La reconnaissance faciale

Source
Futura
Benoît Lefèvre
11 octobre 2018

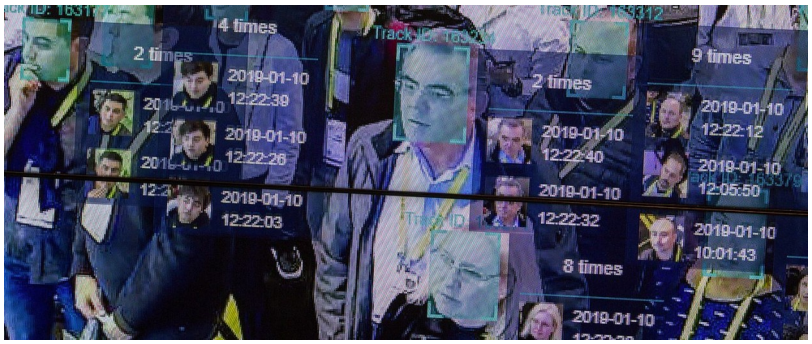
Benoît Lefèvre est cadre dirigeant dans un grand groupe industriel dans les domaines commerce et marketing. Passionné de notre monde contemporain, il a créé le site Étonnante époque.

Faut-il avoir peur de la reconnaissance faciale, une technique qui se perfectionne et qui fonctionne désormais à grande échelle ? Oui, nous dit Benoît Lefèvre, un commentateur attentif des avancées du numérique, qui détaille les réalisations en développement dans le monde.

Shenzhen Chine, prospère voisine de Hong Kong. Chen vient de traverser la rue au rouge. Il est repéré par une caméra de vidéosurveillance équipée d'un logiciel de reconnaissance faciale de la start-up chinoise SenseTime. Son nom apparaît immédiatement sur des écrans géants, jeté en pâture à la vindicte populaire. Il y restera jusqu'à ce qu'il se soit acquitté de son amende. Je vous propose une plongée dans l'univers glaçant des technologies de reconnaissance faciale.

Roissy Aéroport. J'ai hâte de rentrer à la maison après un long voyage. Il y a malheureusement 45 minutes d'attente pour franchir le contrôle des passeports. Je peste contre notre pays archaïque. Mais cela, c'était avant. Depuis début juin, vingt portails de reconnaissance faciale ont été installés à Roissy. L'opération est simple : avant le sas, vous posez la photo de votre passeport sur un lecteur. Vous avancez ensuite dans le sas qui scanne votre visage et le compare à celui du passeport grâce à son système de reconnaissance faciale. Quinze secondes après, le tour est joué. Vous pouvez passer.

La reconnaissance faciale permettra suivant le même principe de faciliter de nombreuses opérations du quotidien. Adieu la carte de crédit pour retirer de l'argent au distributeur. Il reconnaîtra votre visage. Adieu le code pour allumer votre téléphone. Il reconnaîtra son maître... Adieu le badge pour rentrer dans votre entreprise, que vous perdez régulièrement... Et puis en vous reconnaissant, on peut vous proposer instantanément des publicités sur mesure. En Chine, où l'on ne s'embarrasse pas trop avec la protection des données personnelles, toutes ces applications font déjà partie de la vie quotidienne.



L'intelligence artificielle révolutionne la reconnaissance faciale

Nous sommes déjà familiers depuis plusieurs années avec les technologies de reconnaissance faciale. Je me souviens m'être bien amusé avec le logiciel de photos Picasa qui repérait les principaux visages et permettait de regrouper facilement les photos en fonction des personnes présentes. C'est aujourd'hui de la préhistoire et, d'ailleurs Picasa a disparu, devenant Google Photos.

Les technologies d'intelligence artificielle et de *deep learning* sont arrivées. Elles permettent de

changer les voix et les visages sur une vidéo. Vous ne serez donc pas surpris qu'elles permettent également une amélioration sans précédent des technologies de reconnaissance faciale. Jusqu'à présent, la reconnaissance faciale fonctionnait bien avec des visages statiques. Avec l'intelligence artificielle, les caméras reconnaissent aussi des individus en mouvement, en train de marcher ou au volant de leur véhicule, sur des vidéos comme sur des photos.

Les Chinois sont à la pointe dans ce domaine. En avril dernier, la jeune start-up chinoise SenseTime annonçait une levée de fonds de 600 millions de dollars (521 millions d'euros) devenant ainsi l'entreprise d'intelligence artificielle la plus valorisée au monde. Elle a récidivé cet été avec l'annonce de l'injection d'un milliard de dollars par le japonais Softbank.

La Chine a équipé massivement ses rues de 170 millions de caméras de vidéo-surveillance. Elle compte tripler ce chiffre dans les cinq ans à venir. L'État chinois dispose d'une base de données complète de photos des citoyens chinois. Restait le chaînon manquant permettant de connecter à grande échelle ces caméras et cette base de données. C'est ce à quoi travaille SenseTime avec ses logiciels rendant les caméras intelligentes et ses solutions big data pour traiter la masse de données générées par les caméras.

La surveillance des citoyens se généralise dans le monde

Ce système de surveillance de masse se développe en Chine suivant le même modèle que les systèmes de notation sociale à travers une collaboration entre l'État chinois et des entreprises privées. Étonnante alliance entre le parti communiste chinois et des entreprises qui ressemblent aux start-ups de la Silicon Valley...

Tout cela n'est donc plus de la science-fiction. Mais, dira-t-on peut-être, la Chine n'est pas la France et cela n'arrivera pas chez nous en Occident. Pas si simple. Nos rues sont déjà équipées de caméras de vidéo-surveillance et la menace terroriste renforce la demande de sécurité.

Aux États-Unis, les GAFA s'activent sur ce sujet. Amazon commercialise Amazon Rekognition, son logiciel de reconnaissance faciale s'appuyant sur l'intelligence artificielle. Ses fonctionnalités ressemblent à s'y méprendre à celles des logiciels de SenseTime. Ce logiciel suscite la controverse aux États-Unis. La puissante association ACLU (*American Civil Liberties Union*) dénonce les risques de dérive dans l'utilisation par les polices locales d'Amazon Rekognition.

Au mois de juillet, Brad Smith, le président et directeur des affaires juridiques de Microsoft, mettait en garde dans un long article sur les risques de dérive des systèmes de reconnaissance faciale. Il alertait notamment sur les énormes problèmes qu'elles posent pour la liberté individuelle et appelait solennellement l'État américain à légiférer de manière urgente sur le sujet. En France, l'utilisation de la reconnaissance faciale pour le compte de l'État nécessite à ce jour d'être autorisée par un décret pris en Conseil d'État, après avis favorable de la Commission nationale de l'informatique et libertés (Cnil).

Les technologies de reconnaissance des visages vont donc nous mettre rapidement devant un choix de société. Nous avons déjà accepté sans broncher que nos smartphones nous tracent. Abandonnerons-nous un nouveau pan complet de notre liberté individuelle contre un supplément de confort au quotidien et plus de sécurité collective ? L'Europe semble condamnée à subir ce choix tant la maîtrise technologique lui a échappé. Affaire à suivre. Le débat ne fait que commencer.

1. Peut-on faire confiance à la reconnaissance faciale ?

Source
lefigaro.fr
Victoria Castro
20 juillet 2018

Depuis quelques mois, des caméras de surveillance à Londres identifient automatiquement les « personnes recherchées » dans la foule. Leur taux de réussite médiocre relance les débats sur les excès possibles de la reconnaissance faciale, de plus en plus utilisée.

Début juillet, l'aéroport de Nice a inauguré des portiques de reconnaissance faciale pour faciliter le contrôle des passeports des passagers, peu de temps après une initiative similaire des Aéroports de Paris. Utilisée par la police aux États-Unis, en Grande-Bretagne ou encore en Chine, la reconnaissance faciale s'intègre aussi aux caméras de surveillance pour repérer automatiquement les suspects dans la rue, ou scruter les foules lors d'événements publics.

Le développement rapide de cette technologie a même poussé le président de Microsoft Brad Smith à demander au législateur américain un cadre réglementaire. Au-delà des questions de respect de la vie privée, les algorithmes utilisés sont capables d'erreurs et peuvent être biaisés pour certaines communautés.

A Londres, 98 % d'individus détectés par erreur

Depuis le 28 juin, la police londonienne a commencé à tester un dispositif de reconnaissance faciale dans les espaces publics de la ville, qui compare les visages des passants avec un fichier des personnes recherchées. Or, d'après des données sur l'efficacité du système obtenues lors d'essais préliminaires, 98 % des individus détectés comme « suspects » n'auraient rien à se reprocher. Un tel taux de faux positifs n'a rien d'inhabituel. Au Pays de Galles, les gardiens de la paix avaient scanné les visages de 170.000 supporters de football venus assister à la finale de la Champions League 2017. Sur les 2.470 personnes identifiées comme délinquants potentiels se trouvaient 2.297 individus absents de la liste des suspects, soit 92 % de faux positifs.

« Je suis complètement à l'aise [avec l'utilisation de cette technologie] et nous allons poursuivre son expérimentation », a déclaré la commissaire Cressida Dick début juillet, malgré ces mauvais chiffres. Des officiers humains font en effet le tri parmi les personnes détectées par les machines. Les essais à Londres sont encore trop limités pour avoir conduit à des arrestations. De leur côté, les forces de l'ordre du pays de Galles ont arrêté 450 individus en neuf mois avec l'aide de cette technologie, dont aucun détecté par erreur.

Difficulté du mouvement

La reconnaissance d'images ou de visages fonctionne assez bien dans des conditions statiques et à faible distance de la caméra, quand l'on regarde son smartphone pour le déverrouiller par exemple. C'est ce cas dans les aéroports, où des bornes scannent les visages des passagers pour les comparer avec les photos de leurs passeports biométriques. Dès que les individus bougent ou se trouvent à distance dans une foule, le résultat est bien plus aléatoire. Dans un autre contexte, des chercheurs de l'université de Jérusalem avaient entraîné un algorithme à reconnaître différents animaux en leur en montrant des images fixes (par exemple, un ours polaire). Mais quand ils lui font visionner un ours polaire en vidéo, l'algorithme y voit successivement un babouin ou une belette.

Le problème n'est pas seulement technique ; il est aussi éthique. En Chine, la reconnaissance faciale est déployée à grande échelle à des fins de surveillance, mais aucun chiffre ne filtre sur l'efficacité réelle de ces systèmes. D'après le *New York Times*, les lunettes à reconnaissance faciale dont dispose aujourd'hui la police chinoise ne fonctionnent que si la personne ciblée se tient immobile pendant plusieurs secondes. Ces technologies sont donc essentiellement dissuasives. « L'idée est que si les gens craignent d'être surveillés, ils seront plus obéissants », résume Martin Chorzempa de l'institut Peterson, dans une interview accordée au *New York Times.*

Introduction de biais

Parmi les autres inquiétudes, celles des biais des algorithmes de reconnaissance. Parce qu'ils sont majoritairement entraînés sur des photos d'hommes de type caucasien, les erreurs de reconnaissance sont bien plus importantes chez les femmes et les minorités raciales. Une étude de février 2018, basée sur les algorithmes de Microsoft et d'IBM, avait trouvé un taux d'erreur quasi nul pour des hommes blancs, mais de 21 à 35 % pour des femmes noires. La crainte est que la technologie vienne renforcer les discriminations policières.

En France, l'utilisation de la reconnaissance faciale pour le compte de l'État nécessite d'être autorisée par un décret pris en Conseil d'État, après avis favorable de la Commission nationale de l'informatique et libertés (CNIL). Cette dernière n'a pour l'instant validé la technologie qu'aux aéroports de Paris et de Nice, ainsi qu'à l'entrée de l'Eurostar. Des « caméras intelligentes » sont installées dans le métro parisien depuis octobre 2017, mais celles-ci ne reconnaissent pas les visages et se contentent d'alerter la police en cas d'activité suspecte ou tapageuse.

Source
Slate.fr
Aaron Mak
15 février 2019

2. Se servir de la reconnaissance faciale lors d'un procès, une délicate question éthique

En 2015, des agents infiltrés travaillant avec le bureau du shérif de Jacksonville photographièrent un homme en train de vendre pour cinquante dollars de cocaïne. Les enquêteurs étant incapables de l'identifier, ils décidèrent de se tourner vers un système de reconnaissance faciale baptisé FACES (*Face Analysis Comparison Examination System*), qui s'appuie sur une base de données constituée par plus de trente-trois millions de photos de permis de conduire et de photographies judiciaires. Conçu pour renvoyer plusieurs correspondances potentielles pour une image donnée, il désigna

Willie Allen Lynch et quatre autres suspects. Après enquête, les inspecteurs arrêtèrent Lynch pour le crime en question et il fut finalement condamné à huit ans de prison.

Un usage mal encadré et caché

La Floride a commencé à mettre en place son système de reconnaissance faciale en 2001, soit longtemps avant la plupart des autres États américains. Et aujourd'hui, en Floride, les autorités effectuent chaque mois environ 8.000 recherches *via* FACES, soit presque deux fois la moyenne des unités de reconnaissance faciale du FBI. Le *Center on Privacy 9 Technology* (centre sur la vie privée et la technologie) de Georgetown a révélé dans un rapport publié en 2016 que le logiciel n'avait pas fait l'objet d'une vérification pour éviter les erreurs ou les mauvaises utilisations. En outre, le bureau du shérif de Jacksonville a également déclaré qu'il n'avait aucune politique officielle concernant FACES.

« *La Floride possède le système de reconnaissance faciale le plus avancé de tous les États-Unis. C'est celui qui fonctionne depuis le plus longtemps et qui donne les meilleurs résultats* », affirme Jennifer Lynch (aucun lien de parenté avec le prévenu), responsable du service surveillance-litiges de l'Electronic Frontier Foundation. Ce sont même les forces de l'ordre de l'État de Floride qui ont conseillé le FBI lorsque ce dernier a mis en place son propre système de reconnaissance faciale. Jennifer Lynch ajoute : « *Il n'est pas surprenant que la Floride soit le premier État où une affaire comme celle-ci puisse être portée en appel. Il est très probable qu'il y aura d'autres cas de ce genre à l'avenir.* » En dépit de la prolifération de la technologie dans l'État, les avocats locaux de l'assistance judiciaire ont expliqué aux chercheurs de Georgetown que la police n'avait jamais divulgué d'informations sur les utilisations spécifiques du système dans des affaires pénales.

