01 NET
Pays : FR
Périodicité : Bimensuel
OJD : 95662

Date : Du 20 mai au 02 juin 2020
Page de l'article : p.30-32
Journaliste : Yves Marzio

Comprendre contre-enquête

DANS L'ŒIL DES CAMÉRAS

La reconnaissance faciale est devenue la norme en Chine. Les citoyens sont surveillés 24h/24 et peuvent être verbalisés au moindre faux pas. Dans un contexte de menace sanitaire et terroriste, la France s'intéresse aussi à ces technologies. Souriez, vous êtes filmés… et identifiés !

Connaissez-vous NtechLab? En janvier 2020, cette société russe a été mandatée par la mairie de Moscou pour relier 100 000 des 170 000 caméras de vidéosurveillance de la ville à leur système de reconnaissance faciale. «*La probabilité d'une erreur de notre algorithme dans la reconnaissance des visages est de 1 sur 15 millions*», se targuait à l'AFP son directeur général Alexandre Minine. Crise sanitaire Covid-19 oblige, Serguei Sobianine, maire de la capitale russe, a annoncé que le système veillerait au bon respect du confinement. En janvier, la police londonienne annonçait, quant à elle, le déploiement de la reconnaissance faciale dans certains lieux stratégiques de la capitale pour identifier des individus fichés. Qu'en est-il en France à l'heure où des drones munis de caméras survolent des passants pour leur diffuser des messages de prévention dans le cadre de l'épidémie de coronavirus? Le basculement dans une société dystopique à la *Minority Report* est-il inéluctable?

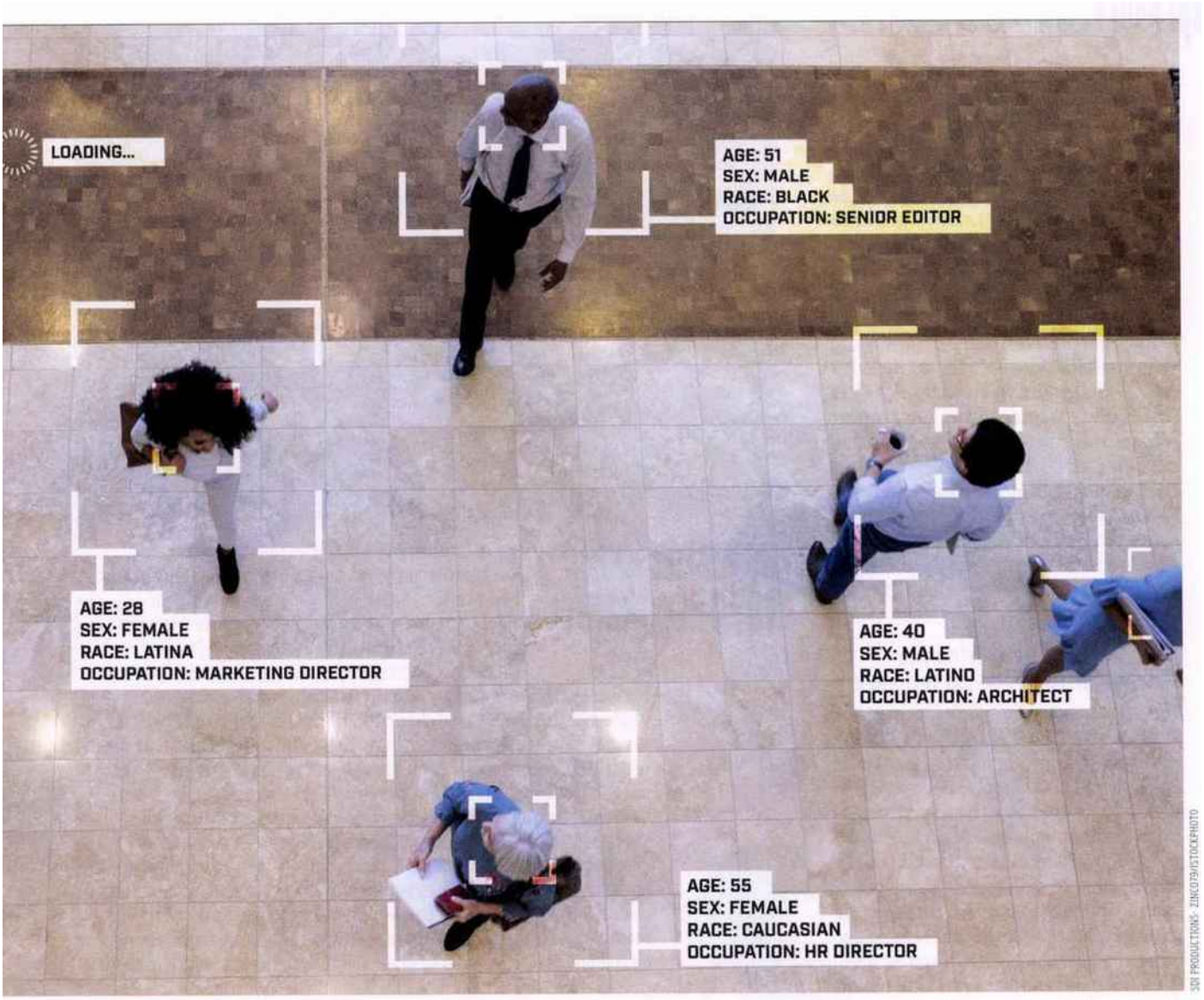
«*À la Commission nationale de l'informatique et des libertés* (Cnil), *nous observons une hausse des demandes de projets d'expérimentation de la reconnaissance faciale*», reconnaît Félicien Vallet, ingénieur. Néanmoins, les lois européennes ne permettent pas le déploiement tous azimuts de cette technologie. Ce cadre légal dépend essentiellement des usages. Or, la reconnaissance faciale englobe une multitude d'applications allant du déverrouillage de son smartphone, à l'identification d'un terroriste dans une foule, en passant par l'authentification des voyageurs dans les aéroports. Pour la Cnil, toutes ces utilisations «*ne soulèvent pas les mêmes enjeux, notamment en termes de contrôle des personnes sur leurs données*».

