. Dès le premier pont, il repère trois caméras. Et constate :

« Ça ne sert à rien d'essayer de se cacher ici. »

Sept minutes après avoir posé un pied sur le trottoir de Guiyang, plusieurs policiers l'entourent. Même s'il n'avait pas quitté sa voiture, Sudworth ne serait pas resté incognito beaucoup plus longtemps. A chaque feu rouge, les caméras scannent les visages des conducteurs.

Dans d'autres villes, comme Shanghaï ou Shenzhen, les visages des piétons qui traversent au rouge sont projetés sur les abribus, ou sur des panneaux géants, tant qu'ils n'ont pas payé leur amende…

Royaume-uni

En catimini, le Royaume-Uni s'impose en champion de la reconnaissance faciale

En quelques années, et en toute discrétion, le pays est devenu l'un des plus en pointe dans cette technologie. Les logiciels ont tant progressé qu'ils inquiètent les défenseurs des libertés individuelles pour leurs capacités de surveillance de masse inégalées.

Par Cécile Ducourtieux Publié le 03 septembre 2019 à 02h27 - Mis à jour le 03 septembre 2019 à 10h55

Temps deLecture 7 min.

Beaucoup d'usagers de l'Eurostar connaissent King's Cross Saint Pancras. La gare terminus par laquelle ils débarquent à Londres se situe au cœur de ce quartier en pleine ébullition. Google y a déplacé son siège, la fameuse école d'art Central Saint Martins se trouve à deux pas, comme la boutique de souvenirs Harry Potter devant laquelle les fans du petit sorcier patientent dans la file d'attente pour s'offrir une réplique de son écharpe ou un selfie devant l'entrée du quai 9 3/4 d'embarquement vers Poudlard.

Personne, avant des révélations du *Financial Times*, mi-août, ne soupçonnait qu'en ce lieu grouillant de monde une expérience de reconnaissance faciale était menée. Depuis quand, dans quel objectif et avec combien de caméras activées ? Mystère. Interrogée par le quotidien britannique, l'agence Argent, chargée de la mise en valeur du site, s'est contentée d'affirmer que la technologie *« vise à assurer la sécurité du public ».* Jointe quinze jours plus tard, une porte-parole de l'agence ajoute : *« King's Cross collabore activement avec les bureaux* [du régulateur britannique des données personnelles] *Information Commissioner's Office* [ICO]. *»*

Ce dernier a en effet annoncé l'ouverture d'une enquête, dès la publication de l'article du quotidien économique. *« Scanner les visages des gens quand ils vaquent en toute légalité à leurs activités quotidiennes, avec l'objectif de les identifier, peut représenter un danger potentiel pour la vie privée, et cela doit tous nous concerner,* a déclaré, mi-août, Elizabeth Denham, la patronne de l'ICO, dans un communiqué. *Spécialement si ces technologies sont utilisées sans que les gens soient tenus au courant ni n'en comprennent le fonctionnement. »*

D'autres révélations, toutes aussi troublantes, ont suivi au cœur de l'été. Canary Wharf, l'énorme quartier d'affaires de l'est de Londres, serait lui aussi sur le point de s'équiper, toujours selon le *Financial Times*. Le 16 août, l'ONG Big Brother Watch listait les lieux, un peu partout au Royaume-Uni, où la technologie était désormais utilisée, à l'insu de *« millions de consommateurs » : « Il s'agit d'une vraie épidémie »,* concluait l'association londonienne.

Visages scannés

Des essais ont ainsi été menés en 2018 dans l'enceinte du Meadowhall, à Sheffield, l'un des plus vastes centres commerciaux du nord de l'Angleterre. Mais aussi au Trafford Center de Manchester, un autre temple du shopping, qui a potentiellement pu concerner 15 millions de personnes. A Birmingham, le centre de conférences Millennium Point est également concerné, tout comme des casinos et des maisons de paris (la chaîne Ladbrokes). Plus surprenant, le Word Museum, à Liverpool, a utilisé la technologie en 2018, au sein d'une exposition consacrée au premier empereur de Chine et à son armée de terre cuite.

Fin août, le *Sunday Times* racontait encore que Manchester City, le club de Premier League, comptait lui aussi utiliser la technologie pour limiter les files d'attente les jours de match à l'entrée de l'Etihad Stadium. Fournie par la société texane Blink Identity, elle permettrait de scanner 50 visages à la minute et de distinguer les détenteurs de billets des autres.