Et, en effet, dans le rapport de police relatif à l'arrestation de Willie Allen Lynch, les autorités n'ont pas écrit qu'elles avaient consulté FACES. Le prévenu n'a même appris l'existence de la technologie en question que des mois après avoir cherché personnellement à faire témoigner les inspecteurs et la criminologue impliquées. Au cours d'une déposition préalable au procès, la criminologue qui avait soumis la photographie du dealer à FACES a aussi expliqué que le logiciel note la qualité de la correspondance à l'aide d'un système d'étoiles. Elle avait remarqué qu'il n'avait attribué qu'une seule étoile à Lynch, mais que les autres correspondances potentielles n'en avaient reçu aucune. Elle ne connaissait pas le nombre maximum d'étoiles qu'il était possible d'obtenir.

Plusieurs failles dans le système

Au cours de son procès, Lynch a affirmé qu'il avait été mal identifié. Toutefois, le tribunal a rejeté sa demande d'avoir accès aux photographies des autres personnes identifiées par FACES comme des correspondances possibles, pour la simple raison que les inspecteurs ne les avaient pas vues non plus. L'un des principaux arguments de l'appel de Lynch était que l'État était allé à l'encontre du précédent juridique établi par la Cour suprême dans l'affaire Brady contre Maryland, qui indique que les procureurs doivent remettre à la défense des preuves potentiellement à décharge. « *Si l'une ou l'autre des photographies des autres correspondances potentielles établies par le programme de reconnaissance faciale ressemble au vendeur de drogue ou au prévenu, il y a clairement eu violation du précédent Brady contre Maryland et le prévenu devrait avoir droit à un nouveau procès* », a écrit l'avocat de Lynch dans sa requête pour une nouvelle audition. (Le bureau du shérif de Jacksonville a déclaré publiquement que les inspecteurs n'utilisent FACES que conjointement avec d'autres outils d'enquête. Dans le cas présent, les enquêteurs se sont également appuyés sur le récit d'un témoin oculaire –contesté par la défense– ainsi que sur le casier judiciaire de Lynch pour l'accuser).

Jake Laperruque, avocat principal du Constitution Project travaillant sur la reconnaissance faciale et la vie privée, souligne que les photographies d'autres correspondances FACES ne sont pas les seules potentiellement à décharge dans ce scénario. Des facteurs tels que la qualité des algorithmes, les seuils de confiance et le format de retour des correspondances peuvent tous affecter la précision de la technologie. Compte tenu de ces problèmes, beaucoup soutiennent que, conformément à la jurisprudence Brady, la police devrait être tenue de révéler lorsqu'un logiciel de reconnaissance faciale a été utilisé.

« *Sans savoir que la reconnaissance faciale a été employée et sans en connaître les détails, il est impossible pour les accusés de savoir si l'usage qui en a été fait dans le cadre de l'enquête était approprié*, explique Laperruque. *C'est comme si une enquête de police reposait sur le récit d'un témoin oculaire, mais qu'on ne le disait pas à l'accusé ou qu'on ne lui précisait pas s'il se trouvait à deux mètres ou à deux cents lorsqu'il a vu la scène.* »

Le fait que Lynch soit noir soulève également des questions quant à l'exactitude de FACES dans

ce cas précis, car les logiciels de reconnaissance faciale sont réputés avoir du mal à identifier les personnes de couleur. Les chercheurs du MIT ont publié l'an dernier une étude qui mettait à l'essai trois des systèmes de reconnaissance faciale les plus avancés qui soient. Ils ont constaté que les taux d'erreur étaient d'environ 1 % pour les hommes à peau claire, 12 % pour les hommes à peau foncée et 35 % pour les femmes à peau foncée.

Ce mois-ci, cependant, la Cour d'appel du 1er District a confirmé la condamnation de Lynch au motif qu'il ne pouvait pas prouver que les autres photos de la base de données lui ressemblaient, même si ni Lynch, ni son avocat en appel, Victor Holder, n'ont pu avoir accès à ces photos. Sans elles, ils n'ont pas pu soutenir que l'issue du procès aurait pu être différente. La cour a également noté que le jury avait eu l'occasion de comparer les photos de Lynch avec celles du dealer.

« De vives inquiétudes quant aux droits de l'homme »

Victor Holder a déclaré au Florida Times Union qu'il envisageait d'autres possibilités pour faire appel. « *Les autorités policières de Floride se servent actuellement d'un système de reconnaissance faciale alors que la population est peu (voire pas du tout) au courant qu'aucune norme uniforme ne régit son utilisation et qu'il n'y a aucune surveillance publique par le corps législatif de Floride* », affirme-t-il.

Plus de sensibilisation et de transparence au sujet de la reconnaissance faciale augmenterait les interrogations à propos de cette technologie dans les salles d'audience. «*En général, lorsque l'on a recours à la reconnaissance faciale comme point de départ d'une enquête, on risque de voir se soulever des interrogations lors du procès quant à la fiabilité du système*, explique Jake Laperruque. *Quand les policiers utilisent des empreintes digitales lors de leur enquête (même s'il ne s'agit pas d'une preuve irréfutable), si c'est l'élément qui les a poussés à déclarer la personne suspecte ou à aller fouiller sa maison, l'avocat de la défense va immanquablement interroger l'expert en empreintes digitales sur ses méthodes et ses compétences*.»

Pour Sarah St. Vincent, chercheuse et avocate de Human Rights Watch, l'affaire de Willie Allen Lynch soulève également des questions sur l'utilisation apparemment systématique des technologies de reconnaissance faciale par les services de police. « *Avoir recours à un logiciel de surveillance puissant, de reconnaissance faciale, pour une affaire de vente de drogue d'une valeur de cinquante dollars, soulève de vives inquiétudes quant aux droits de l'homme*, dit-elle. *Si le gouvernement considère pouvoir recourir à des méthodes de surveillance pouvant empiéter sur les droits fondamentaux avec autant d'efficacité que la reconnaissance faciale, il ne devrait l'envisager que dans des cas d'une gravité extrême*. » (La police a eu des occasions plus importantes d'utiliser cette technologie, comme l'année dernière, quand elle s'est servie du logiciel de reconnaissance faciale pour identifier le tireur suspecté de la fusillade dans la salle de rédaction du Capital Gazette, au Maryland.)

Si Lynch n'avait pas pris sur lui de se plonger dans les dépositions et de déposer des requêtes manuscrites dans son affaire, il n'aurait peut-être jamais appris le rôle joué par FACES dans son arrestation. Le fait que les autorités policières ne signalent pas ces cas pourrait bien empêcher le système juridique américain d'examiner aussi ces questions. « *Nous devons au moins savoir quand le système de reconnaissance faciale est utilisé afin que les tribunaux, les avocats de la défense et les procureurs puissent discuter conjointement de la question*, affirme Sarah St. Vincent. *Je ne suis pas certaine qu'aujourd'hui, l'utilisation de cette technologie soit habituellement dévoilée.* »

Source
L'Usine Digitale
Aude Chardenon
14 août 2019

3. Des législateurs américains identifiés comme criminels par la technologie de reconnaissance faciale d'Amazon

Une petite trentaine de membres de l'Assemblée de l'Etat de Californie ont été identifiés à tort comme délinquants par la technologie de reconnaissance d'Amazon. L'American Civil Liberties Union espère que les conclusions de ce test l'aideront à faire interdire l'usage de ces dispositifs par la police.

Les partisans de l'usage des technologies de reconnaissance faciale en matière de sécurité n'ont qu'à bien se tenir. Aux Etats-Unis, l'American Civil Liberties Union (ACLU) a révélé mardi 13 août 2019 lors d'une conférence de presse que 26 membres de l'Assemblée de l'Etat de Californie ont été identifiés à tort comme des personnes délinquantes lors d'un test qu'elle a orchestré.

Trop de faux positifs

Le test consistait à comparer les visages de 120 législateurs à ceux d'une base de données de 25'000 clichés de délinquants à l'aide du logiciel de reconnaissance faciale d'Amazon, Rekognition. Plus d'une personne sur cinq a donc été identifiée à tort comme un individu figurant dans la base de données... et donc ayant un casier judiciaire, explique le Los Angeles Times.

Pour Phil Ting, membre de l'Assemblée de San Francisco faisant partie de l'échantillon concerné, cette expérience « confirme que la technologie de reconnaissance faciale n'est pas prête à être déployée et encore moins pour une utilisation avec des caméras équipant les forces de l'ordre ». Autre élément clé : plus de la moitié des personnes identifiées de façon erronée étaient des personnes de couleur.

Un précédent en 2018

La police californienne n'est pas encore dotée de tels dispositifs, mais l'ACLU souhaite interdire par anticipation l'utilisation de la reconnaissance faciale dans les caméras de surveillance des forces de l'ordre. Elle soutient ainsi l'AB 1215, également connu sous le nom de « Body Camera Accountability Act », qui interdit l'utilisation de systèmes de reconnaissance faciale et de surveillance biométrique dans les caméras de police. L'organisme de protection des droits civils outre-Atlantique, soutenu par bon nombre de personnalités démocrates, accuse cette technologie d'être particulièrement préjudiciable aux personnes de couleur, ainsi qu'aux femmes, autres victimes selon eux des erreurs de la technologie.

À terme, les opposants à l'identification par reconnaissance faciale craignent l'augmentation des tensions entre société civile et forces de l'ordre dans un pays où les abus de la police à l'encontre des communautés font régulièrement la une des médias. Pour Matt Cagle, avocat spécialisé dans les technologies et les libertés civiles à l'ACLU, « même si cette technologie était 100% fiable, des caméras corporelles activées par reconnaissance faciale faciliteraient des violations massives des droits civils des Californiens ».

Adopté par l'Assemblée de Californie en mai, le texte doit être voté au Sénat californien dans les prochaines semaines. Le New Hampshire et l'Oregon l'ont adopté en 2017. En 2019, ce sont 28 membres du Congrès qui avaient été identifiés à tort comme des criminels, là encore par Rekognition.

Source
Slate.fr
Claire Levenson
9 septembre 2017

4. Un algorithme peut deviner l'orientation sexuelle de quelqu'un à partir d'une photo

Deux chercheurs en psychologie et informatique à l'université de Stanford ont trouvé qu'un algorithme était capable de déterminer si une personne était homosexuelle à partir d'une simple photo postée sur un site de rencontres.

Dans leur article, bientôt publié dans le *Journal of Personality and Social Psychology*, ils expliquent qu'en analysant deux photos, l'une d'un homme gay et l'autre d'un homme hétérosexuel, leur modèle de prédiction permet de trouver l'homme gay 81 % du temps. Si les chercheurs donnent cinq photos de chaque homme, le modèle a alors raison sur l'orientation sexuelle 91 % du temps. C'est apparemment un peu plus difficile pour les femmes : les prédictions sont exactes 71 % du temps avec une photo, et 83 % avec cinq.

Dans les deux cas, l'intelligence artificielle était beaucoup plus efficace que les êtres humains, qui avaient raison dans 61 % des cas pour les hommes et seulement 54 % des cas pour les femmes. Pour l'étude, plus de 35'000 photos d'hommes et femmes sur des sites de rencontres ont été utilisées.

Les résultats sont moins bons lorsque l'algorithme ne sait pas que l'un des hommes en photo est homosexuel, et l'autre pas. Mais le modèle réussit très bien à sélectionner les personnes les plus susceptibles d'être homosexuelles parmi de nombreuses photos. Les personnes de couleur ne sont pas prises en compte et les autres formes de sexualité n'ont pas été recherchées, précise le Guardian.

Le modèle de prédiction mis en place par les chercheurs Michal Kosinski et Yilun Wang de Stanford fonctionne en deux temps. Tout d'abord, un logiciel qui analyse les détails du visage, et ensuite un autre qui connecte ces détails avec l'orientation sexuelle. En effet, les chercheurs ont trouvé certaines corrélations en analysant un grand nombre de données. Les hommes homosexuels ont tendance à avoir des mâchoires plus étroites, des nez plus longs et des fronts plus grands que les hétéros. Alors que les femmes homosexuelles ont tendance à avoir des mâchoires plus larges et des fronts plus étroits.

«Les visages contiennent beaucoup plus d'information sur l'orientation sexuelle que celle qui sont perçues et interprétées par le cerveau humain», écrivent les auteurs de l'étude.

Selon eux, ces résultats tendent à étayer la théorie selon laquelle l'orientation sexuelle est liée au contact avec certaines hormones avant la naissance. Kosinski et Wang n'ont pas inventé de nouvelle technologie, juste utilisé des logiciels et données déjà disponibles. Leur but n'était pas de créer ce que certains appellent un « gaydar » (une machine qui détecte l'homosexualité) mais de montrer que c'est possible et potentiellement dangereux. En effet, des gouvernements qui ont des lois anti-LGBT pourraient utiliser ces outils sans l'autorisation des individus analysés. Interviewé par le Guardian, le professeur de psychologie Nick Rule explique au sujet de cette technologie :

« Les auteurs ont montré à quel point c'est puissant. Maintenant, nous savons qu'il nous faut des protections. »

Dans un monde où certains pays condamnent encore l'homosexualité, la possibilité d'une telle étude est effrayante, et pose des questions éthiques et de vie privée.

Source
Slate.fr
Léa Polverini
26 avril 2018

5. La police indienne identifie près de 3000 enfants disparus grâce à la reconnaissance faciale

Il aura fallu seulement quatre jours à la police de New Delhi pour identifier 2930 enfants disparus. La performance le doit à l'usage de la technologie de reconnaissance faciale.

Le 6 avril, le ministère du Développement des femmes et des enfants annonçait que l'une des hautes cours du pays venait de commander le test d'un logiciel de reconnaissance faciale.

Réaliser un travail manuel impossible

Utilisé sur près de 45'000 enfants de New Delhi, il a donc permis d'en identifier 6,5 % comme étant portés disparus, à partir de la base de données TrackChild mise en place par le ministère, qui regroupe les photos d'enfants disparus et retrouvés et certaines informations mises à disposition par la police.

« *L'Inde compte actuellement presque 200'000 enfants disparus, et autour de 90'000 qui sont hébergés dans diverses institutions de protection de l'enfance. Il est presque impossible pour*

quiconque de parcourir manuellement les photos afin de les faire correspondre à chaque enfant », a déclaré à The Better India Bhuwan Ribhu, le porte-parole de Bachpan Bachao Andolan (BBA), une organisation indienne de protection de l'enfance.

C'est cette organisation qui lancé le développement du logiciel, en travaux depuis près de deux ans. Alors que le projet de poursuivre cette utilisation des technologies de reconnaissance faciale pour identifier d'autres disparus est poussé par la BBA et encouragé par la Commission nationale pour la protection des droits de l'enfant indienne, cela ne va pas sans poser des questions vis-à-vis de la politique de confidentialité.

