Le vrai visage de la reconnaissance faciale

La Quadrature du net – Juin 2019

Joy Buolamwini – Juin 2018

Le vrai visage de la reconnaissance faciale

La Quadrature du net - juin 2019

La Quadrature du Net est contre la reconnaissance faciale, d'accord : mais pourquoi ? Dès qu'on aborde le sujet en public, on voit se dessiner deux attitudes opposées. D'un côté, le solide bon sens qui ne voit pas pourquoi on se priverait de la possibilité d'identifier efficacement les criminels dans une foule, et pour qui tous les moyens sont bons, puisque la fin est juste. De l'autre côté, la peur réflexe devant cette technique de surveillance – souvent plus vive que devant d'autres techniques de surveillance pourtant très répandues – parce qu'elle est exploitée au cinéma comme outil d'un pouvoir policier totalitaire. C'est entre ces deux pôles, fantasme contre fantasme, qu'on peut essayer de comprendre les enjeux de la reconnaissance faciale.

Reconnaissance facile

Un·e terroriste est en fuite dans les rues d'une capitale : il suffit d'analyser en direct les images des caméras de surveillance de la ville pour læ situer en quelques minutes. Un·e enfant s'est perdu·e ? Vite, les caméras de tous les lieux publics sont interrogées, et l'enfant est retrouvé·e en moins d'une demi-heure.

Les personnes chargées de vendre des systèmes de reconnaissance faciale ne manquent pas d'imagination pour convaincre le grand public de l'efficacité de leurs produits. Le contexte sécuritaire, accentué par les attaques terroristes de 2015, entretenu par le personnel politique et amplifié par les médias de masse, leur ouvre un boulevard idéologique et des lignes de crédit généreuses.

Autant dire qu'en matière de fantasme, les partisan·es de la reconnaissance faciale généralisée ne sont pas en reste. Le seul fait que la surveillance permanente des rues et des espaces publics soit considérée comme une solution miracle à l'insécurité dans la société devrait suffire à disqualifier l'outil : il est incapable de répondre aux objectifs qu'on veut lui donner.

Comment ça marche ?

Il existe plusieurs types de reconnaissance faciale. Leur point commun, c'est un logiciel capable de repérer dans une image (photo ou vidéo) des structures de visage et de les comparer point à point avec d'autres images. Il faut ensuite distinguer deux formes de « reconnaissance ».

Si on compare les images avec d'autres images de la même source – les différents angles de vue dans une galerie commerciale, par exemple – alors on veut « identifier » quelqu'un·e : c'est-à-dire isoler une personne (« identique » à elle-même !) parmi d'autres et la suivre ainsi dans ses déplacements, soit parce qu'on estime qu'elle a un comportement suspect, soit pour renseigner la galerie commerciale sur le parcours de ses clients.

Quand on reconnaît les visages dans une foule pour les comparer à un jeu de visages de personnes recherchées, il s'agit aussi de les « identifier ».

En revanche, on, parle d'« authentification » quand on compare le visage d'une personne à un visage de référence. L'authentification est couramment utilisée comme système de déverrouillage : le visage saisi par la caméra doit correspondre à l'image enregistrée dans un badge (c'est le cas du système prévu pour les lycées de PACA) ou dans une base de données de personnes autorisées (par exemple à l'entrée d'une entreprise). C'est un procédé testé aussi pour le retrait d'argent à un distributeur, en renfort du PIN.

C'est le seul exemple où la reconnaissance faciale vise toujours à protéger la confidentialité des données et l'intimité de la personne : quand on choisit de déverrouiller son téléphone avec la reconnaissance faciale, c'est parce qu'on espère que personne d'autre ne pourra le faire.

L'identification est utilisée par la police pour reconnaître des personnes recherchées. On peut en voir un exemple concret et efficace sur le site d'Interpol.