En quelques années, et en toute discrétion, le Royaume-Uni est devenu l'un des pays du monde les plus en pointe dans cette technologie permettant d'identifier automatiquement des personnes à partir de captures de leur visage. Les logiciels concernés ont tant progressé qu'ils inquiètent au plus haut point les défenseurs des libertés individuelles pour leurs capacités de surveillance de masse inégalées. Surtout quand les caméras de reconnaissance sont couplées à d'énormes bases de données de visages enregistrés. Les médias occidentaux ont rapporté, début 2019, que la Chine en faisait usage à l'encontre des populations musulmanes ouïgoures.

C'est d'abord la police britannique, qui, ces trois dernières années, a procédé à de nombreux tests, notamment la police du Grand Londres (lors des carnavals de Notting Hill en 2016 et en 2017) et la police du Pays de Galles du Sud. Officiellement, pour améliorer la sécurité des citoyens britanniques. Mais, désormais, nombre d'opérateurs privés s'y mettent, en toute impunité. *« En principe, les caméras dotées d'un système de reconnaissance faciale scannent les visages, puis les confrontent à des bases de données,* explique Pete Fussey, professeur de sociologie à l'université d'Essex. *Le problème, c'est que, bien souvent, nous ignorons de quelles bases de données il s'agit et quel est le véritable objectif de la surveillance* [commercial ? sécurité ?]. *En grande partie parce que ces technologies sont vendues à des sociétés privées qui les déploient dans des espaces privés. »*

420 000 caméras à Londres

Comment un pays réputé pour son absence de carte d'identité peut-il être à ce point en pointe ? L'énorme réseau de caméras de vidéosurveillance déjà existant (les « CCTV ») aide considérablement au déploiement de la nouvelle technologie. Londres en compte ainsi 420 000 dans le métro, les écoles, les supermarchés, les entrées d'immeuble… Grâce à elles, la capitale britannique est la ville au monde la plus surveillée après Pékin (470 000 caméras), selon une étude du think tank américain Brookings Institution datant de 2017. *« La reconnaissance faciale est pour l'essentiel une technologie logicielle, elle peut donc être installée sur les caméras existantes. Pour bien fonctionner, elle nécessite cependant une haute qualité d'optique, donc elle est souvent utilisée avec des caméras haut de gamme »,*précise néanmoins Pete Fussey.

Ces caméras ont été déployées massivement à partir des années 1990, notamment pour prévenir les attentats de l'Armée républicaine irlandaise (l'IRA). Le réseau s'est densifié après les attentats de Londres de 2005. *« Il y a une contradiction dans notre pays. D'un côté, nous sommes très fiers de notre état de droit et des libertés publiques, mais, d'un autre côté, nous avons une grande complaisance pour le risque de leur érosion. Il semble qu'aujourd'hui il n'y ait pas d'autre pays, à part la Chine, qui fasse une utilisation aussi inconsidérée de la reconnaissance faciale »,* déplore Silkie Carlo, directrice de Big Brother Watch.

Qu'en pensent les citoyens, pour la plupart dans l'ignorance de ces expériences tous azimuts ? Le seul sondage sérieux, encore que très restreint, date de mai. Il a été mené par le London Policing Ethics Panel (un organe indépendant censé organiser le dialogue entre la police de Londres et ses habitants), auprès d'un panel de 1 092 Londoniens.

Que révèle-t-il ? Un peu plus d'un tiers seulement des personnes interrogées s'inquiètent des expérimentations menées par la police du Grand Londres depuis 2016. Mais la préoccupation monte chez les jeunes (16-24 ans), les habitants*« d'origine asiatique ou noire »*. Et 38 % des jeunes du panel déclarent qu'ils éviteraient de participer à une manifestation si la police y utilisait la reconnaissance faciale. Hannah Couchman, membre de l'association britannique Liberty, en est convaincue : *« Le public est de plus en plus concerné. Le fait que San Francisco, en Californie, aux portes de la Silicon Valley, ait choisi d'interdire l'usage de la reconnaissance faciale est un signal important. »*

Absence de cadre juridique spécifique

Les militants sont d'autant plus inquiets qu'au Royaume-Uni la technologie prospère en l'absence de tout cadre juridique spécifique. Les lois existantes ne sont pas adaptées, estime Daragh Murray, chercheur, comme M. Fussey, au Centre des droits humains de l'université d'Essex. *« Le règlement européen RGPD*[règlement général de protection des données, entré en vigueur en mai 2018]*s'applique au traitement des données privées, comment elles sont stockées ou partagées. Il ne porte pas sur le fait de savoir s'il est approprié ou non d'utiliser la reconnaissance faciale. »*