Il y a une semaine, en Chine, un homme souffrant de maladie mentale ayant disparu depuis plus d'un an avait été retrouvé par sa famille grâce au réseau de surveillance fonctionnant par reconnaissance faciale. Si ce dernier peut permettre de retrouver la trace de disparus, il demeure un outil de contrôle aux potentialités redoutables.

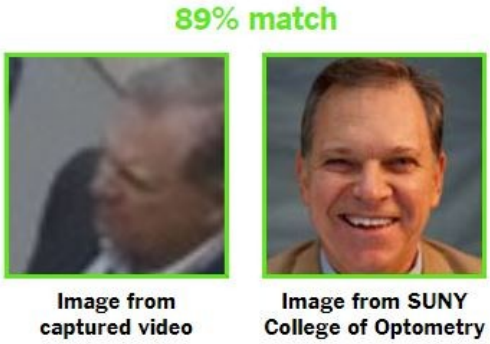
6. Enquête. La reconnaissance faciale, une technologie incroyablement efficace

Source
Courrier international
5 mai 2019

Article original de
Sahil Chinoy dans *The New York Times*
16 avril 2019

Trottoir, route, gare : tous ou presque, nous traversons quotidiennement au moins un espace public. Convaincus, pour la plupart, que l'historique détaillé de nos déplacements et la liste des personnes qui nous accompagnent restent privés. Une confidentialité que la reconnaissance faciale, mise en œuvre sur les réseaux de caméras déjà en place dans la plupart des grandes villes, vient menacer.

Pour démontrer avec quelle facilité on peut suivre des individus à leur insu, nous avons collecté des images publiquement accessibles (le plus souvent sur le site web de leur employeur) de personnes circulant aux abords de Bryant Park, à New York, et fait passer toute une journée d'enregistrement à la moulinette du logiciel de reconnaissance faciale d'Amazon. En neuf heures d'images, nous avons détecté 2750 visages (ce qui ne signifie pas 2 750 personnes, un même individu pouvant apparaître sur plusieurs clichés). La reconnaissance faciale a proposé plusieurs identifications possibles, dont une correspondance avec un portrait professionnel de Richard Madonna, professeur à la faculté d'optométrie de l'université d'État de New York (Suny), avec un taux d'exactitude de 89 %. Coût total de l'opération : environ 60 dollars [54 euros].



"Ma première réaction a été : 'Mon dieu, c'est incroyable !' raconte Richard Madonna, que nous avons contacté pour lui décrire notre expérience et son résultat. *Je n'en reviens pas de la facilité avec laquelle j'ai été identifié, parce que bon… on ne voit que le côté de ma tête."*

Pour cette expérience, nous avons constitué une base de données à partir de photos venant exclusivement de sites Internet publics, et avons sollicité l'accord de Richard Madonna avant publication de cet article.

Depuis des décennies, des millions de caméras comme celles que nous avons exploitées ont été installées par des entreprises et des particuliers, qui ont ainsi créé sans le vouloir les infrastructures d'une surveillance de masse. Par le passé, il fallait qu'un être humain regarde les enregistrements et tente d'identifier les individus – impossible donc de fournir un historique exhaustif des mouvements de chacun. Aujourd'hui, la technologie de reconnaissance faciale a atteint une vitesse et une fiabilité qui rendent possible la création d'un redoutable système de surveillance.

La législation ne suit pas

Or la législation, elle, est en retard. Aux États-Unis, l'utilisation de la reconnaissance faciale n'est pour ainsi dire pas encadrée.

"La technologie a progressé plus rapidement que je ne l'aurais jamais imaginé", reconnaît Jennifer Lynch, directrice chargée des litiges liés à la surveillance à l'Electronic Frontier Foundation. Une vitesse telle que la juriste serait aujourd'hui favorable à une interdiction pure et simple de l'usage de la reconnaissance faciale par les pouvoirs publics.

À Bryant Park, par exemple, les caméras ont été installées il y a plus de dix ans afin de permettre aux citadins de voir, en été, si les pelouses étaient accessibles à ceux qui viennent bronzer, ou, en hiver, si la patinoire n'était pas bondée. Selon l'entreprise gestionnaire du parc, cette vidéosurveillance n'a pas la vocation d'un système de sécurité.

Notre expérience vient toutefois montrer qu'avec un accès à quelques caméras et à une technologie de reconnaissance faciale, un seul individu peut pister les habitudes quotidiennes des gens : à quelle heure ils arrivent au travail, avec qui ils prennent un café, s'ils quittent le bureau un peu tôt. Sur les images qui l'identifient, Richard Madonna est en chemin pour aller déjeuner avec un candidat à un poste – c'est dire les informations délicates que peut révéler un historique des sorties déjeuner de citoyens respectueux de la loi.

Les forces de l'ordre et les pouvoirs publics ont eux aussi accès à un vaste réseau de vidéosurveillance. Ajoutez-y une riche base d'images de visages (comme une base de permis de conduire), et il devient possible de pister les gens dans toute une région, en temps réel. Rien ne prouve qu'une telle surveillance soit mise en œuvre, aujourd'hui, aux États-Unis. Mais si ce n'est pas le cas, ce n'est pas parce que la technologie ne le permet pas. L'année dernière, les entreprises du secteur assuraient pouvoir comparer des images en temps réel à une base de données comptant plusieurs milliards de visages.

Risque pour la liberté d'expression

Du côté des forces de l'ordre, on utilise la reconnaissance faciale pour repérer des criminels présumés et retrouver des enfants disparus. Mais les défenseurs des libertés publiques dénoncent le risque de dégradation de la liberté d'expression si les autorités en venaient à pister les déplacements de chacun – par exemple, identifier les participants à une manifestation. Une inquiétude qui ne relève pas de la pure hypothèse : lors des manifestations de 2016 en réaction à la mort de Freddie Gray, victime d'une arrestation brutale par la police de Baltimore, les forces de l'ordre ont utilisé la reconnaissance faciale sur des images postées sur les réseaux sociaux pour identifier les manifestants faisant l'objet d'un mandat d'arrêt. Comme le résume Jennifer Lynch :

"Dès lors que l'État est capable de nous suivre à la trace et de nous identifier partout où nous allons, il devient impossible de parler anonymement ou d'être un acteur anonyme de la société."

New York est bien loin de ce qui se pratique en Chine, où le nombre de caméras de surveillance installées par l'État est de 1 pour 7 habitants. Cependant, selon l'American Civil Liberties Union (Aclu), la police new-yorkaise a tout de même accès, rien que pour Lower Manhattan [un quartier de New York], aux images captées par plus de 9000 caméras.

"Nous comparons les visages filmés par des caméras sur les scènes de crime aux photos des fiches anthropométriques", explique dans un courriel le sergent Jessica McRorie, porte-parole du New York Police Department. "*Nous ne faisons aucune collecte massive ou aléatoire de clichés de visages dans les images fournies par notre réseau de caméras, ni dans celles venues d'Internet ou des réseaux sociaux."*

Les forces de l'ordre utilisent l'outil d'Amazon

Amazon fait partie des entreprises qui commercialisent des services de reconnaissance faciale. L'entreprise met en avant les applications positives de Rekognition, le logiciel que nous avons utilisé, comme le rôle qu'il peut jouer dans la recherche d'enfants disparus. Ses utilisateurs doivent se conformer à la loi et respecter les droits d'autrui, insiste Amazon, cependant critiquée pour promouvoir activement sa technologie auprès des forces de l'ordre.

Rekognition est ainsi utilisé, et activement, par le bureau du shérif du comté de Washington, dans l'Oregon, notamment pour enquêter sur des petits délits comme le vol à l'étalage. La police d'Orlando, en Floride, a également déployé cette technologie dans le cadre d'un programme pilote.

Le logiciel ne prend pas de décision [il n'attribue pas une identité à une personne sur une image] et se contente de fournir des prévisions [et donc un pourcentage de correspondance entre un visage sur une image enregistrée et une personne identifiée sur une autre image], insiste-t-on chez Amazon, et le niveau de confiance affiché doit être croisé avec une intervention humaine. La société recommande ainsi de ne tenir compte que des niveaux de confiance supérieurs à 99 % pour des usages à des fins d'identification ou de sécurité publique. Les détracteurs de la reconnaissance faciale dénoncent l'opacité de la façon dont ces taux sont obtenus et le fait qu'Amazon ne peut concrètement rien faire pour faire appliquer ces recommandations. Aucune des correspondances que nous avons obtenues à partie des vidéos de Bryant Park, justes ou fausses, n'atteignait 99 %.

Matt Wood, directeur général chargé de l'intelligence artificielle chez Amazon Web Services, admet que Rekognition, comme toute information mise à disposition des forces de l'ordre, peut être utilisé à mauvais escient. "*Un service de police l'utilisant doit être tenu de rendre des comptes aux personnes et à la justice s'il enfreint les libertés publiques"*, estime-t-il – même si, ajoute-t-il, Amazon n'a eu vent d'aucun usage abusif de la part des pouvoirs publics.

En janvier pourtant, l'Aclu a envoyé à Amazon une lettre pour lui demander d'arrêter de vendre son logiciel à des services de police et des organismes gouvernementaux, dénonçant par ailleurs son retard, en termes de protection des libertés publiques, par rapport à Google ou Microsoft.

"La documentation marketing de Rekognition a tout du petit guide de surveillance dans un régime autoritaire", résumait Nicole Ozer, chargée des technologies et des libertés civiles pour le compte de la branche californienne de l'Aclu, dans un communiqué daté de l'année dernière.

Aux États-Unis, aucune loi fédérale n'encadre le recours à la reconnaissance faciale. La plupart des États n'ont pas de réglementation non plus (à quelques exceptions près, dont l'Illinois et le Texas), pas plus que la ville de New York, où un conseiller municipal a toutefois proposé, l'année dernière, un arrêté imposant aux entreprises un devoir de transparence sur leur utilisation de ce genre de technologie – une disposition qui s'appliquerait à notre expérimentation, mais pas à l'utilisation de la reconnaissance faciale par les forces de l'ordre. "*C'est un peu le Far West",* lâche Jennifer Lynch, de l'Electronic Frontier Foundation.

Un vide juridique qui est déjà exploité par certains. Selon l'enquête menée par le Center on Privacy and Technology [centre d'études sur la vie privée et les technologies] de la faculté de droit de l'université Georgetown (Washington DC), les services d'un shérif de l'Arizona ont en 2007 entré dans leur base de données tous les permis de conduire et fiches anthropométriques du Honduras ; en Floride, un bureau du shérif effectue 8000 recherches par mois sans que ses agents aient à les justifier par une présomption raisonnable d'infraction.

Le centre d'études de Georgetown, l'Electronic Frontier Foundation et d'autres organismes ont formulé des propositions réglementaires : exiger que les agents des forces de l'ordre aient une présomption raisonnable avant de procéder à une recherche, prohiber, sauf cas de vie ou de mort, la reconnaissance faciale en temps réel à partir des bases de données de type permis de conduire, ou encore interdire les recherches fondées sur l'opinion politique, la couleur de peau ou les croyances religieuses.

Une forme de surveillance inédite

Même Amazon appelle de ses vœux la création d'un cadre juridique imposant l'intervention humaine et la transparence. Mais pour certains, la technologie est en soi si dangereuse qu'aucune loi ne peut efficacement l'encadrer.

"De l'interdiction de la technologie de reconnaissance faciale dépend la prospérité future de l'homme", écrivent sans détour Woodrow Hartzog, professeur de droit et d'informatique à l'université Northeastern, et Evan Selinger, professeur de philosophie au Rochester Institute of Technology. Car la reconnaissance faciale diffère radicalement des autres formes de surveillance, explique Woodrow Hartzog, et elle se révèle infiniment plus dangereuse. Un visage est difficile à cacher et peut être observé à grande distance, contrairement à une empreinte digitale. Il existe déjà des bases de données recensant le nom et le visage de citoyens lambda, par exemple celle des permis de conduire. Et dans une large mesure, la surveillance via la reconnaissance faciale peut être mise en œuvre grâce à des caméras déjà présentes dans nos rues.

Mais peut-être est-il déjà trop tard pour une interdiction, ou même un moratoire. Un peu partout aux États-Unis, des services de police exploitent déjà la reconnaissance faciale, rappelle Clare Garvie, du Center on Privacy and Technology de Georgetown.

"Nous ne pouvons pas cantonner les forces de l'ordre à des technologies du XXe siècle au seul motif que celles du XXIe siècle comportent des risques."

Richard Madonna, l'enseignant que nous avons identifié à Bryant Park, voit très bien la tension qui s'exerce. D'abord étonné quand nous l'avons contacté, il nous a expliqué que lui-même parlait souvent à ses étudiants du rapport bénéfice-risque. Et le professeur entrevoit bien les bénéfices immenses que pourrait apporter la reconnaissance faciale.

Mais c'est aussi une technologie porteuse d'abus potentiels, poursuit-il, puisque des particuliers comme des États peuvent s'en servir pour pister un groupe donné ou n'importe quel individu… et même un homme qui traverserait tranquillement Bryant Park.

Source
Korii
Clément Lasserre
10 juin 2019

7. Pourquoi les États-Unis ont-ils peur de la reconnaissance faciale ?

Alors que la technologie se perfectionne et se généralise, le débat est ouvert outre-Atlantique sur la dangerosité et les conséquences de son utilisation.

Parce qu'elle intègre les écoles

En ce début juin 2019, un district de l'État de New York devait implémenter un système de reconnaissance faciale au sein de huit écoles. Nommé Aegis, ce dispositif est conçu pour repérer des menaces telles qu'une personne portant une arme ou identifier un individu connu de la justice. Aegis promettait également de ne pas suivre les mouvements des élèves et de conserver les enregistrements pendant seulement soixante jours.

Malgré ces précisions, l'association new-yorkaise pour les libertés civiles a protesté contre cet outil et demandé la suspension du projet, arguant que « *San Francisco a interdit cette technologie, alors que cette grande ville est la plus proche de toutes les personnes qui la comprennent le mieux* [une référence à la Silicon Valley, ndlr]. *Pourquoi voudrions-nous qu'elle arrive à New York et dans un endroit où il y a des enfants ? ».*

Le 30 mai dernier, à quelques jours du lancement du programme, le département pour l'éducation de l'État de New York a demandé son report, jugeant que le district n'a pas démontré que « *le cadre nécessaire était en place pour protéger la vie privée des personnes concernées et pour sécuriser correctement les données ».*

Le district a fait savoir qu'il ne suivrait pas cette recommandation et que le test commencerait bien à partir du 3 juin.

Parce que San Francisco l'a interdite

San Francisco, dont la baie abrite les géants de la Silicon Valley et les start-ups du monde des nouvelles technologies, vient de devenir la première ville américaine à bannir l'utilisation de la reconnaissance faciale par les services de police ou les agences gouvernementales. La technologie pourra toujours être exploitée par les commerces, les individus et les services fédéraux, comme l'aéroport de la ville.

