Les technologies de reconnaissance faciale mises au point pour lutter contre la radicalisation et leurs développements depuis 2015

Sommaire

Introduction : le développement de la reconnaissance faciale

La reconnaissance faciale progresse, sous la pression des forces de l'ordre et de renseignement, des industriels qui créent ces outils, de l'État qui en bénéficie et de maires soucieux de leur réélection
Avant 2015, on avait développé des programmes de photographie des plaques d'immatriculation de véhicules trop rapides. On commençait à élaborer des lectures automatiques des lettres ou numéros de ces plaques.
La lutte contre la radicalisation a permis le lancement de plusieurs programmes de recherche à partir de 2015. Chaque année de nouveaux programmes ont été financés avec les financements de luttes contre la radicalisation, aussi bien en Chine qu'aux Etats-Unis ou en Europe. Où en est-on quatre ans après ?
Les changements ont été très rapides parce que d'autres demandes que les demandes sécuritaires sont rapidement apparues. Les technologies changent en conséquence. Actuellement, on peut lire à plusieurs kilomètres sur les lèvres d'une personne distante sans rien entendre directement. On envisage donc de conduire les voitures sans pilote à la voix lue sur les lèvres et non plus identifiées par des sons.
Mais ces transformations nées en partie des nécessités de la sécurité (où elles n'ont d'ailleurs pas été très efficaces jusqu'à présent) ne portent-elles pas atteintes à la vie privée fondement de la démocratie. Que faire dans ce cas ?

La reconnaissance faciale : un nécessaire débat

La CNIL a publié, vendredi 15 novembre, un document visant à poser un cadre à l'utilisation de cette technologie, de plus en plus présente dans notre quotidien. Un débat public sur ce sujet est indispensable, et il est même tardif.

Publié le 16 novembre 2019 à 09h11

La reconnaissance faciale évoque un imaginaire inquiétant de surveillance généralisée et de dystopie, à mi-chemin entre le *1984*prophétique de George Orwell et la très actuelle série à succès *Black Mirror*. Déjà utilisée dans plusieurs pays, cette technologie est pourtant appelée à faire de plus en plus partie de notre univers quotidien. Il est donc urgent de la dissocier des fantasmes.

Il existe différentes formes de reconnaissance faciale. Encadrés et contrôlés, certains usages pratiques peuvent être utiles et sans danger, comme les fonctions de déverrouillage de certains téléphones ou la possibilité de se créer un compte sécurisé en ligne pour accéder aux services publics.

D'autres applications, cependant, constituent une menace réelle pour les libertés individuelles. Le recours à la reconnaissance faciale dans l'espace public, à l'insu des passants et en temps réel, en est un exemple. Il ne s'agit pas de simple vidéosurveillance mais d'un changement de paradigme, consistant à identifier et surveiller chacun pour en repérer quelques-uns, à l'aide de données biométriques : à l'inverse d'un mot de passe, un visage ne peut être changé lorsqu'il est perdu ou compromis.

En France, le cadre juridique existant n'interdit pas complètement la reconnaissance faciale. Un nombre croissant d'acteurs suggèrent de l'assouplir, afin de permettre une utilisation plus large de cette technologie. Le secrétaire d'Etat chargé du numérique, Cédric O, a pris position en faveur de la multiplication d'expériences. L'industrie est elle aussi très intéressée par les bénéfices qu'elle peut retirer de cette technologie.

Un débat public sur cet important sujet paraît indispensable. Il est même tardif. La Commission nationale de l'informatique et des libertés (CNIL) a publié, vendredi 15 novembre, un document visant à en poser le cadre afin, a expliqué au*Monde* sa présidente, Marie-Laure Denis, de *« définir le code de la route des usages de la reconnaissance faciale ».*

Ce débat doit aussi se nourrir des retours d'expérience à l'étranger. Au Royaume-Uni, certaines tentatives, comme celle de vidéosurveillance pendant le carnaval de Notting Hill à Londres, il y a deux ans, ont tourné au fiasco. San Francisco, une ville qui a été aux premières loges sur les technologies numériques plus tôt que d'autres, a voté son interdiction. En Chine, la reconnaissance faciale peut servir à payer sans carte de crédit ni monnaie et simplifier la vie quotidienne en milieu urbain surpeuplé, mais elle est aussi un redoutable instrument de contrôle de la société par un régime autoritaire. Tout cela est à étudier de très près, avec un esprit ouvert mais de la manière la plus rigoureuse possible.