Donner aux citoyens le droit de ne pas être « flashé » par des caméras biométriques ? La Commission européenne y réfléchit, assurait le *Financial Times,* fin août. C'est illusoire, estime M. Murray : comment s'exclure volontairement d'une expérimentation de reconnaissance faciale, quand elle est pratiquée dans un lieu public comme King's Cross ? A part en évitant le quartier ou en dissimulant systématiquement son visage ? *« Pour que les citoyens soient protégés, la loi ne doit pas viser à leur donner un droit individuel de retrait, mais à encadrer les pratiques des acteurs choisissant de déployer cette technologie »,*explique M. Murray. Liberty et Big Brother Watch prônent une interdiction totale dans les lieux publics.

Encore faudrait-il que les politiques s'en mêlent. Mais, au pays du Brexit, *« les députés n'ont pas le temps pour des débats sérieux à Westminster »,* déplore Silkie Carlo. Certains ont émis des réserves, comme la chef du Parti vert, Caroline Lucas, et le conservateur David Davis. En attendant qu'ils prennent le sujet à bras-le-corps, c'est la justice qui pourrait trancher. Pour la première fois, un cas a été porté devant les tribunaux. Ed Bridges, un résident de Cardiff (Pays de Galles), a déposé plainte en mai contre la police du Pays de Galles du Sud, auprès d'un tribunal local, après avoir été flashé durant une manifestation contre le commerce des armes.

Cécile Ducourtieux (Londres, correspondante)

France

La reconnaissance faciale progresse, sous la pression des industriels et des forces de l'ordre

Le secrétaire d'Etat au numérique, Cédric O, souhaite susciter davantage d'expérimentations. Mais plus d'une dizaine de projets de recherche ont déjà été menés ces dix dernières années.

Par Martin Untersinger Publié le 14 octobre 2019 à 03h27 - Mis à jour le 14 octobre 2019 à 18h29

Temps deLecture 5 min.

Le centre de supervision urbain de la ville de Nice expérimente la reconnaissance faciale, le 15 avril 2016. Sylvestre / MAXPPP

« N'ayons pas de pudeurs de gazelle ! » Le 2 septembre, devant des sénateurs, le ministre de l'intérieur, Christophe Castaner, a la ferme intention de lancer le débat sur la reconnaissance faciale. *« Lors de l'attentat à Lyon* [en mai]*, nous avons identifié l'auteur par le biais de la vidéoprotection. L'événement a eu lieu à 16 h 30, mais il a été interpellé le lendemain, le temps qu'une trentaine d'enquêteurs regardent image par image l'ensemble du réseau pour refaire son parcours. Avec un système d'intelligence artificielle, quinze minutes après on aurait su où il était allé. »*

Comme le ministre de l'intérieur, responsables politiques et forces de l'ordre lorgnent depuis plusieurs années les technologies de reconnaissance faciale. En juin, la mairie de Nice a mené une médiatique expérimentation sur la voie publique. Pour sécuriser les démarches en ligne, le gouvernement teste Alicem, une application mobile comparant des photos prises *« en selfie »* à celles contenues dans les passeports. Non sans polémique.

« J'aimerais expérimenter dans les transports la reconnaissance faciale (…) *au moins pour des personnes condamnées pour faits de terrorisme »,* a encorerécemment réclamé Valérie Pécresse, présidente de la région Ile-de-France. Face à ces tentations, le cadre légal français, s'il n'interdit pas la reconnaissance faciale, est encore très strict. Si bien que Cédric O, le secrétaire d'Etat au numérique, a décidé d'annoncer lundi 14 octobre dans nos colonnes vouloir un comité chargé de susciter davantage d'expérimentations de cette technologie.

Fichier massif de 7 millions de personnes

Dans les interstices laissés par la loi, les utilisations de la reconnaissance faciale aux lourds enjeux de libertés publiques ont pourtant progressé. Les forces de l'ordre peuvent d'ores et déjà interroger un fichier de police à l'aide d'une photo, pour retrouver l'identité d'un suspect : le massif fichier des antécédents judiciaires, qui contient les photos de plus de 7 millions de personnes. Et ce en dépit des réserves de la Commission nationale de l'informatique et des libertés (CNIL), qui pointait *« des risques importants pour les libertés individuelles ».*

Les enquêteurs aimeraient étendre cet outil à d'autres fichiers, notamment ceux des personnes recherchées (FPR) et des ressortissants étrangers en France. Techniquement possible, elle ne l'est pas en l'état du droit : l'utilisation de la reconnaissance faciale est explicitement prohibée dans ces deux fichiers, comme pour beaucoup d'autres.