De la simple authentification à l'enfer orwellien

À cet égard, il faut distinguer deux applications: l'authentification et l'identification. Dans le premier cas, le système vérifie si vous êtes bien celui ou celle que vous prétendez être. L'illustration la plus parlante est le système Parafe du contrôle de l'immigration des aéroports parisiens. Une caméra filme votre visage et le compare à la photo de votre passeport. Si les deux coïncident, vous êtes authentifié. Dans le second cas, une caméra vous filme (cela peut être à votre insu, notamment dans la rue), et un algorithme extrait les caractéristiques de votre visage – ou gabarit – et le compare à des dizaines de milliers d'autres préenregistrés dans une base de données biométriques centralisée. Le système fait alors la correspondance et vous identifie.

Si l'intelligence artificielle sous-jacente est similaire dans les deux cas (voir encadré p.32), l'exploitation des données est radicalement différente. «*Dans le cadre d'une authentification, vos données biométriques sont stockées sur votre passeport dont vous êtes le seul détenteur. En revanche, l'identification nécessite que les caractéristiques biométriques de votre visage et votre identité soient enregistrées au préalable dans une base*», insiste Jean-Luc Du-

par **Yves Marzio**



gelay, professeur à l'école d'ingénieur Eurecom, à Sophia Antipolis (Alpes-Maritimes). Or, en France, la base de données TES (titres électroniques sécurisés) rassemble d'ores et déjà les données biométriques de tous les détenteurs de cartes d'identité et de passeports, notamment l'image numérique du visage et l'empreinte digitale.