Lorsque la question de la protection des données personnelles a émergé, ses défenseurs ont été accusés de mener un combat d'arrière-garde et d'entraver l'innovation. Il faudra s'en souvenir dans le débat sur la reconnaissance faciale : aujourd'hui, partout sur la planète et jusqu'aux technophiles Etats-Unis, la loi européenne sur les données, successeure d'une directive européenne elle-même inspirée de la loi française dite « informatique et libertés » de 1978, est citée comme modèle.

Il n'est pas inutile de rappeler l'article premier de cette loi de 1978 :*« L'informatique doit être au service de chaque citoyen. Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques. »*

Le big data, Les pressions de l'État, du secrétaire d'État au numérique et des industriels

Par Martin Untersinger Publié le 14octobre 2019 à 03h27 - Mis à jour le 14 octobre 2019 à 18h29

Le centre de supervision urbain de la ville de Nice expérimente la reconnaissance faciale, le 15 avril 2016. Sylvestre / MAXPPP

« N'ayons pas de pudeurs de gazelle ! » Le 2 septembre, devant des sénateurs, le ministre de l'intérieur, Christophe Castaner, a la ferme intention de lancer le débat sur la reconnaissance faciale. *« Lors de l'attentat à Lyon* [en mai]*, nous avons identifié l'auteur par le biais de la vidéoprotection. L'événement a eu lieu à 16 h 30, mais il a été interpellé le lendemain, le temps qu'une trentaine d'enquêteurs regardent image par image l'ensemble du réseau pour refaire son parcours. Avec un système d'intelligence artificielle, quinze minutes après on aurait su où il était allé. »*

Comme le ministre de l'intérieur, responsables politiques et forces de l'ordre lorgnent depuis plusieurs années les technologies de reconnaissance faciale. En juin, la mairie de Nice a mené une médiatique expérimentation sur la voie publique. Pour sécuriser les démarches en ligne, le gouvernement teste Alicem, une application mobile comparant des photos prises *« en selfie »* à celles contenues dans les passeports. Non sans polémique.

« J'aimerais expérimenter dans les transports la reconnaissance faciale (…) *au moins pour des personnes condamnées pour faits de terrorisme »,* a encorerécemment réclamé Valérie Pécresse, présidente de la région Ile-de-France. Face à ces tentations, le cadre légal français, s'il n'interdit pas la reconnaissance faciale, est encore très strict. Si bien que Cédric O, le secrétaire d'Etat au numérique, a décidé d'annoncer lundi 14 octobre dans nos colonnes vouloir un comité chargé de susciter davantage d'expérimentations de cette technologie.

Fichier massif de 7 millions de personnes

Dans les interstices laissés par la loi, les utilisations de la reconnaissance faciale aux lourds enjeux de libertés publiques ont pourtant progressé. Les forces de l'ordre peuvent d'ores et déjà interroger un fichier de police à l'aide d'une photo, pour retrouver l'identité d'un suspect : le massif fichier des antécédents judiciaires, qui contient les

photos de plus de 7 millions de personnes. Et ce en dépit des réserves de la Commission nationale de l'informatique et des libertés (CNIL), qui pointait *« des risques importants pour les libertés individuelles »*.

Les enquêteurs aimeraient étendre cet outil à d'autres fichiers, notamment ceux des personnes recherchées (FPR) et des ressortissants étrangers en France. Techniquement possible, elle ne l'est pas en l'état du droit : l'utilisation de la reconnaissance faciale est explicitement prohibée dans ces deux fichiers, comme pour beaucoup d'autres.

Les forces de l'ordre peuvent aussi rechercher un suspect sur les données des caméras de vidéosurveillance saisies dans le cadre d'une enquête judiciaire. De nombreuses entreprises proposent ces services. Par exemple la société Brainchip, qui a travaillé avec la police de Toulouse. Sa technologie, capable de faire de la*« biométrie à la volée »* se branche, en différé, sur les images collectées par vidéosurveillance.

Par ailleurs, selon un décompte du *Monde*, plus d'une dizaine de projets de recherche ont été menés ces dix dernières années, souvent sur fonds publics et en partenariat avec des services de police ou de gendarmerie, pour entraîner les algorithmes et adapter la reconnaissance faciale aux besoins des forces de l'ordre.