Des exemples comme celui-ci alimentent le fantasme qui sous-tend la reconnaissance faciale : si on peut scanner toustes les passant·es et identifier celleux qui sont suspect·es, alors la criminalité reculera et la sécurité augmentera.

Méconnaissance faciale

Mais le moindre défaut de la reconnaissance faciale, c'est qu'elle ne marche pas très bien. On le sait parce que de nombreuses expériences sont conduites dans le monde, et que les résultats publiés sont assez étonnants, en comparaison des espoirs démesurés que suscite la technique.

La société SenseTime, en Chine, se vante par exemple de pouvoir identifier un individu qui commet une « incivilité » dans la rue, afin d'afficher son visage sur des écrans géants et le soumettre au mépris public. Mais une expérience menée aux États-Unis s'est conclue sur le constat que la reconnaissance faciale sur des automobilistes ne fonctionne pas encore.

LIST OF EVENTS AND DATES WHERE SOUTH WALES POLICE HAS USED AFR

Show 10 entries Search:

Event	Date	True-positives	False-positives	Incorrect police stops ('interventions')
UEFA Champions League Final Week (Cardiff Airport, Train station and City Centre)	29/05/2017 - 03/06/2017	173	2,297	TBC
Elvis Festival (Porthcawl)	23/09/2017 - 24/09/2017	10	7	1
Operation Fulcrum 'Day of Action' (Cardiff)	19/10/2017	5	10	2
Anthony Joshua v Kubrat Pulev Boxing (Cardiff)	28/10/2017	5	46	2
Wales v Australia Rugby (Cardiff)	11/11/2017	6	42	2
Wales v Georgia Rugby (Cardiff)	18/11/2017	1	2	0
Wales v New Zealand Rugby (Cardiff)	25/11/2017	3	9	2
Wales v South Africa Rugby (Cardiff)	02/12/2017	5	18	5
Kasabian Concert (Motorpoint Arena, Cardiff)	04/12/2017	4	3	0
Liam Gallagher Concert (Motorpoint Arena, Cardiff)	13/12/2017	6	0	0

Ce document fuité par la police britannique recense, pour chaque expérience de reconnaissance faciale (Event), le nombre d'identifications réussies (True-positives), le nombre de faux positifs (False-positives), et le nombre d'interpellations injustifiées (Incorrect police stops).

Nos collègues anglais de Big Brother Watch, au Royaume-Uni, qui militent notamment contre l'utilisation de la reconnaissance faciale, ont publié des chiffres à propos des expériences menées par la police britannique. Iels montrent que le taux de reconnaissance

est très bas, et que les « faux positifs », c'est-à-dire les identifications erronées, sont nombreuses. Certaines ont même entraîné des interventions infondées de la police.

La sécurité des forts

L'échec des identifications n'est pas imputable seulement à un défaut de la technique : le germe de l'échec est dans les personnes qui programment la reconnaissance faciale. Le logiciel qui analyse les visages et les compare à d'autres visages est dans la plupart des cas conçu par des hommes blancs. Surprise : la reconnaissance faciale des femmes et des personnes non-blanches atteint un taux d'échec et de faux positifs supérieur à la moyenne.

Que ses concepteurices le veuillent ou non, ce qu'on appelle « les biais de l'algorithme », ses effets indésirables, sont en réalité les biais cognitifs de celleux qui le conçoivent : le racisme et le sexisme de l'algorithme dérivent du racisme et du sexisme institués par la société, et consciemment ou inconsciemment reproduits par les concepteurices de ces outils.[1]

Dans le cadre d'un usage policier de la reconnaissance faciale, les personnes les plus faibles socialement seront ainsi plus souvent victimes d'erreurs policières que les autres.

Société de contrôle

Les philosophes Michel Foucault et Gilles Deleuze ont défini de façon très précise plusieurs types de coercitions exercées par les sociétés sur leurs membres : ils distinguent en particulier la « société disciplinaire » (telles que la société en trois ordres d'Ancien Régime ou la caserne-hôpital-usine du XIXe siècle) de la « société de contrôle » qui est la nôtre aujourd'hui.