La police de San Francisco a mis à l'essai un dispositif de reconnaissance faciale entre 2013 et 2017. Elle s'en servait pour retrouver à la fois des petit·es délinquant·es et des auteurs de tueries de masse.

Cette décision pourrait en appeler d'autres. Dans la même région, Oakland considère une directive similaire. Au niveau national, un projet de loi a été soumis pour interdire l'utilisation commerciale de la reconnaissance faciale et la collecte de données sur les consommateurs et consommatrices.

Parce qu'elle n'est pas assez fiable

Le principal argument des pro-bannissement est le manque de fiabilité de la technologie. Les exemples de biais se multiplient, pour une intelligence artificielle pourtant censée être impartiale.

La plateforme Uber s'est retrouvée sous le feu des projecteurs à cause de son système d'identification, qui ne fonctionne pas correctement dans le cas d'une personne transgenre.

L'Administration américaine pour la sécurité des transports a quant à elle reconnu que les portiques des aéroports avaient tendance à sonner davantage au passage d'une femme noire.

Une étude du MIT a démontré que les programmes de reconnaissance faciale étaient plus

efficaces pour distinguer des hommes blancs que des personnes racisées. Dans ce contexte, difficile d'imaginer une application généralisée de cette technologie alors que les mauvais exemples se multiplient.

Parce qu'une partie de la classe politique s'y oppose

Comme pour toute innovation technologique connaissant une avancée soudaine, la loi accuse un temps de retard pour statuer. Les États se penchent sur la reconnaissance faciale les uns après les autres.

La populaire députée démocrate Alexandria Ocasio-Cortez s'est exprimée sur le sujet lors d'une audition du Comité de surveillance et de réforme. Elle a fait part de son inquiétude quant au déploiement massif de ce genre de dispositif dans le pays et affirme que la reconnaissance faciale est « *liée à la réalité politique d'une montée globale de l'autoritarisme et du fascisme* ».

La crainte d'un État surveillé à la Big Brother est forte dans le camp des adversaires de la technologie. Déjà très répandue en Chine, où elle est l'un des outils du totalitarisme technologique mis en place par Pékin, l'utilisation de la reconnaissance faciale dans la rue ou les transports commence à se propager à d'autres pays du monde, la France n'étant pas à l'abri.

Entre les défauts de fiabilité de ses performances, le manque de transparence dans l'utilisation des données collectées, l'absence de cadre juridique et la méfiance de la population, la reconnaissance faciale connaît encore de nombreux obstacles à sa démocratisation.

Source
lesoir.be
Jennifer Mertens
20 mai 2019

8. La Chine va installer 2,76 milliards de caméras de surveillance

La Chine va renforcer ses méthodes de surveillance avec la mise en place de 2,76 milliards de caméras dotées de la reconnaissance faciale.

En 2016, l'Empire du Milieu comptabilisait déjà 176 millions de caméras de surveillance à travers son territoire. Un chiffre déjà bien impressionnant, mais qui va continuer de croître jusqu'en 2022 avec l'objectif de déployer 2,76 milliards de vidéosurveillances. Une omniprésence de technologies de pistage qui permettra de surveiller les 1,4 milliard d'habitants que compte le pays.

Les caméras seront dotées de la reconnaissance faciale – comme c'est déjà le cas avec les caméras actuelles – qui, sur base d'une base de données d'images numériques, seront capable d'identifier automatiquement une personne filmée.

Depuis les attentats du 11 septembre, le marché des caméras et technologies de surveillance a connu un bond exponentiel en Chine. La modernisation des villes de l'Empire du Milieu a également joué sur la présence de vidéosurveillance, ainsi que la volonté du gouvernement de contrôler la population.

L'augmentation des caméras de surveillance dans les villes a montré « des résultats remarquables » en termes d'améliorations de la sécurité publique, de la prévention et de la répression de la criminalité, ainsi que l'amélioration de la gestion du trafic et des véhicules d'urgence, explique Inside China Tech.

Contrairement aux États-Unis où la reconnaissance faciale est principalement utilisée dans les aéroports, cette forme de technologie est beaucoup plus implantée dans le quotidien des Chinois. En effet, la reconnaissance faciale est déjà utilisée dans le cadre scolaire afin de contrôler l'absentéisme des écoliers et étudiants. Évidemment, on retrouve également ses caméras aux points de contrôle des frontières, notamment dans les aéroports, ainsi que dans les rues et lieux publics.

Le pays souhaite mettre en place un réseau de vidéosurveillances omniprésent, fonctionnel et contrôlable au niveau national d'ici 2020. Une volonté qui pose de nombreuses questions, notamment en termes de libertés personnelles et de protection de la vie privée.

Source
Slate.fr
Léa Polverini
30 mai 2019

9. Pourquoi la Chine applique-t-elle la reconnaissance faciale aux pandas ?

Il reste un peu moins de 2000 pandas géants sauvages sur le territoire : la reconnaissance faciale permettrait de suivre leur trace.

Après avoir développé un vaste système de surveillance par reconnaissance faciale pour ses citoyens, c'est les pandas que la Chine entend pister grâce aux nouvelles technologies.

Des chercheurs du Centre chinois de conservation et de recherche pour les pandas géants ont développé une application pour identifier ces animaux, devenus symboles diplomatiques du pays. C'est sur une base de 120'000 photographies et 10'000 vidéos de pandas géants que s'appuiera l'application.

Préserver les pandas géants

Un recensement mené en 2014 par le gouvernement avait établi qu'il restait sur le territoire chinois 1.864 pandas géants vivant dans la nature, disséminés dans trois provinces de l'ouest du pays, le Sichuan (80 %), le Shaanxi et le Gansu. Il y aurait également 548 pandas en captivité.

Afin de préserver l'espèce, le gouvernement avait annoncé l'an dernier la création d'une réserve colossale, le Parc national du panda géant, qui devrait faire près de 16'860 kilomètres carrés – soit un peu moins que deux fois la taille du parc américain de Yellowstone – et qui coûterait 10 milliards de yuan, soit 1,3 milliards d'euros.

La reconnaissance faciale pourrait permettre dans cette perspective de garder une trace du nombre de pandas, et d'évaluer l'efficacité des politiques de conservation.

« *L'application et notre base de données nous aidera à rassembler des données plus précises et plus complètes sur la population, la répartition, l'âge, le ratio genré, la naissance et les morts des pandas sauvages, qui vivent dans les tréfonds des montagnes et qui sont difficiles à suivre* », a déclaré Cheng Peng, l'un des chercheurs travaillant sur le projet.

Reconnaissance faciale pour tous

Il y a déjà eu en Chine des cas de reconnaissance faciale appliquée aux animaux, comme en 2017 sur des poulets. La pratique s'ancrait alors dans une logique commerciale, puisqu'il s'agissait de suivre le parcours des volailles depuis leur ferme jusqu'aux étals des marchés, afin de rendre compte d'un élevage censé être plus « éthique ».

Ces applications animales ne sont cependant que l'élargissement d'une politique de surveillance de masse menée par le régime: en République popualaire de Chine, la reconnaissance faciale est utilisée à grande échelle dans une perspective de fichage de la population, notamment pour constituer des registres de «crédits citoyens ». Elle est également employée dans le cadre de la déportation et de la persécution des Ouïghours, une minorité turcophone musulmane de la province du Xinjiang.

Source
konbini.com
Thibault Prévost
4 juin 2019

10. Reconnaissance faciale et pornographie : la dystopie en embuscade

Au-delà de ce supposé outil de traque d'actrices X, c'est la démocratisation des outils de reconnaissance faciale qui terrifie.

Ainsi, le 28 mai, nous aurions franchi un nouveau (et énième) palier dans le solutionnisme indécent. Sur Twitter, Yiqin Fu, thésard de l'université de Stanford, postait une capture d'écran dégotée sur le réseau social chinois Weibo. Dans ce texte, dont la traduction a depuis été vérifiée par *Motherboard* aux États-Unis, un utilisateur anonyme, qui se dit basé en Allemagne, se vante d'avoir mis au point un système de reconnaissance faciale capable d'identifier les profils de réseaux sociaux de femmes à partir de leur visage sur des plateformes de contenu pornographique de type Pornhub. Le concept : permettre à ceux qui le souhaitent de « *vérifier si leurs copines ont déjà fait du porno* ».

Forcément, ce genre de nouvelle laisse un arrière-goût un peu dégueulasse dans la bouche, mais le pire est encore devant nous. Selon la traduction de Yiqin Fu, le projet représente près de six mois de travail. Il aspire près de 100 téraoctets (100'000 gigaoctets) de données glanées sur cinq des plateformes les plus fréquentées du X, et compare les visages récoltés aux bases de données de Facebook, Instagram, TikTok, Weibo « et autres ». Selon l'utilisateur, le bidouillage aurait déjà permis d'identifier plus de 100'000 actrices à travers le monde. Sur Weibo, conclut Yiqin Fu, la majorité des 1000 commentateurs exprime son engouement pour le service. Le seuil de l'écœurement est franchi.

Légal ? Certainement pas (en Europe)

Pour le moment, il n'existe aucune preuve formelle que ce système existe – pas de capture d'écran, pas de code, pas de bases de données, rien qu'un compte GitLab vide. Les questions que l'hypothèse de son existence soulève, en revanche, sont déjà là. L'une des premières (et des plus dépassionnées) porte sur la légalité de l'initiative, particulièrement au regard du règlement général sur la protection des données (RGPD) européen.

Interrogé sur Weibo, le mystérieux créateur assurait que tout allait bien puisqu'il n'avait encore rien divulgué, que la base de données qu'il avait construite n'était pas publique et que le travail sexuel était légal en Allemagne. Le 31 mai, contacté (toujours sur Weibo) par le *MIT Technology Review*, le programmeur (qui a toujours refusé de livrer son identité) semble avoir entre-temps compris les risques qu'il encourait.

En Europe comme en Californie (capitale mondiale de l'industrie du X), il existe un cadre légal étroit pour collecter des données et assurer le droit à l'anonymat en ligne, et ce genre de *doxxing* à grande échelle (le fait de révéler des identités en ligne sans consentement des personnes concernées) pourrait facilement lui valoir un procès. À plus forte raison lorsqu'il s'agit de données biométriques. L'article 9 du RGPD, rappelle le chercheur en cybersécurité Michael Veale, encadre leur récolte à des seules fins de recherche. Le programmeur, écrit le *MIT Technology Review,* s'est donc excusé et affirme avoir tout effacé… tout en réaffirmant que son algorithme existait bien.

La technologie au service de la misogynie

Fin de l'histoire ? Tant s'en faut. Si tout dans ce fait divers algorithmique donne envie de rendre son déjeuner, il a néanmoins eu le mérite de provoquer un débat sur Twitter et parmi la presse spécialisée. Eh oui, certains ont soutenu le créateur du système au motif, tout à fait recevable, qu'un tel algorithme pourrait éradiquer le *revenge porn*.

Placé entre de bonnes mains – comme une agence gouvernementale correctement supervisée par une entité indépendante, ou une ONG tout aussi supervisée –, il pourrait permettre à chacun de vérifier s'il existe des vidéos X de soi en ligne, de remonter leur trace et de les faire disparaître, à la manière d'un droit à l'oubli. C'est envisageable. Mais au regard des risques, les bénéfices potentiels pèsent bien peu.

Sur Twitter, rapidement, les commentaires horrifiés ont fusé pour pointer du doigt les infernales conséquences d'un tel système, qui verra « *des gens se faire extorquer, agresser et tuer »* Pour la chercheuse Danielle Citron, c'est « *une idée terriblement mauvaise, qui s'appuie sur la surveillance pour accroître encore le contrôle du corps féminin »*.

De fait, le monde de l'innovation nous a malheureusement habitués à l'instrumentalisation terrifiante de l'algorithmie à des fins abusives – il suffit de se souvenir des *deepfakes*, ces programmes capables de placer le visage de votre choix sur un autre corps avec un rendu réaliste. Comme le résume l'autrice féministe Soraya Chemaly sur Twitter, « *la surveillance, l'usurpation d'identité, l'extorsion et la calomnie arrivent toujours aux femmes en premier avant de toucher la sphère publique"*.

Pour preuve, Pornhub lui-même dévoilait un système similaire en grande pompe, dès 2017, pour aider les fans à retrouver leurs actrices fétiches. Son concurrent xHamster lui emboîtait rapidement le pas. En oubliant au passage toutes les victimes de *revenge porn* hébergées sur leur plateforme, et sans réfléchir au fait que si les actrices utilisent un alias, c'est peut-être justement pour éviter d'être harcelées…

Demain, le « *World Wide Face »*

Ce qui importe, dans cette histoire, n'est pas tant que ce programmeur anonyme et son algorithme soient réels ou non. Ce qui importe, c'est qu'aujourd'hui, la démocratisation des algorithmes de *machine learning* (particulièrement dans le domaine de la reconnaissance faciale), l'augmentation de la puissance des processeurs, la chute du coût de la mémoire et les incommensurables volumes de données personnelles que nous dispersons à chaque minute passée en ligne permettent théoriquement à une petite équipe, dotée de quelques connaissances en programmation, de développer un tel système en quelques mois, depuis une chambre. L'idée qu'un type développe dans son coin un système aussi nuisible est *plausible* (un service similaire existe déjà d'ailleurs, au moins).

En 2016, déjà, le *Guardian* s'inquiétait du succès d'une application mobile de reconnaissance faciale russe, FindFace, qui annonçait « *la fin de l'anonymat public »*. Depuis, d'autres algorithmes

sont disponibles. Plus puissants, mieux entraînés. Face à ce constat, la seule chose raisonnable à faire serait de sortir la tête du guidon de l'innovation et de réfléchir. Réfléchir sur la montée en gamme de la biométrie et la reconnaissance faciale massive automatisée et ce qu'elle signifie pour la vie privée, l'anonymat et le consentement. Sur son invasion lente mais progressive de tous les secteurs de notre vie, du trottoir à l'aéroport en passant par la salle de classe. Sur la création, ici et là, de réservoirs à données biométriques géants, malgré les risques de sécurité que la centralisation de données sensibles implique.

Il faut tenter d'anticiper, comme l'a magistralement fait Olivier Ertzscheid (auteur du blog affordance.info) le 3 juin, les scénarios catastrophe d'une société où le visage s'installe au centre des processus régaliens (police et justice, notamment) en même temps qu'il devient monnaie d'échange et de spéculation au sein du capitalisme de surveillance. « *Bienvenue dans le World Wide Face »*, écrit Ertzscheid, ce nouveau paradigme biométrique qui nous ferait regretter le bon vieux temps des données impersonnelles.