Enregistrer la biométrie faciale des passants

Exemple parmi d'autres, le projet Kivaou, financé par l'Agence nationale de la recherche et piloté par Sagem (désormais Safran) et le ministère de l'intérieur, a été conçu pour mettre au point un *« outil de surveillance embarqué permettant d'indexer au fil de l'eau tous les passants et d'enregistrer leur biométrie faciale »*. Selon nos informations, des enquêteurs ont parfois profité de ces expérimentations pour faire progresser leurs investigations.

Les projets se multiplient aussi dans le privé, comme celui lancé par Thales etautorisé par la CNIL en 2016, consistant à tester auprès de volontaires l'identification en temps réel par la vidéosurveillance. Groupe ADP (ex-Aéroports de Paris) a lui aussi mené en 2017 une expérimentation dans l'un de ses terminaux afin d'évaluer la technologie : des salariés volontaires passaient devant des caméras chargées de les reconnaître. Très en pointe sur la question, l'entreprise s'apprête à réaliser une nouvelle expérimentation, pour le contrôle de l'embarquement, au début de l'année 2020.

La question d'un assouplissement du cadre légal se pose en réalité depuis des années. Plusieurs propositions de loi et d'amendement ont été avancées afin de pouvoir relier vidéosurveillance et fichiers policiers par le biais de la reconnaissance faciale, afin de repérer des personnes dans la foule. Interrogé sur ce point en 2016, Bernard Cazeneuve, alors ministre de l'intérieur, avait clairement laissé entendre qu'il travaillait en ce sens. Un projet demeuré lettre morte et une déclaration passée inaperçue. Celui-ci n'a pas souhaité répondre à nos questions.

La technique a progressé et le débat de la régulation se pose à nouveau. La Commission européenne est censée proposer un texte sur l'intelligence artificielle lors des cent premiers jours de son mandat. A cette heure, l'inclusion de la reconnaissance faciale n'est pas tranchée. Certains font des Jeux olympiques (JO) de Paris, en 2024, un objectif. *« Les industriels mettent la pression »,* souffle un bon connaisseur du dossier. Aucune décision n'a été prise à ce stade, mais les expérimentations menées aux JO de Tokyo en matière de reconnaissance faciale seront observées par la Coordination nationale pour la sécurité des Jeux olympiques.

Consensus pour améliorer la technologie

Reste un problème de taille pour ceux qui souhaitent la généralisation de la reconnaissance faciale : si certaines formes de cette technologie sont fiables, d'autres le sont moins. Ainsi, au Royaume-Uni, le bilan de certaines expérimentations est catastrophique.

Il y a donc consensus pour améliorer la technologie. *« Il faut avoir un taux d'efficience de 80 %. On n'y est pas encore. Il faut faire plus d'expérimentations »,*juge un gendarme bien informé. C'est aussi l'avis de Didier Baichère, vice-président de l'Office parlementaire des choix scientifiques et technologiques (Opecst), qui a récemment publié ses travaux sur le sujet.

Il plaide pour que le gouvernement lance une concertation, débouchant sur un rapport dont l'Opecst se chargerait de tirer les conclusions législatives. Les forces de l'ordre tiennent en tout cas à ce nouvel outil. *« La plus-value policière de cette technologie ne fait aucun doute »,* peut-on lire dans une récente note du Centre de recherche de l'école des officiers de la gendarmerie. Selon son auteur, elle pourrait même *« mettre fin à des années de polémiques sur le contrôle au faciès, puisque le contrôle d'identité serait permanent et général ».*

Cédric O : « Expérimenter la reconnaissance faciale est nécessaire pour que nos industriels progressent »

L Le secrétaire d'Etat au numérique, Cédric O, souhaite susciter davantage d'expérimentations. Mais plus d'une dizaine de projets de recherche ont déjà été menés ces dix dernières années.

Le secrétaire d'Etat au numérique annonce vouloir créer, en coordination avec la CNIL, une instance de supervision et d'évaluation.