Dans une « société de contrôle », les mécanismes de coercition ne sont pas mis en œuvre par des autorités constituées qui les appliquent au corps social par contact local (autorité familiale, pression hiérarchique dans l'usine, surveillant de prison, etc.), mais sont incorporés par chacun·e (métaphoriquement et littéralement, jusqu'à l'intérieur du corps et de l'esprit), qui se surveille ellui-

[1] Voir article suivant.

même et se soumet à la surveillance opérée par d'autres points distants du corps social, grâce à une circulation rapide et fluide de l'information d'un bord à l'autre de la société.[2]

Qui peut souhaiter d'être soumis·e à un contrôle dont les critères lui échappent ? C'est pourtant ce que nous acceptons, en laissant s'installer partout la vidéosurveillance et la reconnaissance faciale.

La mairie de Nice, dirigée par Christian Estrosi (LR), a fait scandale au printemps 2019 en organisant une expérience lors du carnaval de la ville. Sur la base du volontariat, certaines personnes préalablement identifiées devaient être reconnues dans la foule. Mais la ville de Nice envisage d'aller plus loin, en authentifiant les passager·es du tramway dont le comportement serait « suspect ».

Qu'est-ce qui définit un comportement suspect ? Avoir un type maghrébin et un sweat à capuche entre sûrement dans les critères. Mais quoi d'autre ? Une expression faciale fermée, une nervosité visible ? Quelles émotions sont-elles considérées comme étant un danger pour la société ? Où peut-on consulter la liste ? On voit bien la part fantasmatique et arbitraire qui fonde tout projet d'anticiper la criminalité.

Sous prétexte que « prévenir vaut mieux que guérir », on organise en réalité, dans des usages quotidiens bien réels et valables dès aujourd'hui, une inversion générale de la charge de la preuve.

En temps normal, la police judiciaire doit rassembler par l'enquête des preuves à charge pour inculper quelqu'un·e. C'est à l'accusation de faire la preuve de la culpabilité du suspect. Ce travail est collectif, encadré par une procédure et un tribunal.

En revanche, sous l'œil de la caméra et face aux algorithmes de reconnaissance faciale, c'est à chacun·e que revient, à tout instant et en tout lieu, la charge de prouver son innocence. Comment ? En offrant son visage à l'identification et en adoptant un comportement qui ne déclenchera aucune alarme au fond d'un ordinateur de la police.

[2] http://1libertaire.free.fr/DeleuzePostScriptum.html

La loi de l'œil

On peut penser qu'il s'agit, sous nos yeux, d'un choix de société délibéré. En l'absence de cadre juridique clair, les dispositifs de reconnaissance faciale s'installent dans la hâte, avec un effet immédiat : chacun·e intériorise la contrainte de la surveillance et adapte insensiblement son comportement à ce regard abstrait. Il est psychologiquement naturel et moins coûteux de s'y plier, même avec une ironie protectrice, plutôt que de remettre en cause les décisions arbitraires qui sont imposées sans discussion.

L'intériorisation de la surveillance, la culpabilité par défaut, s'accompagnent d'un ajustement inconscient à une loi non écrite. C'est l'effet Hawthorne, sorte d'effet placebo mental : savoir qu'on est surveillé modifie l'attitude. La surveillance n'a pas besoin de punir chaque individu pour s'exercer sur tous.

Refuser la reconnaissance faciale est une première nécessité, l'encadrer par la loi écrite aussi.

Éducation au contrôle

Pourquoi vouloir installer un dispositif de reconnaissance faciale à l'entrée d'un lycée ? C'est en cours à Marseille et à Nice, un projet encore porté par monsieur Estrosi, et combattu par La Quadrature du Net. Quel intérêt, alors que des surveillant·es à l'entrée de l'établissement pourraient tout aussi bien reconnaître les élèves autorisé·es, repérer les intru·ses, et affronter les problèmes éventuels avec humanité ? La réponse est triste : parce que la machine est censée être moins chère.

