

La banalisation de la reconnaissance faciale : un enjeu de société

Description

Surveillance des espaces publics, accès aux services administratifs, l'utilisation de cette technologie biométrique d'authentification et d'identification continue de s'étendre en Europe ([voir La rem n°46-47, p.25](#)). Les caméras « intelligentes » portent à l'évidence atteinte à notre vie privée, en menaçant notre liberté de circuler de façon anonyme. Quel contrôle – selon quelles limites ? et par quelle instance ? – sera effectué sur ce marché florissant de logiciels qui, de surcroît, engendrent bon nombre d'erreurs et de discriminations liées aux biais algorithmiques ([voir La rem n°50-51, p.45](#)).

En août 2019, le quotidien britannique *Financial Times* révèle aux Londoniens que le quartier de King's Cross – lieu d'arrivée de l'Eurostar – est équipé de caméras de reconnaissance faciale et que le quartier d'affaires de Canary Wharf est en cours d'installation. L'Information Commissioner's Office (ICO – Autorité de régulation des données personnelles) ouvre une enquête. « *Scanner les visages des gens quand ils vaquent en toute légalité à leurs activités quotidiennes, avec l'objectif de les identifier, peut présenter un danger potentiel pour la vie privée [...], réagit sa présidente Elizabeth Denham. Spécialement si ces technologies sont utilisées sans que les gens soient tenus au courant ni n'en comprennent le fonctionnement* ».

LONDRES COMPTE AUJOURD'HUI PRÈS DE 420 000 CAMÉRAS DE SURVEILLANCE,
CE QUI EN FAIT LA VILLE LA PLUS SURVEILLÉE AU MONDE APRÈS PÉKIN

En réalité, des millions de Britanniques ont déjà eu, sans le savoir, le visage scanné par des caméras de reconnaissance faciale au cours d'expérimentations menées en 2018. En août 2019, la liste des lieux équipés sur le territoire est établie par l'ONG Big Brother Watch, parmi eux des centres commerciaux, un centre de conférence, un musée, des casinos, etc. « *Il n'y a pas d'autres pays, à part la Chine, qui en fassent une utilisation aussi inconsidérée* », explique Silkie Carlo, directrice de l'ONG, à propos de la technologie de reconnaissance faciale au Royaume-Uni.

Londres compte aujourd'hui près de 420 000 caméras de surveillance, ce qui en fait la ville la plus surveillée au monde après Pékin, qui en a 470 000. Le Royaume-Uni dispose de plus de 4 millions de caméras de surveillance sur l'ensemble de son territoire – environ une caméra pour 14 habitants. En marchant aujourd'hui dans la capitale britannique, on peut être filmé, chaque jour, par 300 caméras.

CAPABLE DE SCANNER 300 VISAGES À LA SECONDE, LE LOGICIEL CHOISI PAR LA POLICE A RÉALISÉ PLUS DE 80 % D'IDENTIFICATIONS ERRONÉES

Depuis 2016, la police britannique, notamment dans le Grand Londres et au Pays de Galles, s'appuie sur ces équipements pour installer des logiciels de reconnaissance faciale et déclare renforcer ainsi la sécurité des citoyens, notamment lors de grandes manifestations comme le Carnaval de Notting Hill. Comme l'explique Pete Fussey, professeur de sociologie à l'université d'Essex, la surveillance par le biais de la reconnaissance faciale est devenue un véritable marché, sans qu'aucune législation *ad hoc* ne vienne l'encadrer. De nombreuses entreprises privées l'utilisent et pourtant, ni les moyens – les bases de données d'images auxquelles les scans de visage sont comparés –, ni la finalité de cette surveillance, ne sont connus. *« Il y a une contradiction dans notre pays. D'un côté, nous sommes très fiers de notre État de droit et des libertés publiques, mais, d'un autre côté, nous avons une grande complaisance pour le risque de leur érosion »*, constate la directrice de Big Brother Watch.

Une équipe de chercheurs de l'université de l'Essex a procédé à l'étude des résultats de six tests de reconnaissance faciale menés par la police de Londres à Westfield, un centre commercial dans le quartier de Stratford. Capable de scanner 300 visages à la seconde, le logiciel choisi par la police, NeoFace de la société Nec, a réalisé plus de 80 % d'identifications erronées, appelées « faux positifs » : sur les 42 visages repérés par la machine, 26 personnes ont été arrêtées et finalement 8 ont été identifiées avec certitude à partir de la base de données des personnes suspectées, base de données qui, en outre, n'était pas à jour. Selon les chercheurs : *« Aucune autorisation légale explicite pour la reconnaissance faciale en direct n'est présente dans le droit britannique. »* Ils considèrent *« que toute ingérence dans les droits d'une personne devrait être justifiée par une « nécessité » au sein d'une société démocratique »*.