Identification, surveillance, triage

Notre salut, c'est qu'il y a quelque chose de foireux au royaume du World Wide Face. Nous voilà confrontés à une technologie défaillante, plus dangereuse encore qu'une reconnaissance faciale infaillible. De nombreux acteurs publics et privés (les seconds vendant leurs systèmes aux premiers, contre l'avis de leurs salariés) nous pressent pourtant de l'accepter sans réserve, que ce soit pour notre sécurité, comme à Nice, ou pour débloquer rapidement l'écran de notre téléphone. Ne nous laissons pas leurrer : reconnaître automatiquement des visages avec 100 % de précision est loin d'arriver. En 2019, nos IA ont encore du mal à différencier un chihuahua d'un muffin.

Rappelons quelques évidences. La reconnaissance faciale, outil statistique, génère des faux positifs à la chaîne (au Royaume-Uni, on frôle les 100 % d'erreur pendant les tests). La reconnaissance faciale, parfois entraînée sur des données biaisées, discrimine des populations déjà marginalisées (on se souviendra que les systèmes de Google avaient pour péché mignon, courant 2015, de confondre les Noirs avec des gorilles). Parfaite, elle serait implacable ; imparfaite, heureusement, elle n'est *que* terrifiante.

Imaginez les conséquences d'un faux positif de l'algorithme d'identification d'actrices porno pour une femme lambda, qui ressemblerait un peu trop à l'une d'elles aux yeux des machines. Imaginez son compte Facebook ou Instagram lié par la myopie algorithmique à un profil Pornhub. Rappelez-vous qu'on ne négocie pas avec une fonction mathématique, même si celle-ci vous pourrit la vie par erreur. « *Toute identification*, martèle Ertzscheid, *est d'abord une désignation. »* Et toute désignation porte en soi la promesse de la stigmatisation. Que vous soyez identifié correctement ou pas importe peu, une fois que le sceau est apposé.

Vendue comme utopie d'une police incontestable (car forcément neutre, transparente et dépassionnée), la reconnaissance faciale automatisée n'est rien de tout cela. Elle est un outil au service d'un projet politique obsédé par la surveillance, le suivi, le triage. Elle n'a rien d'inévitable, encore moins d'urgent (la mairie de San Francisco vient tout simplement de l'interdire) dès lors que l'on s'intéresse davantage à ses dérives qu'à ses bénéfices. La tête dans le guidon du progrès technique, nous risquerions de ne pas voir venir le précipice.

Source
Siècle digital
Éléonore Lefaix
8 août 2019

11. En Russie, la reconnaissance faciale va être utilisée pour surveiller les chauffeurs de taxis fatigués

À travers l'utilisation de ce logiciel, l'objectif étant de réduire les accidents en Russie. Si les chauffeurs sont trop fatigués, ils se verront bloquer la prise de nouvelles courses.

En France, Uber a lancé depuis plusieurs mois une limitation du nombre d'heures de conduite consécutives des chauffeurs afin de prévenir la fatigue au volant. Plus récemment, la société a invité ses chauffeurs à faire davantage aux autres et notamment aux cyclistes, afin d'éviter les accidents. En Russie les activités de Yandex.taxi (société de VTC) ont fusionné avec Uber en 2017. Pour éviter les accidents et la fatigue au volant, Yandex.taxi va utiliser la reconnaissance faciale afin de détecter la fatigue chez les chauffeurs comme le rapporte Bloomberg.

Surveiller le chauffeur et lui bloquer de nouvelles courses

Le dispositif va être placé sur le pare-brise des véhicules. Ce dernier sera en mesure d'identifier

les conducteurs fatigués en surveillant leurs yeux, les bâillements et d'autres indicateurs montrant des signes de fatigue. Le logiciel utilisé peut surveiller 68 points faciaux. Si un chauffeur est trop fatigué, la technologie pourra lui interdire de prendre d'autres courses et donc l'obliger à faire une pause.

Des mesures misent en place pour améliorer la sécurité

En Russie, le nombre d'accidents impliquant un taxi a augmenté de 25 % à Moscou, en 2018. La Russie a donc demandé aux sociétés de prendre les choses en main afin d'éviter les accidents. Les chauffeurs ont l'habitude d'utiliser plusieurs applications afin de maximiser leur chiffre d'affaires.

La technologie de Yandex a déjà été testée dans 100 voitures et devrait prochainement s'étendre au reste des chauffeurs. Même si Yandex utilise la reconnaissance faciale et bloquera les chauffeurs fatigués, les autres applications n'utilisent pas forcément cette technologie. Les conducteurs ont donc la possibilité de continuer à prendre d'autres courses via d'autres services. Une initiative encourageante qui devrait être uniformisée aux autres services.

Point à noter : aucune information sur le traitement des données n'a été communiquée. On ne sait pas si les chauffeurs seront surveillés toute la journée, après X heures de conduite, comment les données seront stockées et utilisées. Par ailleurs, comme on peut le voir dans la photo en haut de l'article, la caméra du logiciel semble également prendre en photo le passager, quid de sa vie privée ?

Source
sciencepost.fr
Yohan Demeure
8 août 2019

12. Cette IA est capable d'identifier des émotions humaines à partir de simples photos

Baptisée EmoNet, cette intelligence artificielle créée par des chercheurs américains a été capable de déterminer des émotions humaines parmi différentes catégories. Le fait est que cette IA est capable d'une telle prouesse à partir d'une simple photographie où d'une image de film !

Plus d'une dizaine de catégories d'émotions

Dans une publication de la revue *Science Advances* du 24 juillet 2019, des chercheurs des universités de l'État du Colorado et de Duke ont présenté leur IA nommée EmoNet. Celle-ci s'est montré capable d'identifier 11 catégories d'émotions humaines en visionnant de simples images. Grâce au réseau neuronal d'EmoNet, pas moins de 2000 images ont été analysées puis classées dans différentes catégories d'émotions. Selon les chercheurs, des émotions telles que le désir sexuel et le manque ont pu être identifiées avec une précision de 95 % !

En revanche, d'autres sentiments liés à la joie et l'amusement ont été déterminés, mais avec un peu plus de mal. En effet, les traits du visage étant similaires, il a été assez compliqué de faire la différence. À savoir que l'intensité des émotions a également pu être analysée sur ces mêmes images.

Pourquoi de telles recherches ?

Les meneurs de l'étude ont également passé des bandes annonces de films à EmoNet. Le but ? Déterminer la catégorie du film en fonction des émotions présentes sur les images. Dans le cadre de cet exercice, l'IA s'est montrée performante à raison de 75 % des cas. Des humains ont également participé à l'expérience. Ces volontaires ont été mis face à des images pendant que leur activité

cérébrale était mesurée. Selon les résultats, l'IA est aussi pertinente que les humains pour déceler une émotion et l'identifier.

Selon les meneurs de l'étude, ces recherches ont un but particulier. En effet, il s'agit de permettre une amélioration des relations humain/machine, mais également amener à une meilleure modération de certains contenus.

En 2018, nous évoquions une intelligence artificielle mise au point par des chercheurs australiens et allemands. Celle-ci s'était montrée capable de déterminer la personnalité de quelqu'un en suivant simplement ses mouvements oculaires ! L'objectif est de permettre l'élaboration d'un dispositif capable de deviner la personnalité d'un individu parmi cinq grands critères. Citons le neuroticisme, l'extraversion, l'amabilité, la conscienciosité ainsi que l'ouverture, autrement dit le « big five » en psychologie.

Source
fredzone.org
Holy
4 septembre 2019

13. Chine : un homme suspecté de meurtre a été arrêté grâce à un système de reconnaissance faciale

La technologie ne cesse de nous surprendre avec ses multiples capacités. En Chine, certaines entreprises utilisent une application basée sur l'intelligence artificielle pour leur permettre d'identifier leurs clients.

Récemment, un système de reconnaissance faciale a permis aux autorités d'arrêter un homme suspecté d'avoir tué sa petite amie et d'avoir tenté de scanner son visage pour pouvoir obtenir un prêt.

Selon les rapports, l'homme a été officiellement arrêté vers le début du mois d'août, bien que le meurtre se soit produit y il a plusieurs mois de cela.

Une histoire d'argent

D'après les autorités, le suspect aurait tué sa partenaire le 11 avril dernier en l'étranglant avec une corde. Selon les informations, le couple se serait disputé à cause de problèmes d'argent, c'est ce qui aurait incité l'homme à passer au meurtre. Après avoir effectué son méfait à Xiamen, l'homme s'est enfui à Sanming, sa ville natale qui se trouve à environ quatre heures de route de là.

Arrivé à Sanming, le présumé meurtrier a essayé d'obtenir un prêt sur Money Station en utilisant l'identité et le visage de sa partenaire. Seulement, le système de reconnaissance faciale n'a pu identifier la défunte, car le système nécessite le clignement des yeux du client pendant le processus d'approbation. D'autre part, l'application a également détecté la voix d'un homme et non celle d'une femme.

Pour voir ce qui n'allait pas, les employés de l'entreprise ont procédé à une vérification manuelle. C'est alors qu'ils ont constaté que la cliente en question avait des ecchymoses sur le visage et des marques rouges au niveau de son cou.

Plusieurs accusations

A part le fait d'être le principal suspect du meurtre de sa petite amie, plusieurs autres accusations pèsent également sur l'homme. Le South China Morning News a en effet déclaré qu'il a aussi été accusé d'avoir volé 30'000 yuans, soit 4200 dollars qui se trouvaient sur le compte de la victime. Il a ainsi utilisé le téléphone de cette dernière pour retirer l'argent.

Selon les informations, le suspect a également utilisé le téléphone de la défunte pour mentir à ses parents en leur disant que celle-ci était en voyage. Pour expliquer l'absence de sa petite amie au travail, il a demandé un congé à l'employeur de celle-ci.

Quoi qu'il en soit, on se demande si les systèmes de vérification biométrique seront aussi efficaces dans d'autres situations, par exemple contre les voleurs qui deviennent actuellement de plus en plus rusés.

Source
Clubic
Benjamin Bruel
8 septembre 2019

14. Les caisses automatiques à reconnaissance faciale sont une réalité en Chine

Un sourire, pas de carte bleue, de porte-monnaie ou de liquide : la reconnaissance faciale pour payer ses achats ne cesse de se développer en Chine, malgré les inquiétudes concernant le respect de la vie privée.

Plusieurs centaines de systèmes de point de vente ont été installés dans des villes chinoises pour imposer la reconnaissance faciale comme nouveau système de paiement.

Relier les visages à des comptes bancaires

Le système de paiement par téléphone mobile chinois est le plus avancé et le plus développé au monde. On connaît également le système de « crédit social » utilisé par le pays, qui fonctionne en partie par la reconnaissance faciale.

Désormais, c'est un autre type de technologie qu'utilise à outrance la Chine : l'achat par reconnaissance faciale. Les consommateurs chinois peuvent ainsi faire leurs achats simplement en passant leur tête devant une machine de point de vente équipée de caméras, qui relie les traits de leur visage à un système de paiement digital ou un compte bancaire.

« *Je n'ai même plus besoin d'emmener mon téléphone portable avec moi, je peux sortir faire mes achats sans rien emmener* », explique Bo Hu, propriétaire d'une chaîne de boulangeries de la ville de Beijing, à l'AFP. « *Ce n'était pas envisageable aux premiers stades du paiement mobile, c'est seulement après le développement de la reconnaissance faciale que nous avons pu payer sans avoir besoin de rien* ».

Selon l'agence de presse francophone, les consommateurs chinois semblent « *imperturbables* » face au développement de cette technologie et aux questions qu'elle soulève quant à la sécurité des données et le respect de la vie privée.

Des « *sourires pour payer* » dans une centaine de villes

La technologie est développée et mise en place par Alipay, le bras financier du géant de l'e-commerce chinois Alibaba. Bien que ce système reste encore marginal en comparaison du paiement mobile, l'entreprise a déjà implanté ses machines dans une centaine de villes et compte investir plus de trois milliards de yuan (420 millions de dollars) dans les trois prochaines années, pour consolider la présence de ces moyens de paiement.

De son côté, Tencent, mastodonte du jeu vidéo et propriétaire de l'application WeChat, le WhatsApp chinois aux 600 millions d'utilisateurs, a dévoilé sa nouvelle technologie de paiement par reconnaissance faciale sur mobile en août, dénommée « Frog Pro ». De nombreuses start-up essaient également de trouver une place sur ce marché qui s'annonce juteux…

Notons en outre que, récemment, un sondage du site d'informations technologiques *Sina Technology* a dévoilé que 60 % des participants affirmaient que scanner leur visage les faisaient se sentir « *moche* », ce qui a conduit Alipay à promettre l'ajout de « filtres embellissant ». Orwellien.

Source
lemonde.fr
Pascal Gitton
17 février 2020

15. Les biais biométriques et ethniques des logiciels de reconnaissance faciale

Développée depuis longtemps, la reconnaissance faciale est aujourd'hui au centre de nombreux débats questionnant la mise en œuvre de cette technologie, notamment sur un plan éthique. Avec des décisions parfois hésitantes comme celles de la Commission européenne qui, après avoir annoncé un moratoire sur l'utilisation de cette technologie, est revenue en arrière quelques jours après. Afin de pouvoir comprendre les enjeux, il est important de bien connaître ces algorithmes et leurs biais. C'est pour contribuer à cette maîtrise que Charles Cuvelliez et Jean-Jacques Quisquater nous présentent une étude récente analysant des produits commercialisés.

De quoi parle-t-on ?

On a tendance à confondre – à tort – reconnaissance faciale et analyse faciale. Avec l'analyse faciale, c'est une ou plusieurs propriétés continues liées au visage (âge, fatigue, stress, ...) qui sont analysées. Elle a pour but de déterminer une quantité qui permet de verser une personne dans une catégorie (son sexe, son état émotionnel, ...). Les algorithmes utilisés sont construits avec une connaissance présupposée des catégories en question.

La reconnaissance faciale et les algorithmes qui la sous-tendent calculent, sur la base du visage à reconnaître, un ensemble de valeurs qui caractérisent l'identité de la personne. Ils comparent ces valeurs soit avec celles d'une base de données lorsqu'il s'agit d'identifier une personne (identification), soit avec une image du visage prise antérieurement (authentification), par exemple pour déverrouiller un smartphone ou une application bancaire. Un score de similitude est calculé, puis comparé à un seuil fixé par le développeur de l'algorithme. Ce seuil, atteint ou non, décide si le

visage est reconnu.