Propos recueillis par Martin Untersinger Publié le 14 octobre 2019 à 09h12 - Mis à jour le 14 octobre 2019 à 20h23

Cedric O, le secrétaire d'Etat au numérique, à l'Elysée, le 17 septembre. LUDOVIC MARIN / AFP

Alors que les forces de l'ordre poussent au développement de la reconnaissance faciale, Cédric O, le secrétaire d'Etat au numérique, propose de

créer une instance de supervision en coordination avec la Commission nationale de l'informatique et des libertés (CNIL).

Le gouvernement réfléchit-il à des changements législatifs pour élargir l'utilisation de la reconnaissance faciale ?

Cédric O : Comme souvent, la technologie est en avance sur la régulation. Aujourd'hui, la reconnaissance faciale entre dans nos vies sans que son cadre d'utilisation n'ait encore été clarifié. Elle offre de nouveaux usages, de nouvelles opportunités, mais surtout crée beaucoup de fantasmes du fait de l'absence d'un vrai débat citoyen sur les lignes rouges que nous souhaitons collectivement poser.

Faut-il faciliter les expérimentations en la matière ?

Il ne faut pas avoir une vision exclusivement nihiliste de la reconnaissance faciale : il y a beaucoup d'usages qui, s'ils sont bordés juridiquement et techniquement, ne posent aucun problème et apportent de la

simplification – par exemple, pour tout ce qui nécessite aujourd'hui de se présenter à un guichet ou pour valider une formation en ligne. Expérimenter est également nécessaire pour que nos industriels progressent.

Que proposez-vous ?

Je propose de créer en coordination avec la CNIL une instance spécifique, composée de membres issus de différentes administrations et régulateurs, sous la supervision de chercheurs et de citoyens. Cette instance superviserait et évaluerait les expérimentations. Dans un deuxième temps, il faut un débat citoyen sur le sujet afin d'examiner les questions légitimes sur l'équilibre entre usages, protection et libertés. Il me semble par ailleurs important qu'il y ait une supervision de la société civile car le sujet est trop sensible : l'Etat doit se protéger de lui-même.

L'utilisation de mécanismes de reconnaissance faciale en temps réel sur les images de vidéosurveillance est-elle envisageable ?

Je suis extrêmement partagé sur la question. On en voit très bien l'utilité, par exemple pour identifier des terroristes dans une foule, mais aussi les risques. Il faut donc en définir très clairement le cadre et les garanties pour éviter la surveillance généralisée. Je pense que nous devons avoir un débat citoyen sur le sujet, en associant les parlementaires et les élus locaux. C'est, d'une certaine manière, aux Français de choisir, car les décisions seront lourdes de conséquences. C'est le genre de décisions sur lequel vous ne revenez que très difficilement. Et nous avons une responsabilité vis-à-vis des générations à venir. Il ne faut toutefois pas se laisser emporter par une vision dystopique ni utopique de la reconnaissance faciale et se saisir de la question à un moment où le débat est encore relativement apaisé.

Concernant Alicem, une application mobile de reconnaissance faciale qui sert à se connecter aux services publics, comprenez-vous la levée de boucliers ?

Il y a beaucoup de fantasmes. Alicem est aujourd'hui en test sur quelques milliers de personnes. En matière d'identité numérique, nous ne prévoyons à ce jour aucun mécanisme qui obligerait à passer par la reconnaissance faciale. Si l'utilisateur de l'application souhaite s'en servir, il doit explicitement donner son consentement au préalable. Lors de l'inscription à l'application, le logiciel utilise la caméra pour vérifier que l'utilisateur du téléphone portable est bien le détenteur du titre d'identité. Les prises de vue ne quittent pas le téléphone et ne sont pas conservées. Enfin, la reconnaissance faciale n'est plus jamais utilisée lors de l'utilisation de l'application. Nous sommes ouverts à des techniques alternatives d'authentification forte et il y aura, le cas échéant, des mécanismes d'enrôlement qui ne passent pas par la reconnaissance faciale.

Une ouverture générale du dispositif en novembre a été évoquée, qu'en est-il ?

C'est une proposition qui a été faite, mais cette date me semble prématurée. Nous avons saisi le Conseil national du numérique et les députées Paula Forteza et Christine Hennion ont débuté un travail pour le compte de l'Assemblée nationale sur le sujet de l'identité numérique. Nous n'ouvrirons pas le test plus largement avant que nous ayons eu leurs premiers retours.