En Suède, fin août 2019, l'autorité de protection des données a infligé sa première amende, d'un montant équivalent à 20 000 euros, pour non-respect du RGPD (règlement général sur la protection des données) à l'encontre d'une école située dans le nord du pays. À l'automne 2018, l'établissement a testé, durant trois semaines, la technologie de reconnaissance auprès d'une classe, afin de surveiller l'assiduité de ses vingt-deux élèves. Si le consentement des élèves a bien été recueilli par l'établissement scolaire, l'Autorité de protection des données considère néanmoins qu'il s'agit d'un traitement illégal de données sensibles, *« étant donné le déséquilibre manifeste entre la personne concernée et le responsable du traitement »*. En outre, l'établissement scolaire a omis d'en informer *a priori* l'Autorité et n'a procédé à aucune étude d'impact.

En France, la ville de Nice, qui compte une caméra pour 145 habitants, est la première à tester la reconnaissance faciale sur la voie publique. En février 2019, cette technologie a été expérimentée, durant les trois jours du carnaval, avec six caméras réparties dans un périmètre délimité et signalé.

« EN QUOI UN AGENT HUMAIN, QUI CONNAÎT PERSONNELLEMENT LES ÉLÈVES, SERAIT-IL MOINS EFFICACE QU'UNE CAMÉRA DE RECONNAISSANCE FACIALE »
Martin Drago, juriste à LQDN

Conformément à l'article 9 du RGPD disposant que l'interdiction de principe au traitement des données biométriques, dites données sensibles, peut être levée en cas de consentement des personnes concernées, seules des volontaires pouvaient participer à l'exercice. Afin d'évaluer l'efficacité du dispositif, il s'agissait pour la mairie de repérer, en temps réel, dans la foule, une personne « recherchée », un enfant perdu ou une personne âgée vulnérable égarée. Selon l'entreprise Confidentialia qui le commercialise, le logiciel israélien utilisé, AnyVision, est capable d'identifier une personne à partir d'une photo très ancienne ou même si la caméra n'a pu scanner que son profil. Depuis l'entrée en vigueur du RGPD ([voir La rem n°42-43, p.21](#)), la Commission nationale de l'informatique et des libertés (Cnil) dispose de prérogatives d'enquête et de sanction plus importantes mais son autorisation préalable n'est plus requise pour la mise en place d'un dispositif de traitement de données à caractère personnel. La Commission a fait savoir cependant qu'elle regrettait avoir été informée très tardivement par l'équipe municipale – moins d'un mois avant le début de l'expérience –, afin de pouvoir encadrer le déroulement du test. Elle a pu exiger toutefois l'installation de panneaux informant les habitants de l'obligation de consentement.

À la demande de la Cnil, la mairie de Nice a présenté, en juillet 2019, un bilan de son expérimentation de reconnaissance faciale sur la voie publique. Selon la municipalité, le logiciel AnyVision a parfaitement tenu ses promesses : ni une photo, datant de plusieurs décennies, ni le port d'une paire de lunettes de soleil ou d'une casquette n'ont constitué un obstacle pour l'identification d'un visage dans la foule. Aucune plainte n'a été enregistrée et la police municipale considère l'outil « *fiable et pertinent* ». La Cnil souhaite néanmoins obtenir des compléments d'information, jugeant très insuffisantes les données concrètes sur l'efficacité du dispositif (éléments chiffrés, biais constatés...).

Une autre expérimentation de surveillance à partir de données biométriques a été programmée dans la région Sud (anciennement PACA). Votée en conseil régional en décembre 2018, elle porte sur l'installation de « portiques virtuels » dans deux lycées publics, Les Eucalyptus à Nice et Ampère à Marseille. Des caméras « intelligentes » – équipées d'un logiciel de reconnaissance faciale – serviraient à filtrer les entrées et les sorties de ces établissements scolaires. La Cnil n'intervenant plus qu'*a posteriori*, quatre organisations – La Quadrature du Net, la Ligue des droits de l'homme, CGT Educ'Action des Alpes-Maritimes et la Fédération des conseils de parents d'élèves des écoles publiques des Alpes-Maritimes (FCPE) – ont pris les devants, en février 2019, et ont déposé un recours devant le tribunal administratif de Marseille, afin d'obtenir l'annulation de cette décision du conseil régional.