Il y a deux types d'erreur : les faux négatifs et les faux positifs. Un faux négatif correspond à une reconnaissance faciale ayant échoué, c'est-à-dire n'ayant pas reconnu un visage pourtant préalablement enregistré. La victime ne peut déverrouiller son téléphone ou passer des portiques de sécurité. C'est souvent gênant, rarement dangereux. Un faux positif est plus problématique. Une reconnaissance est établie alors qu'elle n'aurait pas dû avoir lieu, ce qui se ramène à une usurpation d'identité : une personne obtient des accès auquel elle n'a pas droit ou bien peut être accusée à tort d'un délit.

Selon l'application, l'impact des faux positifs et faux négatifs n'est pas le même : s'il s'agit d'écarter les hooligans d'un stade, un taux élevé de faux négatifs est moins problématique puisque la probabilité d'avoir un hooligan, déjà interdit de stade, est peu élevée.

De gros progrès

Le NIST (National Institute of Standards & Technology), agence du département du commerce des États-Unis, a entamé une étude comparative des solutions commerciales de reconnaissance faciale depuis plusieurs années. Leurs progrès ont été spectaculaires : les taux d'erreur sont bien inférieurs à ceux de 2010 grâce notamment à l'utilisation des réseaux de neurones profonds (appelés Deep Convolutional Neural Networks en anglais).

La reconnaissance faciale est un problème pratiquement résolu d'un point de vue théorique mais il subsiste encore beaucoup d'algorithmes qui n'atteignent pas la perfection des meilleurs et qui restent cependant intégrés dans des solutions commercialisées. En fait, seuls quelques algorithmes excellent vraiment, notamment pour des images de basse qualité ou pour une reconnaissance faciale qui doit rester efficace sur plusieurs années (c'est-à-dire pour gérer le vieillissement, qui s'il n'est pas bien pris en compte, nécessite par exemple de refaire son passeport). Ne pas choisir un « bon » algorithme, entraîne donc une prise de risques.

S'il paraît évident que la qualité des photos utilisées influe directement sur les résultats, il était difficile d'imaginer l'importance de la présence d'un opérateur qui vous guide au moment de la saisie initiale (orientation de la tête ou expressivité du visage) écrit le NIST. Idéalement, même, il faudrait disposer de plusieurs images d'une même personne dans la base de données de comparaison. L'étude souligne que certains algorithmes ne sont pas stables avec la taille de la base de données : leur taux de faux positifs et de faux négatifs augmente en fonction de cette dernière, ce qui ne permet pas de les utiliser à grande échelle.

Le NIST rappelle que ces algorithmes ne sont pas devenus monnaie courante ; il subsiste des différences de performances importantes qui justifient le maintien d'un test continu d'évaluation.

Cet organisme recommande de ne pas se contenter des simples critères comme le coût ou la facilité d'intégration de l'algorithme dans le système visé. Il faut aussi tenir compte de ses performances, de la possibilité d'un contrôle humain en cas de doute, de la maintenance du code, etc.

Des biais démographiques qui posent question

Le NIST s'est également intéressé aux biais démographiques. Ces faux positifs et/ou ces faux positifs sont-ils plus fréquents pour les femmes, les jeunes, les personnes âgées, sont-ils sensibles à l'origine ethnique ? L'étude a considéré les quatre grands ensembles de photos en usage aux États-Unis : les photos judiciaires et de signalement, les photos des candidats à l'immigration, les photos des candidats à l'obtention d'un visa et les photos aux frontières. Il s'agit en tout de 18.27 millions de photos de 8.49 millions de personnes sur lesquels 189 algorithmes commerciaux de 99 développeurs ont été testés. C'est le taux de faux positifs qui est le plus sensible aux variations démographiques, quel que soit l'algorithme : on observe une variation de ce taux évoluant entre 10 et 100. Les faux négatifs sont plus dépendants de l'algorithme avec une variation du taux en-dessous de 3.

Pour les faux négatifs, le NIST observe un taux d'erreur entre 0.5 % et 10 % selon l'algorithme. Pour les photos d'identité judiciaire, c'est chez les personnes de couleur noire que le taux d'erreur est le moindre. Leur visage vieillit moins vite, pense, pour l'expliquer, le NIST qui ne veut pas relier cette observation à une proportion plus grande de personnes de couleur noire dans l'identité judiciaire.

Avec des photos de haute qualité prises dans le cadre d'une demande d'immigration, le taux de faux négatifs est beaucoup plus bas, et ne recèle, semble-t-il, aucune sensibilité aux différences démographiques. Quant aux images prises dans des conditions plus précaires au passage des frontières, les faux négatifs sont plus élevés pour les personnes originaires d'Afrique, des Caraïbes et pour les individus plus âgés.

Les faux positifs

L'étude a aussi révélé que le taux de faux positifs, plus dangereux donc, était de 2 à 5 fois plus élevé chez les femmes, selon l'algorithme, le pays d'origine ou l'âge. Quant à l'origine ethnique, le taux de faux positifs est le plus élevé pour les Africains de l'est et de l'ouest du continent. Il reste élevé pour les gens d'Amérique centrale. Le taux d'erreur est le moins élevé pour les Européens de l'Est.

Les algorithmes développés par les entreprises chinoises sont les meilleurs, écrit le NIST : non seulement, ils ont des bas taux de faux positifs tant pour les Asiatiques (pour lesquels les autres algorithmes fonctionnent mal) que pour les Caucasiens. L'environnement géographique et culturel du développement de l'algorithme a une importance, ne fut-ce que par le choix des données d'entraînement.

Peut-on limiter ces erreurs ? Oui, lorsqu'il s'agit d'une reconnaissance d'identité, il suffit de passer la base de données en revue plusieurs fois avec plusieurs algorithmes ou d'appliquer des techniques d'évitement (comme présenter à un évaluateur humain tous les faux positifs). Avec un algorithme d'authentification (par exemple déverrouiller un appareil), c'est plus difficile puisqu'on a une décision tout ou rien, sans retour possible. Quelques algorithmes comme Idemia ou NEC3 ne présentent pas de biais démographique et seront d'ailleurs utilisés pour identifier les athlètes aux jeux olympiques de Tokyo, qui brasseront toutes les origines ethniques. De façon plus globale, il faut plutôt privilégier les algorithmes qui produisent des taux de faux positifs ou faux négatifs indépendants de la taille de la base de données de comparaison (Aware, Tevian et Real Networks), ils permettent de faire de la reconnaissance de masse (pour le meilleur ou pour le pire).

Quelles sont les causes des faux positifs et faux négatifs dus aux biais démographiques ? Le NIST ne s'avance pas mais mentionne quelques pistes d'explication, comme les effets de la caméra, notamment l'interaction caméra-individu ou comme on s'en doute la qualité de l'image. Certains algorithmes mesurent la qualité de l'image et refusent carrément une reconnaissance si elle n'est pas suffisante, pour éviter un faux négatif.

Comme le montrent les algorithmes développés en Chine qui présentent moins de biais démographiques, parce que disposant de données d'entraînement plus larges et plus multi-ethniques, étendre les données d'entraînement est un premier remède. Exploiter la finesse de la texture de la peau ou la forme du visage sont d'autres moyens d'améliorer la reconnaissance : il existe un algorithme breveté en 2004 qui a réussi, sur cette base, à distinguer des vrais jumeaux ! La reconnaissance de l'iris n'est pas, non plus, prise en compte dans les algorithmes de reconnaissance faciale. Mais ce n'est pas facile : la précision actuelle des capteurs nécessite d'être positionné très (trop) près de la caméra pour que l'iris soit correctement détecté. Enfin, dernière piste, on peut fixer des seuils différents en fonction du groupe visé, âgé, jeune, d'une certaine origine ethnique, à partir duquel on déclare avoir un faux positif ou un faux négatif variable. C'est assumer les biais démographiques.

Quelle régulation ?

L'Europe hésite : en quelques jours, elle a d'abord annoncé vouloir mettre un moratoire visant à interdire pendant 5 ans la reconnaissance faciale dans les lieux publics, puis elle a fait marche arrière en évoquant la mise en place d'exigences spécifiques pour encadrer cette technologie. Entre le déverrouillage de son mobile et la surveillance continue des citoyens dans la rue, la reconnaissance faciale couvre un très large spectre d'applications. Prenons le temps d'une vraie réflexion éclairée par une bonne connaissance des solutions et des enjeux avant de décider une quelconque utilisation.

Charles Cuvelliez (Ecole Polytechnique de Bruxelles, Université de Bruxelles) & Jean-Jacques Quisquater (Ecole Polytechnique de Louvain, Université de Louvain et MIT)

Source
capital.fr
François Miguet
2 janvier 2020

16. La reconnaissance faciale va-t-elle virer au cauchemar ?

Cette technologie bluffante sera au cœur des futures "villes intelligentes". Mais l'exemple du Big Brother à la chinoise inquiète. Débat entre deux experts aux avis tranchés.

De Pékin à Shanghai, chaque citoyen est désormais noté. S'il jette un mégot ou traverse au feu rouge, s'envolent ses chances de décrocher un job couru ou de prendre l'avion. Ce système orwellien

repose quasi entièrement sur la reconnaissance faciale. Chez nous, pour l'instant, rien de comparable. Mais demain ? Capital a réuni deux experts pour y voir plus clair.

Capital : La reconnaissance faciale est-elle une chance ou une menace ?

Raphaël de Cormis* : Comme toute technologie, la reconnaissance faciale est, en soi, neutre. Tout dépend de la manière dont on l'utilise. Ses premiers développements datent d'il y a une trentaine d'années, mais, avec sa démocratisation, on assiste à un retour de l'imaginaire cyberpunk des années 1970-1980, certains craignant d'être espionnés de toutes parts. On peut le comprendre. Mais il faut savoir que la très grande majorité des projets en la matière se font sans aucune base de données, sansfichier d'aucune sorte. La plupart du temps, et c'est d'ailleurs le cas des sas de passage aux frontières Parafe de Gemalto, qui sont déployés dans les aéroports français, les caméras à reconnaissance faciale se contentent de vérifier si votre visage correspond aux indicateurs biométriques qui figurent déjà, de manière codée, sur votre pièce d'identité. Elles ne collectent ni ne transmettent rien.

Gaspard Koenig :** Je suis d'accord sur l'idée que toute technologie est, en principe, neutre. Du reste, la reconnaissance faciale est, en soi, intéressante, et même assez miraculeuse. Néanmoins, si elle suscite la polémique encore plus que les autres formes d'intelligence artificielle (IA), c'est justement parce qu'elle touche au visage. Or le visage, « la visagéité », comme disait le philosophe Gilles Deleuze, est le reflet de notre identité la plus profonde, de notre moi intime. Quand on utilise la reconnaissance faciale pour déverrouiller son téléphone, ou quand un gouvernement vous propose cette option pour accéder plus simplement à des services administratifs, pourquoi pas. Mais il est inquiétant que l'on puisse recueillir à terme un visage dans l'espace public, à la volée, et de manière non consentie.

En quoi cette technologie peut-elle changer notre quotidien ?

Raphaël de Cormis : D'abord, elle nous aidera à fluidifier les villes dont la démographie va continuer à exploser : avec la gestion des mouvements de foule, ou encore l'identification quasi instantanée d'une personne qui a fait un malaise. Ensuite, elle permettra de créer de la confiance dans les échanges numériques. Les réseaux sociaux pourront demander à leurs utilisateurs, avec leur consentement, qu'ils s'identifient avec leur visage avant de publier un contenu ou de lancer une campagne publicitaire, afin qu'ils puissent vérifier de manière certaine que vous êtes bien un être humain, et non une de ces IA qui diffusent des « fake news » par milliers pour manipuler l'opinion. Cela permettra aussi de sécuriser et de fluidifier les paiements. Il n'y aura plus de fastidieux formulaires (nom, date de naissance, etc.) ni de codes de confirmation reçus par SMS : un selfie suffira. Le but est de parvenir à un système presque aussi fluide et fiable que celui de la poignée de main des commerçants d'autrefois, en apportant plus de simplicité, de chaleur humaine.

Gaspard Koenig : Payer dans un magasin en montrant son faciès à une caméra, comme cela existe déjà en Chine, c'est précisément l'inverse de la chaleur humaine ! En vérité, le risque est grand d'aller vers un monde à la Minority Report. Dans ce livre de Philip K. Dick, adapté par Steven Spielberg, le héros est reconnu par les publicités qui lui proposent une bière quand il rentre fourbu du travail, et par les caméras publiques qui le traquent. Pour leur échapper, il finit par se faire implanter de nouveaux yeux. Quand on voit les manifestants hongkongais tenter, chaque week-end, de masquer leur visage pour déjouer les systèmes de reconnaissance faciale, ce récit paraît prémonitoire.

Le Big Brother à la chinoise débarquera-t-il un jour chez nous ?

Raphaël de Cormis : Le système chinois de « social scoring » (crédit social) doit être remis dans son contexte. Là-bas, on place très haut la notion d'harmonie communautaire. Chez nous, c'est différent. L'Union européenne s'est construite sur le respect des libertés. En France, tout projet de déploiement de caméras dans l'espace public doit être soumis à l'autorisation du Conseil d'Etat. Et le règlement général sur la protection des données (RGPD) européen encadre très rigoureusement les informations biométriques : il faut obtenir le consentement de la personne, garantir un certain degré de protection, assurer un droit à l'oubli, et indiquer à quelle échéance la donnée sera effacée. Enfin, obligation est faite de proposer des solutions alternatives aux usagers. Passer par les sas aéroportuaires automatisés dont nous parlions plus tôt n'est, par exemple, pas obligatoire. Il y a

toujours des guichets.

Gaspard Koenig : Reste que nous vivons dans un monde où la vérification de l'identité semble sans cesse renforcée. Sur ses lignes régionales, la SNCF nous oblige désormais à renseigner notre date de naissance afin que les billets soient nominatifs. En quoi est-ce nécessaire puisque la seule information qui compte est que le billet ne puisse être utilisé deux fois ? En réalité, l'anonymat de chacun est de plus en plus menacé. L'État, les entreprises… tout le monde veut savoir qui fait quoi, qui va où, et pour quoi faire. Prenons garde : selon les termes de Michel Foucault, une société où tout le monde respecte parfaitement la loi, sans espace pour les « illégalismes », déploie des processus de contrôle qui étouffent toute créativité. La « smart city » peut facilement se transformer en « dead city », comme le dit aussi Stuart Russell, un chercheur de l'université de Berkeley (Californie). Les touristes chinois préfèrent d'ailleurs déambuler dans les rues de Paris, témoins de l'ordre spontané, que de se balader dans les artères de leurs villes nouvelles que la planification à la chinoise a rendues inhumaines.