Comment des villes « hyper connectées » contrôlent l'espace public

A Nice, Marseille ou Nîmes, on travaille avec des plates-formes numériques, quitte à repousser les frontières des libertés.

Par Grégoire Allix Publié le 19 décembre 2018 à 05h45 - Mis à jour le 19 décembre 2018 à 11h01

Le centre de supervision urbain de Nice, en août. VILLE DE NICE

Imaginez : depuis la salle de commande d'un centre municipal de supervision, vous contrôlez toute votre ville. Sur un mur d'écrans, vous suivez les individus au comportement « anormal », vous vérifiez les objets abandonnés, vous repérez une altercation dans la rue, sans oublier de surveiller les tramways bondés, de garder un œil sur la crue de la rivière… Pas besoin de chercher au hasard : l'intelligence artificielle vous montre, parmi les images filmées par des centaines de caméras haute définition à vision nocturne, uniquement ce que vous devez voir.

Mieux : vous recevez en direct les vidéos d'attroupements suspects ou de véhicules gênants envoyées depuis leur smartphone par vos administrés, et un algorithme scanne les réseaux sociaux pour anticiper d'éventuels rassemblements à risques.

D'un simple geste sur un terminal numérique mobile – audacieusement baptisé « tablette d'hypervision » –, vous ouvrez ou fermez les bornes d'accès au centre-ville piéton, vous maîtrisez l'entrée des bâtiments publics, vous modifiez les feux de circulation, vous intensifiez l'éclairage d'une rue. Un bruit suspect retentit ? Les caméras de la zone se tournent d'elles-mêmes vers son origine. Sur la carte numérique de la ville, toutes les équipes – police, secours, services techniques – sont géolocalisées, vous pouvez les envoyer sur place au plus vite en cas de besoin…

Ni fantasme ni science-fiction : ces dispositifs sont très exactement ceux que des villes françaises commencent à expérimenter sous le nom générique de « safe city » (la ville sûre), avatar en uniforme de la « smart city », la « ville hyper connectée ». *« La sécurité est, avec la mobilité, le pilier le plus réaliste de la smart city,* estime Marc Darmon, directeur général adjoint du groupe Thales. *Il y a un marché porteur pour ces technologies, par la conjonction de l'urbanisation, de la numérisation et de risques qui s'aggravent. »*

Un mouvement de fond

De Nice à Valenciennes (Nord), de Marseille à la Défense ou à Nîmes, de plus en plus de collectivités se laissent tenter par des plates-formes numériques organisées autour des outils de surveillance et de contrôle de l'espace public.

Un mouvement de fond, en phase avec de puissants intérêts industriels et porté par des subventions publiques, qui prospère dans un certain flou juridique et inquiète les associations de défense des libertés publiques. Construits autour d'une vidéoprotection dernier cri, dopée à l'intelligence artificielle, aux algorithmes et au « big data », ces dispositifs ont l'avantage de rendre bien concret l'un des rêves fondateurs de la smart city : la gestion centralisée de la ville depuis un poste unique de commandement.

C'est le début d'une révolution : la fibre optique et les technologies numériques permettent l'interopérabilité de tous les systèmes, une interconnexion des différents métiers de la ville, qui fonctionnaient jusque-là en silos : l'éclairage

public, la mobilité et le stationnement, la sécurité, les parcs et jardins, les réseaux d'eau ou d'énergie… *« Le même matériel permet d'imbriquer la sécurité avec d'autres enjeux et d'autres fonctions. En mutualisant les équipements, nous multiplions les services, que ce soit dans la gestion quotidienne, pour les grands événements ou en cas de crise »,* explique Nathalie Allegret, directrice du marché Villes et territoires connectés chez Engie Ineo, l'un des poids lourds du secteur.

Mais dans ce schéma, les outils de surveillance occupent une place à part. Au point de faire de la sécurité la première priorité. *« La vidéoprotection n'est qu'une partie de la smart city, mais c'est peut-être la plus importante, car elle donne une vision instantanée du territoire : c'est le cœur et le poumon de la ville, c'est un outil qui sert à la gestion ordinaire de l'espace urbain »,* assume Bernard Serafino, responsable de la sécurité au cabinet du maire de Nîmes.