Le dispositif doit permettre d'assister « *efficacement* » les personnes responsables du contrôle de l'accès aux lycées, selon le souhait du conseil régional. Une soixantaine de lycéens seraient concernés, tous sur la base

du volontariat. Juriste à La Quadrature du Net, Martin Drago défend *a contrario* l'idée suivante : « Dans un lycée, mettre en place une telle technologie, c'est habituer les mineurs à une surveillance sur des données biométriques. Il y a un risque de banalisation de ces technologies de surveillance, qu'on voit arriver dans les gares, les aéroports et qui ne vont pas tarder à arriver dans les villes dans le cadre de la safe city [ville « sûre » grâce aux technologies numériques]. »

LES INDUSTRIELS SAVENT PROMOUVOIR LES TECHNIQUES QU'ILS INVENTENT SANS QUE LA QUESTION DES LIBERTÉS INDIVIDUELLES LEUR PARAISSE UN OBSTACLE

Pour l'heure, l'absence d'une législation *ad hoc* bloque au stade de l'expérimentation l'usage de la reconnaissance faciale dans l'espace public. À terme, le projet « portique virtuel » de la mairie de Nice devrait être étendu à l'ensemble des établissements scolaires, avec pour objectif de réduire la durée des contrôles. Généraliser et donc pérenniser ce dispositif revient à annuler la condition du consentement, selon Martin Drago. Pour le juriste, le caractère « nécessaire et proportionnel » du traitement des données personnelles inscrit dans le RGPD n'est pas évident dans ce cas précis : « En quoi un agent humain, qui connaît personnellement les élèves, serait-il moins efficace qu'une caméra de reconnaissance faciale qui ne marche pas toujours ? »

Outre l'aspect sécuritaire, la question peut également être abordée sous l'angle économique. Un portique automatique permet de réduire le nombre d'emplois. Les industriels savent promouvoir les techniques qu'ils inventent sans que la question des libertés individuelles leur paraisse un obstacle. Dans le cas des deux lycées niçois, l'expérimentation est offerte par l'américain Cisco. L'offre et la demande de services de surveillance sont l'une comme l'autre pressantes. Or à ce nouveau marché correspond un vide juridique. Le récent RGPD n'apporte pas de réponses suffisantes. Pour l'heure, la pérennité d'un dispositif équivalent à celui mis en place dans les deux lycées niçois reste soumise à un décret validé par le Conseil d'État ou encore à une loi qui en déterminerait la mise en œuvre. Depuis plus d'un an, la Cnil plaide pour la définition d'un cadre juridique adéquat, offrant des garde-fous suffisants : « Cette technologie n'en est désormais plus à ses balbutiements. Les enjeux de protection des données et les risques d'atteintes aux libertés individuelles que de tels dispositifs sont susceptibles d'induire sont considérables, dont notamment la liberté d'aller et venir anonymement. »

LE PROJET ALICEM VISE À CE QUE CHAQUE FRANÇAIS PUISSE PROUVER SON IDENTITÉ EN LIGNE, GRÂCE À LA RECONNAISSANCE FACIALE, DÈS 2020, UNE PREMIÈRE EN EUROPE

Les technologies de surveillance appellent à trouver un équilibre toujours délicat entre les impératifs de sécurité et le respect des libertés publiques. L'association La Quadrature du Net est à l'origine d'un recours déposé le 15 juillet 2019 devant le Conseil d'État afin d'obtenir l'annulation de l'autorisation d'une application baptisée Alicem pour « Authentification en ligne certifiée sur mobile ». En phase de test, cette solution d'identité numérique inscrite dans un décret du 13 mai 2019 émane du ministère de l'intérieur et de l'Agence nationale des titres sécurisés (ANTS). Le projet vise à ce que chaque Français puisse prouver son identité en ligne, grâce à la reconnaissance faciale, dès 2020, une première en Europe. Développée par la société Gemalto (groupe Thalès) et fonctionnant uniquement sur le système d'exploitation Android, l'application Alicem est présentée comme un dispositif hautement sécurisé d'authentification pour accéder aux sites des services administratifs regroupés sur la plateforme FranceConnect. Pour créer un compte sur Alicem, l'administré devra scanner, à l'aide de son téléphone portable, la puce se trouvant sur son passeport biométrique, puis se prendre en vidéo sous tous les angles, afin que l'application puisse vérifier la concordance des deux éléments.