La dépense s'amortit en quelques années et les services publics croient faire ainsi des économies, dans un contexte général où les problèmes sociaux sont délégués à l'entreprise privée ou plus souvent laissés à l'abandon, et abordés sous l'angle unique de la répression.
L'installation de caméras est le signe assez sûr d'une politique qui a baissé les bras. La reconnaissance faciale pousse seulement le curseur plus loin dans la prise en charge des relations humaines par des arbres de décisions préprogrammés. On renonce ostensiblement à l'ambition de construire une société.

Bénéfices et usage commerciaux

Les bénéfices attendus de la reconnaissance faciale sont en grande partie des mesures d'économie : moins de personnel pour surveiller de plus grandes surfaces urbaines, et un meilleur ajustement des moyens d'interventions. Les expériences de « safe city » menées aux États-Unis (Chicago, Detroit, en particulier) avaient par exemple pour but de mieux définir les quartiers et les rues où les patrouilles devaient circuler, en fonction des heures de la journée et même des saisons, pour être au plus près des faits de délinquances à réprimer. Dans la logique de la moindre dépense et de la réduction des effectifs, il faut bien « optimiser » le temps de présence des agents et le peu de moyens dont on dispose. Malheureusement, le raisonnement est faussé : les dispositifs techniques de vidéosurveillance exigent un entretien très coûteux. Les communes ne feront aucune économie, et financent les caméras avec des sommes qui manquent cruellement sur d'autres lignes de leur budget. Entre temps, elles auront supprimé un certain nombre de salarié·es.

Mais il ne faut pas perdre de vue que la reconnaissance faciale est également un « marché » aux bénéfices importants.

Pour l'heure, les entreprises se livrent à une course pour concevoir les outils et trouver des villes où les essayer. Ça tombe bien, les villes sont en demande : des appels d'offre plus ou moins transparents sont donc lancés un peu partout en France, alors que la transparence des décisions finales est inexistante, et tandis que les communes sabrent les subventions, l'argent magique ne semble pas manquer pour payer des « solutions » sécuritaires à grand frais, en vue des échéances électorales qui approchent.

Derrière l'engouement pour la vidéosurveillance et la reconnaissance faciale, on voit une convergence d'intérêts entre un agenda politique qui joue volontiers sur la corde de la sécurité publique, et des entreprises qui cherchent à s'emparer de l'immense marché municipal qui s'ouvre à elles, en France d'abord, et dans le monde ensuite.

Le profit à tirer de la reconnaissance faciale ne s'arrête pas là. On voit la technique s'installer aussi dans des centres commerciaux.

Les caméras sont le plus souvent cachées dans les panneaux d'informations qui affichent le plan de la galerie commerciale, comme au Québec ou dans des « totems » qui affichent des vidéos publicitaires. Les réactions des passant·es sont épiées : quelles images retiennent leur attention, quelles boutiques envisagent-iels de visiter, quels sont leurs déplacements, etc. Le but étant bien sûr d'offrir aux visiteur·euses « la meilleure expérience possible »…

À aucun moment le consentement des passant·es n'est demandé, et on ne voit pas bien comment il pourrait l'être, sauf à leur donner le choix entre subir la vidéosurveillance ou quitter les lieux. Devra-t-on bientôt faire ses courses avec un sac sur la tête ?

La question du consentement est centrale dans la protection des données personnelles et de la vie privée, elle est d'ailleurs au centre des exigences du RGPD. Ce n'est donc pas un argument léger. Les lois européennes disent aussi que le consentement ne peut pas être obtenu en échange d'un service qui reviendrait à lui donner une valeur marchande : justifier la reconnaissance faciale dans les galeries commerciales en prétextant que les client·es auront de meilleurs prix ou de meilleures offres n'est pas un argument recevable. C'est au pire un cache-misère pour l'avidité sans limite des marchands, qui traitent tous les passant·es comme des proies.