Le projet de reconnaissance faciale de l'État français, Alicem, a suscité une levée de boucliers. Justifiée ?

Raphaël de Cormis : Je ne m'exprimerai pas sur le projet Alicem. Seul notre client, l'Agence nationale des titres sécurisés (ANTS), est habilité à le faire. Mais, plus généralement, les technologies que nous mettons en œuvre empêchent toute usurpation d'identité. Contrairement à ce que l'on pourrait croire, ni une photo ni un masque à la Mission impossible ne permettent de les déjouer, car elles sont basées sur la reconnaissance très fine des traits « mathématiques » de votre visage et des mouvements de votre tête.

Gaspard Koenig : Certaines associations se sont lancées tambour battant dans cette polémique, à tort. A priori, un système de reconnaissance faciale qui prévoit que les données ne quittent pas le téléphone de l'utilisateur ne me pose pas de problème. Ne sombrons pas dans la technophobie ! Le vrai souci serait que l'État puisse constituer de manière centralisée un mégafichier de données biométriques. Un décret de 2016 le prévoit sous la forme du fichier TES. Génération libre, mon association, l'a contesté devant le Conseil d'État ; nous avons été déboutés. Mais nous poursuivons cette action au niveau européen. Car pour nous, il vaut mieux vivre dans une société plus chaotique, peut-être même plus dangereuse, mais dans laquelle une forme de « droit à l'errance » est préservée.

Le principe de précaution à l'européenne freine-t-il notre compétitivité ?

Gaspard Koenig : Bien sûr, les intelligences artificielles se développent généralement grâce à l'accumulation des données, le big data. Donc, avec le RGPD, qui en restreint la collecte, l'UE a choisi de faire un sacrifice économique au nom des libertés. C'est un choix culturel fort. Et nous ne sommes pas les seuls. En Californie, berceau des technologies, les choses bougent. La ville de San Francisco vient d'interdire la reconnaissance faciale dans l'espace public. En réalité, c'est tout le monde occidental qui est confronté à un dilemme nouveau. Longtemps, on nous a expliqué que le progrès économique et la liberté individuelle marchaient main dans la main. À présent, on constate que l'IA rend ces deux termes antagonistes et qu'il faut trouver un équilibre entre le développement économique, la sécurité et les libertés.

Raphaël de Cormis : La contrainte rend toujours les hommes plus innovants. Collecter de la donnée massivement ne permet pas de répondre à tous les problèmes, et c'est très énergivore. Nous arrivons à d'excellents résultats avec des IA qui ne sont pas basées sur le « machine learning », et qui sont transparentes, explicables et éthiques. Rassurez-vous, sur la reconnaissance faciale, l'Europe est loin d'avoir décroché.

** Vice-président innovation et digital de Thales-Gemalto, l'un des groupes français les mieux positionnés sur cette technologie.*

*** Fondateur de Génération libre, auteur de « La Fin de l'individu, voyage d'un philosophe au cœur de l'intelligence artificielle ».*

Source
Usbek & Rica
Pablo Maillé
10 juin 2020

17. IBM abandonne la reconnaissance faciale au nom de la lutte contre le profilage racial

Face à l'ampleur des manifestations contre le racisme et les violences policières aux États-Unis, la multinationale IBM a annoncé qu'elle renonçait à tout projet de reconnaissance faciale, accusée d'entretenir les discriminations et le profilage racial.

Le mouvement *Black Lives Matter* aura-t-il raison des technologies de reconnaissance faciale ? Alors que les entreprises du secteur comptaient pousser encore plus loin leurs algorithmes en les entraînant à surmonter « *l'obstacle technique* » que constitue le port du masque, la mort de George Floyd, un Afro-Américain de 46 ans, lors d'une interpellation violente à Minneapolis (Minnesota), pourrait freiner leur enthousiasme. Depuis quelques semaines, des dizaines de milliers de personnes manifestent chaque jour dans de nombreuses villes des États-Unis (et ailleurs dans le monde), à la fois pour lui rendre hommage et dénoncer, plus largement, les violences policières et le racisme.

Ni développement, ni recherche

Réagissant à ces évènements, le PDG d'IBM Arvind Krishna a annoncé que sa société n'investirait plus ni dans le « *développement* » ni dans la « *recherche* » en matière de reconnaissance faciale. Une déclaration très officielle, relayée sous forme de lettre à l'intention de certains membres du Congrès américain dont Cory Booker, Kamala Harris ou encore Karen Bass.

« *IBM s'oppose fermement à — et ne tolérera pas — l'utilisation de toute technologie [de reconnaissance faciale], y compris les technologies offertes par d'autres fournisseurs, pour la surveillance de masse, le profilage racial, les violations des droits humains et des libertés fondamentales, ou tout autre objectif non conforme à nos valeurs et à nos principes de confiance et de transparence*, assure le PDG dans sa lettre. *Nous pensons que le moment est venu d'entamer un dialogue national sur l'opportunité et la manière dont la technologie de reconnaissance faciale devrait être utilisée par les autorités chargées de l'application des lois.* » D'après *The Verge*, la déclaration entérine, de fait, l'abandon de tout projet de reconnaissance faciale de la part d'IBM.

Ce revirement apparaît pour le moins surprenant au vu des importants investissements de la multinationale américaine dans le secteur. Comme nous vous l'expliquions dans un précédent article, en 2019, IBM avait notamment annoncé mettre à la disposition de la communauté scientifique une base de données appelée « Diversity in Faces », constituée de photos de près d'un million de visages humains pour servir à nourrir un algorithme de reconnaissance faciale… sans que les personnes concernées n'y aient consenti.

Mais déjà à l'époque, l'objectif était (en théorie) de constituer des bases de données qui rendent mieux compte de la diversité des visages humains afin de « *réduire les biais raciaux* » des algorithmes, évoqués par de nombreuses études menées ces dernières années. Pour n'en citer que deux, il a ainsi été montré que la détection de piétons à la couleur de peau foncée était moins précise que pour les personnes à la peau blanche, ou encore que les algorithmes identifiaient par erreur les

personnes asiatiques ou noires 100 fois plus souvent en moyenne que les personnes blanches.

Le précédent Clearview AI

Cette fois, le nouveau PDG du groupe Arvind Krishna va donc plus loin, plaidant même pour une « *réforme de la police* » dans sa lettre. Sous pression face à l'ampleur des revendications outre-Atlantique, la décision de l'entreprise fait également suite à la récente affaire Clearview AI, du nom de cette start-up ayant constitué une immense base de profils à partir de données publiques disponibles sur les réseaux sociaux. Comme le révélait le *New York Times* au début de l'année, l'application était utilisée par la police américaine mais aussi par des groupes industriels et commerciaux, dont certaines enseignes de la grande distribution comme Best Buy ou Macy's.

Reste à savoir si les appels à des actions similaires de la part d'autres géants du secteur seront entendus. Des organisations comme l'American Civil Liberties Union (ACLU) appellent depuis longtemps Amazon à cesser de fournir sa propre technologie de reconnaissance faciale à la police, l'accusant de « *contribuer à la criminalisation des communautés de couleur* ».

Pour Charlton McIlwain, chercheur et auteur du livre *Black Software: The Internet & Racial Justice, From the AfroNet to Black Lives Matter*, le racisme entretenu par les technologies de surveillance a des origines bien plus profondes, qui ne seront réversibles qu'à condition d'un bouleversement majeur. « *Mandatée par le Congrès, l'entreprise Simulmatics a mené une campagne de surveillance à grande échelle dans les "zones touchées par les émeutes" dès l'été 1967*, rappelle-t-il dans un texte publié par le Massachusetts Institute of Technology (…) *À la fin des années 1960, ce type de données avait contribué à créer ce que l'on a appelé les systèmes d'information sur la justice pénale". Ils ont proliféré au cours des décennies, jetant les bases du profilage racial, de la police prédictive et de la surveillance raciale ciblée.* » Manière de dire que ces phénomènes, eux non plus, ne datent pas d'hier.

Source
letemps.ch
ATS
11 juin 2020

18. Amazon interdit à la police d'utiliser son logiciel de reconnaissance faciale

La suspension du logiciel Rekognition pour les services de la police sera effective pendant un an. La pression est montée, mardi, quand des associations de lutte contre les inégalités raciales ont demandé à Amazon à cesser toute collaboration technologique avec la police américaine .

Après IBM qui abandonne tout projet de recherche sur la reconnaissance faciale, c'est au tour d'Amazon d'interdire à la police d'utiliser son logiciel Rekognition pendant un an. Cette décision intervient dans un contexte de manifestations contre les violences policières et le racisme aux Etats-Unis.

« Nous prônons des régulations plus strictes des gouvernements sur le recours éthique aux technologies de reconnaissance faciale, et le Congrès semble prêt à relever le défi », a indiqué mercredi le géant du commerce en ligne dans un communiqué.

En attendant la réforme de la police par le Congrès

Depuis la mort de George Floyd, un Afro-Américain asphyxié par un policier blanc il y a deux semaines, les entreprises, ainsi que les autorités locales et nationales, tentent de réagir à la pression de la rue et des réseaux sociaux. Les manifestants exigent notamment des réformes en profondeur de la police et des systèmes de surveillance, dont ils estiment qu'ils ciblent les personnes noires de façon disproportionnée.

La Chambre des représentants, à majorité démocrate, a présenté lundi une loi qui vise à « changer la culture » au sein de la police des États-Unis. Elle entend notamment créer un registre national pour les policiers commettant des bavures, faciliter les poursuites judiciaires contre les agents et repenser leur recrutement et formation.

«Nous espérons que ce moratoire d'un an donnera au Congrès suffisamment de temps pour mettre en place des règles appropriées», a ajouté Amazon dans son communiqué mercredi.

Une pétition en ligne pour exiger un changement

Des organisations, comme la puissante American Civil Liberties Union (ACLU), appellent depuis deux ans Amazon à cesser de fournir sa technologie de reconnaissance faciale aux forces de l'ordre. La pression est montée d'un cran mardi, quand des associations de lutte contre les inégalités raciales ont exhorté Amazon à cesser toute collaboration technologique avec la police américaine.

Dans leur pétition mise en ligne, elles accusent le groupe de Seattle « d'alimenter et de profiter de l'injustice systématique, des inégalités et des violences contre les communautés noires ».

« Amazon a longtemps cherché à être la colonne vertébrale technologique de la police et de l'ICE (police de l'immigration) en promouvant activement Amazon Web Services (cloud), son logiciel de reconnaissance faciale (Rekognition) et ses caméras de surveillance (Ring) », a élaboré Athena, un collectif d'associations qui interpellent le groupe sur les impacts négatifs de ses diverses activités. Les caméras Ring servent à assurer la sécurité des particuliers, mais leurs propriétaires peuvent donner - s'ils le souhaitent - accès à la surveillance vidéo à la police.

Des mauvaises utilisations des technologies

« Il aura fallu deux ans à Amazon pour en arriver là, mais nous sommes heureux que l'entreprise ait enfin reconnu les dangers que pose la reconnaissance faciale pour les personnes de couleur, ainsi qu'en termes de droits civils en général», a réagi mercredi Nicole Ozer, directrice des technologies et libertés pour une branche californienne de l'ACLU.

Elle voudrait que la multinationale cesse aussi de vendre les caméras Ring «qui alimentent les interventions policières excessives contre les personnes de couleur ».

Amazon avait reconnu en octobre que, « comme toutes les technologies », la reconnaissance faciale pouvait être « mal utilisée ». Elle avait assuré que ses équipes fournissaient des indications à tous les clients du (logiciel) Rekognition, « y compris les forces de l'ordre, sur la bonne manière de s'en servir ». Le groupe de Jeff Bezos a précisé que le moratoire ne s'appliquerait pas aux organisations qui se servent de Rekognition pour sauver des victimes de trafics d'êtres humains ou retrouver des enfants disparus, comme Thorn ou l'International Center for Missing and Exploited Children.

IBM a annoncé lundi suspendre la vente de logiciels de reconnaissance faciale à des fins d'identification et s'est « opposé à l'utilisation de toute technologie à des fins de surveillance de masse, de profilage racial et de violations des droits et libertés humaines de base ».

Source
Le Monde avec AFP
11 août 2020

19. Au Royaume-Uni, la justice inflige un revers à la reconnaissance faciale

La cour d'appel de Londres a jugé que l'utilisation de la reconnaissance faciale par la police galloise n'était pas suffisamment encadrée. Ils n'ont cependant pas remis en cause le recours à la technologie en soi.

Le Royaume-Uni et ses centaines de milliers de caméras de vidéosurveillance – 420 000 rien qu'à Londres – sont un terrain rêvé pour la reconnaissance faciale. La justice du pays vient pourtant, mardi 11 août, d'infliger un revers à cette technologie controversée employée par un département de la police galloise, estimant qu'elle empiétait trop sur la vie privée.

La cour d'appel de Londres se penchait sur la plainte d'Ed Bridges, un militant pour les droits civiques qui conteste à la police galloise le droit d'utiliser la reconnaissance faciale. Selon lui, cette technique serait discriminatoire et contraire aux lois sur la protection de la vie privée.

Cette dernière a scanné à deux reprises le visage de M. Bridges, à Cardiff – lorsqu'il faisait ses courses de Noël en 2017 puis lors d'une manifestation en 2018. Ce système utilise les images captées par les caméras de vidéosurveillance pour isoler les visages et les comparer avec les photos d'une « liste de surveillance », qui peut inclure suspects, personnes disparues ou présentant un intérêt. Elle est mise en œuvre par le département de police du sud du pays de Galles, dont la juridiction inclut les deux plus grandes villes du pays, Swansea et la capitale, Cardiff. La reconnaissance faciale à la volée a notamment été utilisée en début d'année pour le concert du groupe de métal Slipknot et pour deux matchs de football opposant Cardiff à Swansea.

Une utilisation insuffisamment encadrée

Après avoir été débouté plusieurs fois, le plaignant a obtenu gain de cause, les juges estimant que l'utilisation de la reconnaissance faciale n'était pas suffisamment encadrée. Ils n'ont cependant pas remis en cause le recours à la technologie en soi.

« Trop (de choses) sont laissées à l'appréciation de chaque officier de police », ont considéré les juges. Ces derniers ont souligné qu'il n'existait pas d'indications claires sur les lieux où cette technologie pouvait être utilisée par la police ni sur les modalités conduisant à l'inscription sur la « liste de surveillance ».