Les forces de l'ordre peuvent aussi rechercher un suspect sur les données des caméras de vidéosurveillance saisies dans le cadre d'une enquête judiciaire. De nombreuses entreprises proposent ces services. Par exemple la société Brainchip, qui a travaillé avec la police de Toulouse. Sa technologie, capable de faire de la*« biométrie à la volée »* se branche, en différé, sur les images collectées par vidéosurveillance.

Par ailleurs, selon un décompte du *Monde*, plus d'une dizaine de projets de recherche ont été menés ces dix dernières années, souvent sur fonds publics et en partenariat avec des services de police ou de gendarmerie, pour entraîner les algorithmes et adapter la reconnaissance faciale aux besoins des forces de l'ordre.

Enregistrer la biométrie faciale des passants

Exemple parmi d'autres, le projet Kivaou, financé par l'Agence nationale de la recherche et piloté par Sagem (désormais Safran) et le ministère de l'intérieur, a été conçu pour mettre au point un *« outil de surveillance embarqué permettant d'indexer au fil de l'eau tous les passants et d'enregistrer leur biométrie faciale »*. Selon nos informations, des enquêteurs ont parfois profité de ces expérimentations pour faire progresser leurs investigations.

Les projets se multiplient aussi dans le privé, comme celui lancé par Thales et autorisé par la CNIL en 2016, consistant à tester auprès de volontaires l'identification en temps réel par la vidéosurveillance. Groupe ADP (ex-Aéroports de Paris) a lui aussi mené en 2017 une expérimentation dans l'un de ses terminaux afin d'évaluer la technologie : des salariés volontaires passaient devant des caméras chargées de les reconnaître. Très en pointe sur la question, l'entreprise s'apprête à réaliser une nouvelle expérimentation, pour le contrôle de l'embarquement, au début de l'année 2020.

La question d'un assouplissement du cadre légal se pose en réalité depuis des années. Plusieurs propositions de loi et d'amendement ont été avancées afin de pouvoir relier vidéosurveillance et fichiers policiers par le biais de la reconnaissance faciale, afin de repérer des personnes dans la foule. Interrogé sur ce point en 2016, Bernard Cazeneuve, alors ministre de l'intérieur, avait clairement laissé entendre qu'il travaillait en ce sens. Un projet demeuré lettre morte et une déclaration passée inaperçue. Celui-ci n'a pas souhaité répondre à nos questions.

La technique a progressé et le débat de la régulation se pose à nouveau. La Commission européenne est censée proposer un texte sur l'intelligence artificielle lors des cent premiers jours de son mandat. A cette heure, l'inclusion de la reconnaissance faciale n'est pas tranchée. Certains font des Jeux olympiques (JO) de Paris, en 2024, un objectif. *« Les industriels mettent la pression »,* souffle un bon connaisseur du dossier. Aucune décision n'a été prise à ce stade, mais les expérimentations menées aux JO de Tokyo en matière de reconnaissance faciale seront observées par la Coordination nationale pour la sécurité des Jeux olympiques.

Consensus pour améliorer la technologie

Reste un problème de taille pour ceux qui souhaitent la généralisation de la reconnaissance faciale : si certaines formes de cette technologie sont fiables, d'autres le sont moins. Ainsi, au Royaume-Uni, le bilan de certaines expérimentations est catastrophique.

Il y a donc consensus pour améliorer la technologie. *« Il faut avoir un taux d'efficience de 80 %. On n'y est pas encore. Il faut faire plus d'expérimentations »,*juge un gendarme bien informé. C'est aussi l'avis de Didier Baichère, vice-président de l'Office parlementaire des choix scientifiques et technologiques (Opecst), qui a récemment publié ses travaux sur le sujet.

Il plaide pour que le gouvernement lance une concertation, débouchant sur un rapport dont l'Opecst se chargerait de tirer les conclusions législatives. Les forces de l'ordre tiennent en tout cas à ce nouvel outil. *« La plus-value policière de cette technologie ne fait aucun doute »,* peut-on lire dans une récente note du Centre de recherche de l'école des officiers de la gendarmerie. Selon son auteur, elle pourrait même *« mettre fin à des années de polémiques sur le contrôle au faciès, puisque le contrôle d'identité serait permanent et général »*.