Toutefois, le règlement européen sur la protection des données (RGPD) et la directive « police-justice » considèrent ces données comme sensibles, à l'image de celles relatives aux opinions politiques, à l'orientation sexuelle, aux croyances religieuses et à la santé. À ce titre, le traitement de données biométriques pour identifier une personne est interdit en France, à quelques exceptions près. Notamment si la personne donne son consentement ou si l'intérêt public le requiert, comme en cas de menace pour la sécurité publique: « *La reconnaissance faciale doit alors être autorisée par un texte de loi, par exemple un décret en Conseil d'État, pris après avis de la Cnil* », précise Félicien Vallet. Quoi qu'il en soit, la mise en place d'une banque de données biométriques est particulièrement problématique. Notamment pour son potentiel autoritaire et liberticide.

CE QUE LE GOUVERNEMENT APPELLE « L'ŒIL CÉLESTE », IDENTIFIE EN PERMANENCE LES CITOYENS CHINOIS

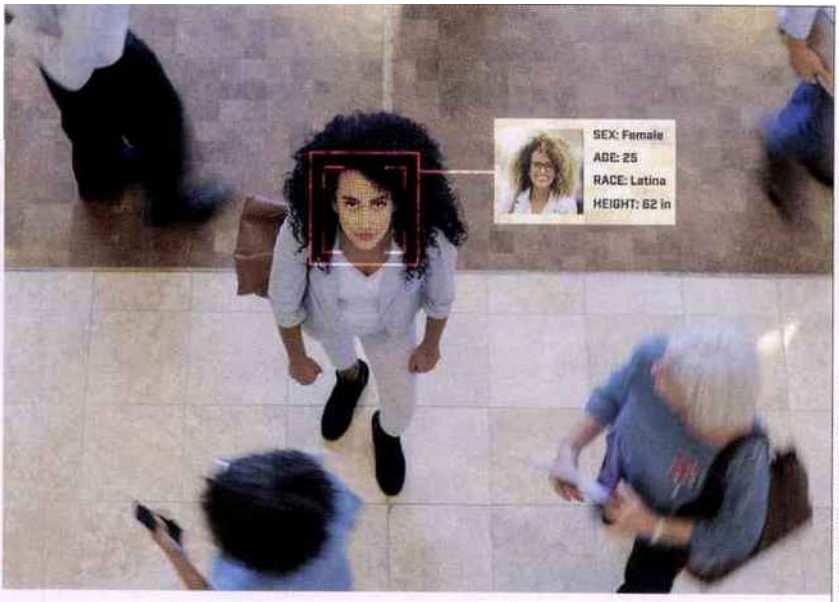
« *De fait, les caméras de surveillance associées à la reconnaissance faciale permettent un traitement à distance, donc potentiellement à l'insu de la personne. Par essence, il peut y avoir un risque de dérive* », prévient Félicien Vallet. Rappelons qu'à Pékin, les passants qui traversent en dehors des clous sont reconnus par les caméras et verbalisés en direct. À chaque coin de rue, ce que le gouvernement appelle « l'œil céleste », identifie en permanence les citoyens chinois. De nombreuses associations, comme la Quadrature du Net en France, dénoncent fermement la centralisation de ces données sensibles, porte d'entrée vers la reconnaissance faciale de masse et l'enfer orwellien.

Cela n'empêche pas quelques expérimentations. En février 2019, la mairie de Nice (Alpes-Maritimes) a ainsi testé la reconnaissance faciale lors du célèbre carnaval de la ville. Cinquante volontaires, des salariés, ont donné leur consentement et ont fourni des photographies de leur visage pour tester si les caméras de vidéosurveillance à l'entrée du carnaval étaient en mesure de les identifier « à la volée » dans la foule. Dans son rapport d'expérimentation, la mairie est dithyrambique sur l'efficacité du dispositif, mis en place par l'entreprise israélienne AnyVision, éditeur de logiciel de reconnaissance faciale. La Cnil reste cependant sceptique sur la pertinence du test niçois et regrette le manque de détails techniques du rapport.