Ils ont aussi reproché à la police galloise de ne pas s'être suffisamment assurée que le logiciel ne présentait pas de biais racistes ou sexistes. La reconnaissance faciale fonctionne quasi systématiquement sur un programme informatique « entraîné » à repérer des visages similaires sur une sélection constituée par un humain. À ce titre, l'algorithme peut reproduire des biais ou des erreurs humaines, dont le racisme. La cour d'appel a aussi souligné le fait que la police galloise n'avait pas correctement évalué l'impact de cette technologie sur la protection des données

Une victoire contre « un outil dystopique »

Ed Bridges s'est déclaré « ravi » du verdict réservé à cet « outil intrusif et discriminatoire » de « surveillance des masses ». L'ONG « Liberty », qui a épaulé le plaignant, a salué une « victoire majeure », appelant à ce que « le gouvernement reconnaisse les graves dangers » de cet « outil dystopique ». La police galloise a annoncé qu'elle ne ferait pas appel.

L'utilisation par la police galloise de cette technologie a été critiquée à maintes reprises, notamment par le rapporteur de l'ONU sur la vie privée ou l'autorité britannique de protection des données. Son efficacité est, elle aussi, contestée : selon une étude de l'université de Cardiff entre juin 2017 et mars 2018, plus de 70 % des identifications réalisées par le système étaient en fait des erreurs.

Source
businessinsider.fr
Albane Guichard
7 août 2020

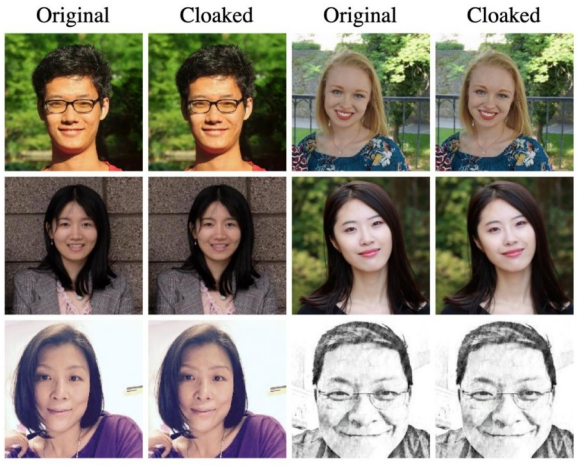
20. Ce logiciel gratuit modifie vos photos pour que vous ne soyez pas identifié par reconnaissance faciale

Vous voulez publier une photo de vous et vos amis sur Facebook sans que le réseau social ne reconnaisse vos visages et vous propose automatiquement de les identifier ? Ce nouvel outil gratuit devrait vous intéresser. Une équipe de chercheurs du SAND Lab, de l'Université de Chicago aux États-Unis, a mis au point un logiciel qui permet de déjouer les systèmes de reconnaissance faciale en altérant très légèrement les photos. Il est téléchargeable gratuitement et existe en deux versions, compatibles avec Mac ou Windows (http://sandlab.cs.uchicago.edu/fawkes/).

Baptisé « Fawkes » — un clin d'œil au masque de Guy Fawkes et au film « V comme Vendetta » —, cet outil rajoute à une photo des détails quasiment invisibles à l'œil nu, mais suffisants pour tromper l'intelligence artificielle qui ne peut plus reconnaître votre visage. Selon les chercheurs, le logiciel a déjà réussi à déjouer des systèmes de reconnaissance faciale de pointe, comme Microsoft Azure Face API, Amazon Rekognition et Face+++, avec un taux de réussite impressionnant de 100 %.

Comment ça marche ?

Fawkes utilise une technique appelée « cloaking » — en français « masquage » — qui consiste à berner les algorithmes de reconnaissance faciale en altérant la base de données de visages dont ils ont besoin pour fonctionner. Au lieu de détecter les traits habituels qui permettent d'identifier un visage précis, le système sera amené à repérer d'autres minuscules détails inventés de toutes parts par le logiciel.



Si vous modifiez une photo de vous à l'aide du logiciel et la publiez ensuite sur Facebook par exemple, le système de reconnaissance faciale détectera qu'il y a bien un visage sur la photo, mais ne sera pas capable de reconnaître qu'il s'agit du vôtre, grâce aux légères altérations créées par Fawkes.

Les chercheurs espèrent que les gens dans le monde entier se serviront de leur logiciel, d'où sa gratuité, car une utilisation massive permettrait de fausser plus efficacement les bases de données de photos des systèmes de reconnaissance faciale. Un algorithme pourrait alors avoir une centaine de photos différentes de vous dans sa base de données sans faire le lien entres elles ni réussir à vous identifier.

Le New York Times avait rapporté le 3 août que les altérations étaient tout de même visibles à l'œil nu sur certaines photos, mais les chercheurs ont depuis mis au point une nouvelle version du logiciel, pour corriger le problème. De quoi poster vos plus beaux selfies sans avoir peur d'être fiché dans une base de données.

Source
letemps.ch
Anouch Seydtaghia
20 février 2022

21. Aspirer 100 milliards de visages, le projet délirant de Clearview AI

L'entreprise new-yorkaise, pourtant visée par de nombreuses plaintes, poursuit le développement d'outils de reconnaissance faciale. Elle veut désormais atteindre les 100 milliards de visages dans sa base de données.

Ni les enquêtes d'autorités de régulation, ni les enquêtes pénales, ni les tentatives de régulation, ni les cris d'alarme de plusieurs ONG. Non, rien, absolument rien ne semble en mesure de freiner les projets délirants de l'entreprise new-yorkaise Clearview AI. Récemment, un article du *Washington Post* détaillait ses projets pour atteindre les 100 milliards de visages dans sa base de données, afin notamment de lancer de nouveaux services. Les risques de dérive sont déjà avérés.

Le nom de Clearview AI avait émergé il y a deux ans, lorsqu'une enquête du *New York Times* avait révélé la technologie développée par cette firme américaine. L'on apprenait alors que cette start-up avait aspiré les visages de 3 milliards de personnes sur Facebook, YouTube, Twitter, Instagram et des millions de sites de recrutement, d'information ou de paiement. Créée par un Australien, Hoan Ton-That, Clearview AI avait alors déjà vendu ses prestations à plus de 600 services de police aux États-Unis.

Tout le monde

Dans les jours qui avaient suivi, face à la colère suscitée par ces pratiques, la plupart des géants de la tech – hormis Amazon – avaient annoncé arrêter leurs projets de reconnaissance faciale. Mais en toute discrétion, Clearview AI a poursuivi ses projets. Et c'est donc grâce à un autre média, le *Washington Post*, que l'on découvre aujourd'hui ses nouvelles ambitions. Le journal américain a consulté des documents financiers rédigés par l'entreprise. La firme affirme être à bout touchant pour posséder dans ses bases de données 100 milliards de visages d'ici un an. Ce sera suffisant, selon Clearview AI, pour garantir que presque tout le monde sera identifiable à l'échelle mondiale.

Actuellement, la société posséderait plus de 10 milliards d'images dans sa base de données, auxquelles s'ajoutent 1,5 milliard de clichés supplémentaires chaque mois. Pour atteindre les 100 milliards de clichés, Clearview n'aurait besoin que d'un financement de 50 millions de dollars. C'est-à-dire presque rien.

Airbnb et Uber intéressés

L'entreprise ne veut pas se contenter de pouvoir identifier n'importe qui sur la base d'une image, ou d'un extrait de vidéo. Selon le *Washington Post*, elle envisage d'identifier des gens via l'analyse de leur démarche. Clearview AI n'exclut pas non plus de pouvoir… prendre des empreintes digitales à distance.

Utilisé par de nombreux services de police aux États-Unis – mais aussi par des entreprises, voire de célébrités, comme l'avait révélé le *New York Times* en 2020 – le logiciel de Clearview AI pourrait intéresser de nouveaux domaines. Dans un communiqué adressé au site Motherboard, l'entreprise affirme que les multinationales Airbnb, Lyft et Uber ont exprimé un intérêt pour ses services. S'agit-il de contrôler l'identité et de surveiller des travailleurs ? Ou des clients ? Ce n'est pas encore clair. Mais citer de tels clients potentiels montre que les tabous de 2020 n'existent sans doute plus en 2022 et que des usages commerciaux de masse de la reconnaissance faciale pourraient bientôt se

généraliser, aux Etats-Unis tout du moins.

Nombreux biais

Du point de vue de la sécurité, le directeur de Clearview se vante en affirmant que ses services ont permis d'identifier certains émeutiers qui avaient pris d'assaut le Capitole le 6 janvier 2021.

Mais des problèmes immenses pourraient survenir si ces systèmes étaient rapidement déployés à large échelle. Il y a bien sûr le risque d'une surveillance de masse, permanente. Et aussi le risque énorme de biais. Selon la société de recherche américaine eMarketer, « Clearview AI ne semble pas investir dans l'amélioration des algorithmes de reconnaissance faciale, qui sont connus pour leurs préjugés raciaux et leur imprécision, qui conduisent à de fausses arrestations. » eMarketer cite plusieurs études ayant démontré ces problèmes. Pour les femmes à la peau foncée, la technologie avait un taux d'erreur de 34,7 %, contre 0,8 % pour les hommes à la peau claire, selon une étude de 2018 du Massachusetts Institute of Technology.

Législation en retard

eMarketer note que «la législation et la réglementation commencent à rattraper l'utilisation de la technologie de reconnaissance faciale, qui pourrait déterminer que l'utilisation des bases de données sans le consentement des utilisateurs constitue une violation de la vie privée ».

Mais même si des enquêtes ont été lancées et des projets de loi élaborés, il y a le risque que les bienfaits supposés de la surveillance via la reconnaissance faciale l'emportent rapidement.

Source
letemps.ch
Anouch Seydtaghia
15 mars 2022

21.1. L'Ukraine utilise le sulfureux logiciel de reconnaissance faciale de Clearview AI

L'objectif du gouvernement de Kiev est d'identifier les Russes, morts ou vivants, sur son territoire. Clearview AI est toujours fortement critiquée pour son ambition d'aspirer 100 milliards de visages sur internet.

C'est une surprise. Fortement critiquée pour son système de reconnaissance faciale, l'entreprise américaine Clearview AI collabore depuis peu avec les autorités ukrainiennes. Son logiciel doit permettre d'identifier des Russes présents sur son territoire, qu'ils soient vivants ou décédés. Ce rapprochement entre les autorités ukrainiennes et la firme new-yorkaise a été initié par cette dernière qui, selon des révélations de l'agence Reuters, a offert ses services gratuitement au pays attaqué par la Russie.

L'Ukraine a commencé samedi à utiliser le logiciel de Clearview AI, notamment pour identifier des personnes aux barrages (checkpoints). Le but est d'identifier des Russes, sans doute pour démasquer des combattants infiltrés parmi les civils et voulant se livrer à des actes de sabotage. Le directeur de Clearview AI, Hoan Ton-That, a précisé qu'il n'offrira pas ses services aux autorités russes.

Identifier des agents russes

En utilisant ce logiciel américain, l'Ukraine pourra identifier les morts plus facilement qu'en essayant de faire correspondre des empreintes digitales, selon ce qu'a écrit Hoan Ton-That à Kiev. Sa lettre, vue par Reuters, indique que la reconnaissance peut être efficace même en cas de lésions faciales. Selon le directeur de Clearview AI, sa technologie peut être utilisée pour réunir des réfugiés séparés de leurs familles, identifier les agents russes et aider le gouvernement à détecter de faux messages publiés sur des réseaux sociaux.

Si Clearview AI est intéressante aux yeux des autorités ukrainiennes, c'est parce que l'entreprise américaine affirme avoir aspiré dans ses bases de données l'ensemble des photos du réseau social VKontakte. Ce dernier, racheté indirectement par les autorités russes fin 2021, compte environ 70 millions d'utilisateurs réguliers. Nettement plus populaire que Facebook – banni depuis une semaine en Russie –, VKontakte est ainsi une base de données précieuse pour Clearview AI.

Une simple app

Comme le démontrait en octobre dernier Hoan Ton-That au magazine *Wired*, sa société a développé une app pour comparer immédiatement un visage pris en photo par un téléphone avec sa base de données.

L'utilisation par l'Ukraine de cette technologie américaine peut potentiellement poser de gros problèmes. Ainsi, son système n'étant pas totalement fiable – comme tous les systèmes de reconnaissance faciale –, le risque est élevé que des personnes soient confondues, avec potentiellement des conséquences dramatiques.

Sans consentement

De plus, Clearview AI a acquis une partie importante de ses photos sans en demander l'autorisation aux réseaux sociaux (que ce soient VKontakte, Facebook, Twitter ou Instagram) et encore moins à leurs utilisateurs.

Aux Etats-Unis, Clearview AI fait l'objet de plusieurs plaintes liées à ces deux problématiques. Soutenant ces plaintes, l'organisation américaine Electronic Frontier Foundation (EFF) défendant les libertés individuelles écrivait ceci mi-février : « La reconnaissance faciale menace de plus en plus la justice raciale, la vie privée, la liberté d'expression et la sécurité de l'information. Nous demandons que les gouvernements cessent d'utiliser cette technologie dangereuse. » EFF demande par ailleurs que de nouvelles lois exigent des entreprises qu'elles obtiennent le consentement de la personne avant de prendre son empreinte faciale. Selon EFF, « l'un des pires contrevenants est Clearview AI, qui extrait les empreintes faciales de milliards de personnes sans leur consentement ».

Davantage de données

Fin février, la société new-yorkaise annonçait ses nouvelles ambitions au niveau mondial. La société veut ainsi détenir 100 milliards de photos différentes de visages dans sa base de données d'ici à un an. Cela signifierait une expansion massive des informations en sa possession: il y a deux ans, lorsqu'une enquête du *New York Times* avait mis en lumière les activités de Clearview AI, cette société avait alors aspiré les visages de trois milliards de personnes sur Facebook, YouTube, Twitter, Instagram et des millions de sites de recrutement, d'information ou de paiement.

Aujourd'hui, de nombreuses polices locales utilisent son système de reconnaissance faciale aux États-Unis. La Belgique a également employé ses services, a priori de manière expérimentale. De nombreux pays ont banni l'emploi des technologies de Clearview AI, mais on ne sait pas lesquels les utilisent, de manière régulière ou dans le cadre de tests.

Craintes en Suisse

Contacté mardi, l'Office fédéral de la justice (Fedpol) n'a pas répondu à nos questions. En 2020, un porte-parole de Fedpol affirmait que ce logiciel n'avait jamais été utilisé, et qu'il ne le serait pas à l'avenir, pour des raisons juridiques. Mais fin 2021, trois organisations (Amnesty International, AlgorithmWatch CH et Société Numérique) lançaient une pétition pour bannir, en Suisse, la reconnaissance faciale automatisée et la surveillance biométrique. Selon ces trois ONG, les forces de police suisses travaillent déjà avec des logiciels de reconnaissance faciale, alors même que la base légale est actuellement peu claire à ce sujet.