La Quadrature du Net dénonce la volonté de normalisation de la reconnaissance faciale à travers cet outil d'authentification qui ne laisse place à aucune alternative. L'association s'appuie sur l'avis de la Cnil, paru en octobre 2018, concernant le projet de décret autorisant Alicem : « *En l'espèce, le refus du traitement des données biométriques fait obstacle à l'activation du compte, et prive de portée le consentement initial à la création du compte.* » En 2012, la création d'une base de données biométriques avait été jugée inconstitutionnelle par le Conseil d'État. Avec Alicem, les données personnelles et sensibles fournies resteront enregistrées exclusivement sur le smartphone de l'administré, assure le ministère de l'intérieur, et la vidéo sera effacée une fois l'authentification faite. Initialement annoncée pour la fin de l'année 2019, l'application Alicem pourrait être opérationnelle dès le mois de novembre 2019.

**SUPPORTERONS-NOUS DEMAIN D'AVOIR À ÊTRE SUBREPTICEMENT « VALIDÉS »
SUR LA BASE DE NOS CARACTÉRISTIQUES PHYSIQUES, BIOLOGIQUES,
COMPORTEMENTALES, VOIRE ÉMOTIONNELLES**

La question de la reconnaissance faciale se trouve également au centre des vastes métamorphoses numériques en préparation que sont les villes « intelligentes » (*smart cities*) et les villes « sûres » (*safe cities*). Quand bien même les outils numériques pourraient faciliter la vie citadine, comment chacun conservera-t-il la liberté de s'en extraire ? Supporterons-nous demain d'avoir à être subrepticement « validés » sur la base de nos caractéristiques physiques, biologiques, comportementales, voire émotionnelles, afin d'accéder à nos démarches quotidiennes ? Car nous agirons, « communiquerons », alors essentiellement par l'intermédiaire des machines. Doit-on compter *a priori* sur les performances en progrès constant de l'intelligence artificielle pour remédier aux erreurs de jugement commises pour l'heure par les machines ? Le taux d'erreur actuel est en effet élevé, particulièrement pour les personnes noires, surtout les femmes – 30 % d'erreurs pour

identifier le sexe d'une femme noire contre 1 % d'erreur pour un homme blanc. Les écarts de fiabilité sont importants selon les systèmes de reconnaissance faciale. Les logiciels de l'entreprise Gemalto, à l'origine des sas de sécurité d'Aéroports de Paris ([voir La rem n°46-47, p.25](#)), ont un taux d'erreur inférieur à 1 %. Avec Rekognition, logiciel de reconnaissance faciale d'Amazon, 28 membres du Congrès américain ont été identifiés comme étant des délinquants. Ce test, organisé en juillet 2018 par l'Union américaine pour les libertés civiles (ACLU), avait pour objectif de démontrer les failles de ce logiciel vendu aux forces de police. En août 2019, un nouvel essai a donné le même résultat. En février 2019, Amazon, à l'instar d'autres entreprises du secteur, appelle à réglementer l'usage de la reconnaissance faciale, recommandant de se fier uniquement à un taux de réussite de 99 % lorsque la technologie est utilisée par les forces de police. En mai 2019, la ville de San Francisco a voté l'interdiction de la reconnaissance faciale, à l'exception des aéroports et des sites relevant des autorités fédérales, expliquant que « *la propension à ce que la technologie de reconnaissance faciale mette en danger les droits civils et les libertés civiques contrebalance nettement ses soi-disant bénéfiques* ».

LA VILLE DE SAN FRANCISCO A VOTÉ L'INTERDICTION DE LA RECONNAISSANCE FACIALE

Même si le taux d'erreur venait à être jugé « acceptable », la question cruciale de la finalité de la reconnaissance faciale demeure. Définir une finalité, c'est déjà en accepter le principe. En Chine, la reconnaissance faciale est un puissant outil de « contrôle social », avec 176 millions de caméras de surveillance. La technologie sert aussi bien à retrouver des criminels, à payer ses achats, à accéder à une bibliothèque, à repérer les piétons qui ne respectent pas les feux ou encore à détecter des comportements « anormaux ». Et la technologie va se perfectionner : une start-up chinoise appelée Watrix a mis au point un algorithme capable de reconnaître une personne à sa posture. Dans une Europe hyper connectée, s'opposera-t-on demain à la liberté de recourir à la reconnaissance des émotions, qui aura atteint les performances annoncées par les *business angels* (investisseurs providentiels) de la high-tech, pour « aider » à l'embauche, la signature d'un contrat, l'inscription à une formation ?