Les utilisations commerciales ou municipales de la reconnaissance faciale prospèrent dans une faille juridique : le phénomène est mal encadré, alors qu'il devrait faire l'objet d'un débat collectif. Mais la sécurité policière et la prospérité des entreprises commerciales sont devenues dans le monde entier l'alpha et l'oméga des politiques publiques.

La possibilité d'interdire

Les personnes les mieux averties des applications de la reconnaissance faciale sont tellement inquiètes qu'elles demandent un encadrement juridique de cette technique. C'est la leçon qu'on peut tirer de la lecture des articles écrits par Brad Smith, juriste de Microsoft. En juillet 2018, il appelait le gouvernement américain à légiférer sans délai pour encadrer les usages de la reconnaissance faciale. Bien placé pour constater les progrès de la technique, il redoute avec gravité qu'elle puisse être utilisée contre les libertés

des personnes, aussi bien par des entreprises privées que par des États. En décembre 2018, il pose quelques jalons pour délimiter le contour de cet encadrement.

On n'est pas obligé de partager son enthousiasme pour certaines applications « positives » de la reconnaissance faciale, dont il donne quelques exemples qui mériteraient d'être regardés de plus près (dans la recherche médicale par exemple). Mais on peut entendre son inquiétude, parce qu'elle n'est pas celle d'un militant habitué à crier au loup : au plus haut niveau de décision, là où une vision panoramique peut embrasser à la fois la connaissance du droit et la connaissance des projets techniques réels, on n'en mène pas large, et ce n'est pas bon signe.

Toutefois, l'empressement de Brad Smith à voir naître une réglementation peut aussi être lu différemment, quand on le rapproche des déclarations récentes de Andy Jassy, président de Amazon Web Services, qui développe le logiciel Rekognition. Il se trouve qu'entre les articles de Brad Smith et l'interview de Andy Jassy, un événement important est survenu : la ville de San Francisco, en Californie, au plus près de la Silicon Valley et des grands sièges des multinationales du numérique, a voté le 14 mai 2019 une décision interdisant à la police locale d'utiliser la reconnaissance faciale. Amazon veut une réglementation parce que l'interdiction pure et simple ne fait pas de bien à ses affaires…

Quant à nous, nous retiendrons qu'il est possible d'interdire les pratiques de surveillance de masse, par la délibération locale et par la loi.

Le visage perdu

La reconnaissance faciale change le visage du monde. Il n'est pas nécessaire de renvoyer aux pires dystopies et à *1984* pour voir tout ce que les pratiques actuelles ont de dangereux. On peut même percevoir un changement anthropologique possible dans le rapport avec le visage.

La reconnaissance faciale attribue au visage, non plus une valeur de personnalité, l'expression même de la singularité d'une personne humaine, mais une fonction de dénonciation : le visage ne

vaut plus pour lui-même, comme singularité prise avec son épaisseur et son secret, mais comme simple signe en lien avec des bases de données de toutes sortes qui permettent de prendre des décisions concernant la personne visée, à son insu.

Dans ce contexte, le visage devient l'identifiant unique par excellence, plus encore que la carte d'identité. Lors de l'expérience du carnaval de Nice, la ville se vantait même d'avoir pu identifier un cobaye dont la photo de référence datait de trente ans. Le visage comme mouchard, le visage qui trahit, merveilleux progrès.

