IA : espoirs et déboires de la reconnaissance faciale

Déverrouillage du smartphone, surveillance de foules, vérification de l'identité : la reconnaissance faciale trouve de plus en plus d'applications. Un outil très performant, parfois très amusant, mais qui suscite aussi des inquiétudes.

Avant de choisir la couleur de leur rouge à lèvres, les clients d'Amazon pourront bientôt l'essayer virtuellement. Cela grâce à la reconnaissance faciale développée par ModiFace, start-up propriété de L'Oréal. « Les consommateurs pourront tester des milliers de rouges à lèvres disponibles sur Amazon et acheter les teintes qui leur vont le mieux », indique Parham Aarabi, PDG de ModiFace, dans un communiqué paru la semaine dernière.

Après son acquisition l'année dernière, le grand groupe français lançait avec la jeune pousse américaine l'application Style My Hair, pour tester des nuances de blond ou de brun sur ses cheveux par le truchement d'un smartphone. Les adolescents sont familiers de ces outils, ces « filtres ». Sur le réseau social Snapchat, ils permettent de se grimer sur un écran en renne, en clown ou en cochon.

C'est drôle, mais d'autres usages ne font pas rire tout le monde : la mairie de San Francisco a décidé le 14 mai d'interdire l'utilisation de la reconnaissance faciale par la police et les services municipaux. « La propension de la technologie de reconnaissance faciale à mettre en danger les libertés civiles surpasse substantiellement ses bénéfices supposés », selon le texte .

Car ces systèmes ne se contentent pas seulement de détecter des visages. L'image prise par la caméra est analysée pour distinguer et mesurer les éléments de la tête. En comparant les informations recueillies dans une base de données, on peut surtout identifier la personne photographiée. Cette technologie de biométrie s'est grandement développée ces dernières années à la faveur de l'explosion de l'intelligence artificielle (IA).

Un mouvement mené par l'amélioration des capteurs, et surtout des algorithmes de traitement des images, principalement les réseaux de neurones artificiels. Avec une précision telle qu'elle permet de remplacer les empreintes digitales pour l'authentification de l'utilisateur dans les dernières générations de smartphones.

La reconnaissance faciale a été notamment utilisée par les polices anglaises et américaines pour retrouver des enfants disparus dans des bases de données d'images pédopornographiques. En Inde, ce sont plus de 3.000 enfants, fugueurs ou enlevés, recueillis dans des institutions qui ont ainsi été identifiés par l'association Bachpan Bachao Andolan.

Les voyageurs qui prennent le train pour Londres depuis la gare du Nord, ou qui embarquent à Roissy-Charles-de-Gaulle, auront aussi constaté la présence de nouveaux portiques de sécurité. Ils ont pour mission de vérifier les identités des passagers lors du passage de la frontière. Chez Aéroports de Paris (ADP), c'est l'entreprise Gemalto, récemment acquise par Thales, qui a conçu le programme informatique Parafe (Passage automatisé rapide aux frontières extérieures) avec le ministère de l'Intérieur.

Les téléspectateurs se souviendront pourtant que les portiques Parafe avaient lamentablement échoué aux tests d'un « Cash Investigation » en 2015. C'était alors Safran qui avait élaboré le système, mais pour les empreintes digitales. Depuis l'été 2018, la reconnaissance faciale est donc utilisée à la place par Gemalto.

L'entreprise espère que sa collaboration avec ADP ne va pas s'arrêter aux frontières, et souhaite la mettre en place « du moment de son enregistrement pour son vol jusqu'au moment où on embarque », explique Raphaël de Cormis, directeur de l'Innovation Labs. L'idée est de « fluidifier le déplacement en évitant de redemander à chaque fois des éléments d'identité grâce à la reconnaissance faciale ».

Depuis, les logiciels de reconnaissance faciale se sont perfectionnés dans leur ensemble : « L'algorithme le plus performant en juin 2018 se trompe vingt fois moins que le meilleur système de 2013 », selon un rapport du NIST (National Institute of Standards and Technology), une agence du département du Commerce américain. Les champions VisionLabs et Yitu arrivent aujourd'hui à un taux d'erreur (le système identifie une personne comme une autre) en dessous de 0,5 %. Ceux des logiciels de Gemalto sont inférieurs à 1 %.

Mais il y a de grandes disparités entre les systèmes : « Beaucoup d'algorithmes ne sont pas près d'arriver [aux meilleures performances actuelles] », note le NIST. Sans compter qu'ils sont souvent moins performants avec des personnes noires et des femmes, des individus qui sont donc davantage susceptibles de subir des contrôles de vérification (lire l’encadré).