« Big data de la tranquillité publique »

La préfecture du Gard a déployé, avec Engie Ineo, un système de vidéosurveillance intelligente à l'échelle des quinze communes de l'agglomération : 600 caméras, reliées à un centre de supervision high-tech, qui permettent de gérer l'espace urbain et de rechercher et de suivre un individu ou un véhicule d'un bout à l'autre de l'agglomération.

La ville de Marseille, de son côté, se fait fort depuis le printemps de mettre en place un *« big data de la tranquillité publique »* grâce aux technologies de Engie Ineo et à une plate-forme de données Oracle, un dispositif censé être opérationnel début 2019. *« La safe city est la première brique de la smart city, c'est un outil d'aide à la décision pour la collectivité »,* décrit Caroline Pozmentier, l'adjointe au maire chargée de la sécurité publique.

Au-delà des images de ses 1 200 caméras – bientôt 1 500 –, la plate-forme collecte et archive les mains courantes des commissariats, les appels au service « Allô Mairie », les informations fournies par les hôpitaux, le service des parcs, les marchés, la voirie, et souhaite, à terme, utiliser les données des opérateurs téléphoniques et analyser les réseaux sociaux.

Le but : *« anticiper les risques »,* mais aussi faire analyser par le logiciel la pertinence des dispositifs mis en place. *« A ce stade, c'est de la prévention, pas de la prédiction, même si on y viendra,* estime M^me^ Pozmentier. *Plus on aura de données, plus la machine sera intelligente. »*

Lire les émotions sur les visages

A Nice, ville qui se revendique la plus « vidéoprotégée » de France, avec 2 200 caméras, et dont les élus sont fiers de faire bonne figure dans les classements des smart cities mondiales, on est prêt à aller plus loin.

La décision de la Commission nationale de l'informatique et des libertés (CNIL) de mettre fin, au printemps, à l'expérimentation Reporty – une application permettant à tout citoyen d'alerter la police municipale en lui adressant un enregistrement vidéo et sonore géolocalisé pour signaler un incident – n'a pas freiné les ambitions du maire (Les Républicains), Christian Estrosi. Celui-ci se félicite *« de faire de sa métropole un terrain d'expérimentation pour les industriels, français et étrangers ».*

Son centre de supervision urbaine s'équipe de toutes les technologies de vidéosurveillance intelligente et de pilotage à distance. Après avoir testé au premier semestre une tablette d'« hypervision » d'Engie Ineo, la ville a lancé un appel d'offres pour en munir durablement ses services. Les passagers du tramway sont filmés par un système qui lit les émotions sur leur visage pour détecter toute situation anormale. Et le conseil municipal a voté, en juin, l'expérimentation d'une batterie de solutions safe city avec Thales, à la tête d'un consortium de quinze sociétés spécialisées dans l'analyse des réseaux sociaux, la géolocalisation, la biométrie ou la simulation de foules.

C'est bien loin de France, à Mexico, que ces solutions ont pris forme. Le groupe Thales a développé dans la mégapole mexicaine, à partir de 2009, une *« solution intégrée de sécurité urbaine »* qui revendique des résultats spectaculaires. *« Nous faisons désormais la promotion de cette architecture en France »,* explique le directeur général adjoint de Thales. Outre Nice, le groupe prépare le même type de démonstrateur à la Défense, pour en faire *« le*

quartier le plus sûr du monde ». « L'idée est de faire la preuve du gain opérationnel pour la collectivité en testant des cas d'usage, de voir ce qui est utile ou non », explique M. Darmon.

Les entreprises chinoises à l'offensive

Parmi les missions du consortium : collecter un maximum de données publiques, municipales ou grâce à des conventions avec des opérateurs privés, pour *« chercher les corrélations et les signaux faibles »,* et, à l'aide de *« nouveaux algorithmes »,* être capable de *« mieux comprendre une situation et de développer des capacités prédictives ».*

L'intelligence artificielle et le croisement des données sont les deux clés de ces technologies, sans lesquelles la vidéosurveillance se révèle généralement largement inefficace. *« Il faut une intelligence artificielle pour détecter les événements anormaux, des situations violentes, et ne soumettre à l'opérateur que ce qu'il doit voir »,* explique M. Darmon. Inutile de programmer ce qu'est un comportement « normal » : *« Le logiciel apprend seul, par l'expérience et par le grand nombre de données, c'est lui qui décide ce qui est anormal. »* Avec pour conséquence que tout comportement s'écartant de la norme sociale risque d'être signalé comme suspect…

Pour les entreprises françaises, s'affirmer sur ces marchés de la sécurité urbaine de pointe est crucial. *« La possibilité de faire visiter la solution safe city mise en œuvre à Nice est un support commercial très important dans le marketing de l'offre sur la scène internationale »,* stipule la convention d'expérimentation entre Thales et la métropole de la Côte d'Azur.