La SNCF a expérimenté des algorithmes de surveillance

« Les pourvoyeurs de logiciels de reconnaissance faciale présentent toujours l'efficacité de leur dispositif sous leur meilleur jour. Pourtant aucun dispositif n'est fiable à 100 % », insiste Kévin Bailly, chercheur à l'Institut des systèmes intelligents et de robotique, à Paris. Plusieurs éléments limitent la fiabilité de la reconnaissance faciale : l'éclairage, l'occultation du visage (port de lunettes, de masque, d'une barbe), la différence d'âge entre le moment où la personne est identifiée et l'âge sur sa photo, et l'orientation du visage. Dans des situations très contrôlées comme dans les portiques des aéroports où le visage est de face, dans des conditions idéales de luminosité, la fiabilité est très bonne, mais dès lors qu'on est dans un environnement urbain, la qualité d'identification se dégrade. *« Prenons l'exemple de l'identification de terroristes fichés au milieu d'une foule,* propose Jean-Luc Dugelay. *Même si un constructeur vous dit que son système a une efficacité de 99 %, cela signifie qu'une personne sur cent sera reconnue à tort comme terroriste. »*

Les technologies de vidéosurveillance de masse ne s'arrêtent d'ailleurs pas à la reconnaissance faciale. Sans utiliser de données biométriques, les algorithmes peuvent également déterminer l'âge et le sexe des individus. Et alors que les villes intelligentes se développent, les industriels sont de plus en plus nombreux à proposer des caméras intelligentes, capables de détecter des « comportements suspects », c'est-à-dire statistiquement inhabituels pour un contexte donné. Au Japon, la start-up Earth Eyes Corp a ainsi développé un logiciel capable de repérer les vols à l'étalage dans les supermarchés et d'informer le personnel de sécurité. En France, fin 2019, la SNCF a expérimenté, dans une relative discrétion, des algorithmes capables de détecter des bagages abandonnés, de repérer des vendeurs à la sauvette, de signaler la présence d'un intrus dans une zone interdite au public, ou de reconstruire le parcours d'usagers (volontaires) dans ses gares. À Toulouse (Haute-Garonne) ou dans le département des Yvelines, les collectivités se sont dotées d'un réseau de caméras intelligentes, tandis qu'à Valenciennes (Nord), le géant Huawei a offert 217 caméras à la mairie de la ville pour expérimenter son projet Safe City : zoom haute définition, vision nocturne, détection des mouvements de foule, des objets abandonnés et des situations inhabituelles… Ces dispositifs pourront prévenir les services de police au moindre mouvement suspect. En 2019, dans un document intitulé *Reconnaissance faciale : pour un débat à la hauteur des enjeux*, la Cnil rappelait la nécessité *« d'intégrer dans l'équation la possibilité de combiner, dans la pratique, ces différents dispositifs, avec pour effet une démultiplication de leur impact pour les personnes. »* Un avenir potentiel où nos libertés individuelles pourraient être mises à mal.●



SDI PRODUCTIONS - ZINKOTHEK/ISTOCKPHOTO

COMMENT UNE IA VOUS RECONNAÎT

Les caméras en elles-mêmes sont incapables de reconnaître un visage. Elles transmettent un flux vidéo à un ordinateur qui l'analyse au moyen d'un algorithme de *deep learning*. Celui-ci utilise un réseau de neurones artificiels dont l'architecture s'inspire du cerveau. En très grand nombre, ces neurones peuvent réaliser des tâches complexes comme reconnaître un objet dans une image. C'est notamment ce qu'utilise Google Images pour agréger les résultats des requêtes des internautes. Mais avant d'être implémenté dans un logiciel de reconnaissance faciale, l'algorithme subit un entraînement sur une base de données de dizaines de milliers de photographies de visages dont l'identité est renseignée. Essai après essai, il corrige ses erreurs d'identification en ajustant la force de la connexion entre chaque neurone. Au terme de cet apprentissage, l'algorithme aura appris à en extraire les caractéristiques pertinentes - ou gabarits - qui permettent de différencier les individus. De quoi l'utiliser enfin dans un logiciel de reconnaissance faciale. La qualité de ce logiciel dépend essentiellement du nombre, de la richesse, et de la variabilité des données d'entraînement.