On peut s'opposer à un prélèvement d'ADN. Mais comment s'opposer aux photos de soi ? Facebook applique un logiciel de reconnaissance faciale aux photos postées par ses utilisateurs. Si un « ami » n'est pas reconnu, le site invite même les utilisateurs à identifier leurs proches. Même en n'ayant jamais eu de compte Facebook, vous figurez peut-être dans cette immense base de données, et Facebook sait mettre votre nom sur votre visage, et vous reconnaître parmi toutes les nouvelles photos postées par vos amis…
Malgré vous, votre visage a un sens pour les caméras qui vous filment. Les pseudo-sciences du 19e siècle prétendaient lire des traits psychologiques dans les traits du visage. Aujourd'hui, chaque visage dans la rue porte un casier judiciaire, un nom, des relations, des opinions exprimées sur les réseaux sociaux, des habitudes de consommation, des engagements divers, et qui sait quoi d'autre encore.

Quand les inconnu·es qui vous croisent dans la rue peuvent accéder à des données sur vous par le simple fait que l'image de votre visage a été captée par des Google Glasses, on amène la puissance coercitive du réseau jusque dans la rue. Sur le réseau, il est possible de prendre plusieurs identités. Mais nos prises de position politiques, notre réseau amical, notre réseau professionnel, notre CV, etc., se retrouvent, dans la rue, associés à un élément unique, visible, et facilement accessible à tous. Les créateurs des Google Glasses ont fini par interdire cette possibilité, pour ne pas tuer leur création dans l'œuf. Si cette technique devenait courante, qui peut assurer que nous n'assisterons pas à l'avènement d'une

époque qui supprimera totalement l'anonymat dans l'espace public ?

Une société de la défaite

Une anthropologue britannique, Sally A. Applin, a récemment publié un article très intéressant sur les dégâts sociaux causés, et surtout révélés, par la reconnaissance faciale[3]. Elle part de la question posée par un dirigeant d'entreprise américain sur Twitter : « Vivons-nous vraiment dans une société aussi dangereuse, pour avoir à ce point besoin de la reconnaissance faciale ? », et la précise : la reconnaissance faciale, pour quoi faire ?

Elle évoque bien sûr les intérêts industriels, et la facilité politique consistant à remplacer le personnel humain par des machines. Mais elle va plus loin : derrière le succès politique et médiatique de la technique à visée sécuritaire, elle voit la peur de l'autre. Le regard remplace la parole, et la distance remplace la rencontre. Même les agents de surveillance ne regardent plus les gens, mais des écrans. Ce qui devrait être un média est devenu une vitre isolante. C'est une logique de traitement des symptômes qui ne s'adresse jamais aux causes.

Elle remarque aussi que la « démocratisation » des caméras, maintenant que chacun porte sur soi un smartphone, a sans doute aussi contribué à leur banalisation, en faisant de chacun le surveillant potentiel de l'autre. C'était d'ailleurs l'idée principale de l'application « Reporty », retoquée à Nice par la CNIL au printemps 2018 : la mairie voulait lancer une application pour smartphone afin que les habitants signalent par vidéo les incivilités dont ils seraient témoins. Sally A. Applin souligne par ailleurs que l'accumulation de millions d'heures de vidéosurveillance que personne n'a le temps de regarder explique peut-être en partie l'enthousiasme des décideurs politiques pour la reconnaissance faciale automatisée : le fantasme de la surveillance totale est matériellement hors d'atteinte, sauf si l'humanité s'y consacre à temps plein, ou si elle délègue le travail à des machines (biaisées).

[3] https://www.fastcompany.com/90336549/the-creeping-threat-of-facial-recognition

Est-ce vraiment le monde que nous voulons ? Cette société sans contact, cette société qui a peur de la parole et de l'engagement physique des uns avec les autres est une société déprimée, qui ne s'aime pas. Il est permis d'en vouloir une autre. Elle commence par interdire la reconnaissance faciale.