À Nice, ville figurant au classement mondial des *smart cities*, le tramway est équipé d'un dispositif de la société Engie Ineo, capable de lire les émotions sur le visage des passagers, afin de détecter un incident. En juin 2018, le conseil municipal de la ville a choisi l'entreprise Thales pour expérimenter diverses solutions *safe city*, avec la participation de quinze sociétés spécialisées dans l'analyse des réseaux sociaux, la géolocalisation, la simulation de foule et la biométrie. Le développement des plateformes *safe city*, centres de supervision urbaine, est soutenu par la Banque publique d'investissement (Bpifrance), les collectivités locales et le Comité de la filière industrielle de sécurité (Cofis) rattaché aux services du Premier ministre. Le maire de la ville précise : « *Je demande à ce que le législateur fasse évoluer les textes, au rythme où évolue la société. Je dispose du logiciel qui permettrait dès demain matin d'appliquer la reconnaissance faciale et d'identifier des individus fichés où qu'ils se trouvent dans la ville... Pourquoi l'interdire ? Est-ce qu'on veut prendre le risque de voir des gens mourir au nom des libertés individuelles, alors qu'on a les technologies qui permettraient de l'éviter ?* »

« SI NOUS N'AGISSONS PAS, NOUS RISQUONS DE NOUS RÉVEILLER DANS CINQ ANS POUR CONSTATER QUE LES SERVICES DE RECONNAISSANCE FACIALE SE SONT ÉTENDUS DE MANIÈRE À EXACERBER LES PROBLÈMES DE SOCIÉTÉ »
Le groupe de chercheurs AI Now

En décembre 2018, le groupe de chercheurs AI Now de l'université de New York, soutenu notamment par Microsoft et Google, appelait les gouvernements à légiférer : « *Le génie de la reconnaissance faciale, pour ainsi dire, émerge de la bouteille. Si nous n'agissons pas, nous risquons de nous réveiller dans cinq ans pour constater que les services de reconnaissance faciale se sont étendus de manière à exacerber les problèmes de société.* »

Selon le *Financial Times*, la Commission européenne intégrerait dans sa future législation sur l'intelligence artificielle des règles visant à encadrer l'utilisation de la reconnaissance faciale par les entreprises et les pouvoirs publics, notamment avec un droit de savoir « où et quand » pour les citoyens européens. Le quotidien économique y voit surtout une façon de faire accepter cette technologie.

Sources :

- Reconnaissance faciale, Biométrie, Cnil, cnil.fr
- « Comment des villes hyper connectées contrôlent l'espace public », Grégoire Allix, lemonde.fr, 19 décembre 2018.
- « Nice va tester la reconnaissance faciale sur la voie publique », *Le Monde* avec AFP, 18 février 2019.
- « Reconnaissance faciale : quatre associations déposent un recours contre les futurs portiques de lycées du sud de la France », Pascal Hérard, tv5monde.com, 19 février 2019.
- « La reconnaissance faciale arrive dans nos lycées : doit-on se méfier ? », Fabien Soyez, cnetfrance.fr,

21 juin 2019.

- « Reconnaissance faciale : nouvelles polémiques après l'échec cuisant de la police de Londres », Pascal Hérard, tv5monde.com, 12 juillet 2019.
- « La Quadrature du Net attaque l'application ALICEM, contre la généralisation de la reconnaissance faciale », La Quadrature du Net, laquadrature.net, 17 juillet 2019.
- « Inquiétudes autour de la reconnaissance faciale pour s'identifier en ligne », Léa Sanchez, *Le Monde*, 28-29 juillet 2019.
- « Facial recognition in school renders Sweden's first GDPR fine », European Data Protection Board, edpb.europa.eu, 22 August, 2019.
- « Reconnaissance faciale : la Cnil tique sur le bilan de l'expérience niçoise », Martin Untersinger, lemonde.fr, 28 août 2019.
- « La Commission européenne envisage de légiférer sur la reconnaissance faciale », *La Correspondance de la Presse*, 29 août 2019.
- « Le Royaume-Uni, champion de la reconnaissance faciale », Cécile Ducourtieux, *Le Monde*, 4 septembre 2019.
- « Alicem sera déployée dès le mois de novembre malgré les critiques », Alice Vitard, usine-digitale.fr, 8 octobre 2019.

Categorie

1. Articles & chroniques

date créée

12 novembre 2019

Auteur

françoise