Bientôt dans des lycées

Cela n'empêche pas le lycée Ampère de Marseille et le lycée Les Eucalyptus à Nice de vouloir lancer une expérimentation à la rentrée, avec le groupe américain Cisco. Les élèves seront munis d'un QR Code sur leur smartphone ou d'un badge qu'ils devront passer sur une borne, puis la reconnaissance faciale validera leur identité. L'objectif est de fluidifier la circulation, mais il n'est pas sûr qu'en heure de pointe le logiciel puisse fonctionner ; les autres lycées ouvrent généralement les portes en grand à ces moments-là.

L'initiative n'est pas sans susciter quelques questions, notamment sur l'étendue de la surveillance. Gaetan Feige, responsable innovation de Cisco France, répond avec une certaine ambiguïté à nos confrères du « Parisien » que son entreprise a mis au point « un système […] qui permet de suivre les déplacements de personnes sans savoir vraiment qui sont les personnes […] afin de s'assurer que les personnes identifiées à l'entrée de l'établissement ont bien le droit d'aller là où elles vont dans l'établissement ». Toutefois, comme le prévoit le règlement européen sur la protection des données, seuls les lycéens consentants pourront participer.

Plusieurs associations (La Quadrature du Net, Ligue des droits de l'homme, CGT Educ'action et FCPE) ont déposé un recours pour stopper cette expérimentation. « On comprend que tout ça vise à forcer les lycéens à donner leur consentement », selon Arthur Messaud, juriste à La Quadrature du Net. Des développeurs se demandent eux-mêmes quelle serait la pertinence d'un « dispositif anti-intrusion », pour reprendre les mots du président de région Renaud Muselier, qui fonctionnerait seulement avec des personnes consentantes. « Le problème de la reconnaissance faciale, c'est que si elle devait se généraliser, elle pourrait permettre de reconnaître toute la population n'importe où, n'importe quand », s'inquiète Arthur Messaud. La crainte du modèle chinois n'est pas loin : le pays utilise actuellement la technologie pour afficher publiquement le visage des personnes qui traversent la rue quand le feu est rouge, ou pour le fichage ethnique et l'oppression de la minorité ouïgoure .

L'avis de la CNIL , non contraignant, est favorable aux expérimentations de Marseille et de Nice. Elle tient à se montrer rassurante sur les conditions des autres utilisations potentielles : « Quand le traitement des données est à des fins sécuritaires dans l'espace public, la base légale, c'est à minima le décret en Conseil d'Etat ou la loi », explique Gwendal Le Grand, directeur des technologies et de l'innovation à la CNIL. Elle avait été consultée en urgence sur une expérimentation qui a eu lieu lors du carnaval de Nice , cet hiver, et assure qu'il y avait des files différentes proposées aux participants, selon qu'ils souhaitaient ou non que leur image soit traitée par l'IA.

Néanmoins, la CNIL a appelé en septembre à un débat démocratique sur les nouveaux usages de la vidéo - un appel resté lettre morte jusqu'à présent. « Le cadre juridique sur la vidéo est un peu ancien, il a été conçu à une époque où le traitement automatique d'images n'existait pas », remarque Gwendal Le Grand. La reconnaissance faciale n'a pas fini d'interroger, et c'est peut-être le contraire qui serait inquiétant, pas la technologie en elle-même.

La reconnaissance faciale biaisée

Les systèmes de reconnaissance faciale sont tributaires des données sur lesquelles ils sont entraînés. Or, il y a souvent moins de femmes et de personnes à la peau sombre dans les bases de données. L'année dernière, la chercheuse Joy Buolamwini a montré que les systèmes se trompaient dans près de 30 % des cas pour identifier le sexe d'une femme noire, contre moins de 1 % pour un homme blanc. IBM a publié depuis une base de données diversifiée pour réduire les biais, mais ils persistent même dans des outils réputés. L'écart en faux positifs (prendre deux individus différents pour la même personne) peut être de 0,2 % entre une femme noire et un homme blanc, d'après le NIST. Ce qui n'a l'air de rien, mais représente une marge importante sur 100.000 personnes. Une erreur qui risque d'entraîner des discriminations lors des contrôles d'identité. 28 membres du Congrès américain, souvent « de couleur », avaient ainsi été confondus comme des criminels par le logiciel d'Amazon, Rekognition, dans une expérience de l'Union américaine pour les libertés civiles. Les actionnaires d'Amazon ont néanmoins décidé, fin mai, de poursuivre la commercialisation de l'outil auprès des autorités.

Source	https://www.journaldunet.com/solutions/reseau-social-d-entreprise/1418978-debat-sur-les-armes-autonomes-la-liste-des-arguments-pour-et-contre/
Auteur	Remy Demichelis Les Echos
Date	12/06/2019