*

When the Robot Doesn't See Dark Skin

Les robots ne voient pas les peaux noires

Joy Buolamwini – The New York Times – Juin 2018

Quand j'étais étudiante et que j'utilisais un logiciel de détection faciale basé sur une intelligence artificielle, le robot que j'ai programmé ne pouvait pas détecter mon visage à la peau sombre. J'ai dû emprunter le visage blanc de ma·on colocataire pour terminer mon projet. Plus tard, quand je travaillais sur un autre projet au Media Lab du MIT, j'ai dû me résoudre à porter un masque blanc afin que ma présence soit reconnue.

Mon expérience rappelle que l'intelligence artificielle, dont on loue souvent le potentiel de changer le monde, peut en réalité renforcer les préjugés et l'exclusion, même quand elle est utilisée avec les meilleures intentions.

Les systèmes d'intelligence artificielle sont façonnés par les priorités et les préjugés – conscients et inconscients – des gens qui les conçoivent, un phénomène que j'appelle « le regard codé ». Des études démontrent que les systèmes automatisés que l'on utilise pour rendre des sentences produisent des résultats biaisés contre les personnes noires, et que ceux que l'on utilise pour cibler les publicités sur internet peuvent discriminer sur la base du genre ou de la race.

Spécifiquement, lorsqu'il s'agit de biais algorithmique dans les technologies d'analyse faciale – mon domaine de recherche et l'un

des points focaux de mon travail avec l'Algorithmic Justice League – le fait que l'appli photo de Google étiquette des personnes noires dans des photos comme étant des « gorilles » et que les logiciels d'analyse faciale marchent bien pour des hommes blancs mais moins bien pour le reste du monde en sont des exemples malheureux.

Aussi dérangeants qu'ils soient, ils ne reflètent pas l'entièreté des risques de cette technologie qui est de plus en plus utilisée par les forces de l'ordre, la police aux frontières, la surveillance dans les écoles et le recrutement.

Les produits d'une entreprise du nom de HireVue, qui sont utilisés par plus de 600 entreprises dont Nike, Unilever et même les écoles publiques d'Atlanta, permettent aux employeurs de filmer des entretiens d'embauche et d'utiliser de logiciels d'intelligence artificielle pour noter les vidéos de chaque candidat selon des indices verbaux et non-verbaux. L'objectif de l'entreprise est de réduire l'impact des biais dans le recrutement.

Mais voilà le piège : les notes du système, selon un journaliste de Business Insider qui a testé le logiciel et discuté des résultats avec le responsable technique de HireVue, reflètent les préférences passées des recruteurs. Donc si une plus grande proportion d'hommes blancs aux comportements sensiblement similaires ont été embauchés par le passé, il se peut que les algorithmes soit entrainés à mieux noter les candidats masculins à la peau claire tout en pénalisant les femmes et les personnes racisées qui ne produisent pas les même indices verbaux et non-verbaux.

Il a été prouvé plusieurs fois que même sans technologie, les gens prennent des décisions de recrutement en faveur des candidats blancs et masculins, toutes choses égales par ailleurs. Sachant cela, l'idée de laisser la notation des candidats à la technologie est compréhensible. Mais comment savoir qu'un·e candidat·e qualifié·e dont les signaux verbaux et non-verbaux liés à l'âge, le genre, l'orientation sexuelle ou la race diffèrent de ceux des bons exemples utilisés dans l'entraînement de l'algorithme ne sera pas noté·e moins bien qu'un·e candidat·e similaire qui ressemble davantage à la sélection ? Nous ne le saurons pas sans tester à plusieurs reprises la technologie et son application.

Les tests que l'on a effectués sur les technologies d'analyse faciale soulèvent des questions. En collaboration avec l'expert en vision informatique Timnit Gebru, j'ai enquêté sur la précision des technologies d'analyse faciale d'IBM, Microsoft et Face++. Sur une tâche simple telle que de deviner le genre d'un visage, toutes les technologies ont eu de meilleurs résultats avec les visages masculins que féminins et on eut particulièrement du mal avec les visages de femmes africaines à la peau sombre. Dans le pire des cas, la technologie était 34% moins fiable pour les femmes noires que pour les hommes blancs.

Considérant la facilité avec laquelle les technologies d'analyse faciale semblent recréer les préjugés de race et de genre, les entreprises qui utilisent HireVue, si elles souhaitent prendre des décisions plus justes, devraient vérifier leurs systèmes afin de s'assurer qu'il n'amplifie pas les préjugés sur lesquels se sont basées les décisions de recrutement antérieures. Il est possible que les entreprises qui utilisent HireVue soient un jour trainées en justice du fait que le logiciel ait eu un impact négatif sur les candidatures de femmes et de personnes issues de minorités, ce qui est contraire au Titre VII de la loi sur les droits civiques.

Les risques liés aux biais des technologies d'analyse faciale vont au-delà du recrutement. Selon le Center on Privacy and Technology de l'université de droit de Georgetown, les visages de la moitié de tou·tes les adultes des Etats-Unis – plus de 117 millions de personnes – sont actuellement dans des réseaux de bases de données de reconnaissance faciale qui peuvent être consultés par la police sans mandat. Ces recherches se basent souvent sur des technologies de reconnaissance faciale qui n'ont pas été testé pour leur fiabilité sur différents groupes de personnes. C'est important car une erreur d'identification peut faire subir à des personnes innocentes des enquêtes policières ou des mises en examen erronées.

Dans le cas de la région de Galles du sud (South Wales), où Big Brother Watch rapporte qu'entre mai 2017 et mars 2018 les visages de plus de 2400 personnes innocentes mal identifiées ont été stockés par la police sans leur consentement, la police a reporté un taux de faux positifs d'identification faciale de 91 pour cent.

Mais il faut se souvenir que même si le taux de faux positifs s'améliore, l'usage injuste de la technologie de reconnaissance faciale ne peut être résolu par un nouveau patch du logiciel. Même la reconnaissance faciale précise peut être utilisée de façon problématique. La police de Baltimore a utilisé des technologies de reconnaissance faciale pour identifier et arrêter des personnes qui se sont rendues aux manifestations de 2015 contre les violences policières qui ont suivi la mort de Freddie Gray à Baltimore.

Nous devons faire face au développement de l'utilisation de cette technologie, et certains progrès ont été faits déjà. L'American Civil Liberties Union (ACLU) demande à Amazon d'arrêter de vendre des technologies de reconnaissance faciale aux forces de l'ordre et conteste l'utilisation de la reconnaissance faciale dans les véhicules utilisé par le Vehicle Face System qui est testé à la frontière Etats-Unis-Mexique. Bien que les législateur·ices du Texas, de l'Illinois et de la Californie aient entrepris de réguler la technologie de reconnaissance faciale, aucune loi fédérale n'existe. Cependant, il existe une esquisse. Un rapport de 2016 de l'université de droit de Georgetown formule une proposition de loi fédérale. Le pouvoir législatif devrait l'adopter.

Nous pouvons également prendre exemple sur ce qui existe à l'international. Le Canada a un statut fédéral régissant l'utilisation de données biométriques dans le secteur privé. Les entreprises telles que Facebook et Amazon doivent obtenir le consentement informé des citoyens pour obtenir leurs informations faciales uniques. Dans l'Union Européenne, l'article 9 du règlement général sur la protection des données (RGPD) demande le consentement exprimé explicite pour collecter des données biométriques des citoyen·nes européen·nes.

Tout un chacun doit soutenir les législateur·ices, les activistes et les développeur·euses de technologie d'intérêt public en exigeant la transparence, l'équité et la responsabilisation dans l'usage des intelligences artificielles qui gèrent nos vies. La reconnaissance faciale influe de plus en plus sur nos vies, mais nous avons encore le temps de l'empêcher d'accentuer les inégalités sociales. Pour cela, nous devons faire face au regard codé.