Le dernier Smart City World Congress, en novembre, à Barcelone, l'a montré : les groupes chinois sont à l'offensive. C'est à Huawei que Valenciennes, dans le cadre de sa démarche de *« transformation numérique »,* a confié le renouvellement de son parc de vidéoprotection, assorti de nouveaux logiciels et d'un centre de surveillance, offrant à la société, en difficulté depuis que les Etats-Unis l'accusent de collaborer avec les services de renseignement chinois, une vitrine pour sa solution safe city.

« Une logique de surveillance massive »

Dans ce contexte, les plates-formes safe city « made in France » sont cofinancées par la Banque publique d'investissement (Bpifrance), subventionnées par les collectivités et encouragées par le Comité de la filière industrielle de sécurité (Cofis), placé sous la tutelle du premier ministre Edouard Philippe.

« C'est important pour les villes de se dire qu'il y a des acteurs français sur ces sujets clés : notre droit est plus contraignant que celui de la Chine ou des Etats-Unis sur la gestion des données », estime Nathalie Allegret, chez Engie Ineo.

Françaises ou non, ces technologies soulèvent quelques inquiétudes. *« La safe city, c'est la prolifération d'outils issus du milieu du renseignement, dans une logique de surveillance massive, d'identification des signaux faibles, des comportements suspects »,* dénonce Félix Tréguer, un responsable marseillais de l'association La Quadrature du Net. *« Ces outils permettront un contrôle social très sophistiqué quand leur potentiel sera optimisé,* estime-t-il. *Nous ne trouvons pas rassurant que la police municipale devienne le service de renseignement de l'espace public urbain et de son double numérique. »*

« Améliorer les secours, la circulation, c'est légitime, mais la généralisation de la vidéosurveillance nous inquiète, et scruter les réseaux sociaux, ce n'est pas le rôle d'un maire ! Sans aucun garde-fou, un outil pareil ne peut pas faire preuve de la neutralité indispensable, redoute Henri Busquet, de la Ligue des droits de l'homme à Nice. *C'est potentiellement un outil de destruction politique, qui fait courir un risque particulier aux opposants, aux journalistes… »*

La tentation du contrôle social

L'inquiétude est d'autant plus vive que certains élus ne cachent pas vouloir repousser les limites du cadre légal. *« On pourrait faire beaucoup mieux,* estime M. Estrosi, qui s'est plusieurs fois heurté à la CNIL. *Ce qui nous limite, c'est la loi, notamment la loi Informatique et libertés de 1978. 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 se 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 ? »*

Municipalités comme industriels le répètent à l'envi : leurs dispositifs respectent scrupuleusement la loi et le Règlement général sur la protection des données (RGPD). *« Il faut sortir du fantasme et de l'hypocrisie : on ne travaille pas sur de la surveillance nominative, on n'utilise que des données anonymisées, cryptées, agrégées,* martèle Caroline Pozmentier à Marseille. *L'objectif n'est pas de mettre un œil derrière chaque individu, on veut simplement prendre le pouls de notre ville pour avoir plus d'agilité. »*

Le *« cahier des clauses techniques »* définissant les objectifs de la safe city marseillaise suggère pourtant l'envie de dépasser ces données anonymes : il est question, pour *« détecter la préparation d'événements sauvages ou d'actes de délinquance »*, comme des *« apéros géants »* ou des *« marchés à la sauvette »*, de conduire une *« analyse des tweets, en s'appuyant sur l'identification des acteurs »*par *« remontée des fils de conversation ».*

Interpellée sur ces expérimentations, la CNIL s'est fendue d'un communiqué le 19 septembre. Elle y prend acte du *« développement rapide de nouveaux outils »*qui *« soulèvent des enjeux importants pour les droits et libertés individuelles des citoyens ».* Et appelle *« d'urgence à un débat démocratique sur cette problématique ».* En 2017, dans un cahier consacré à la smart city et aux données personnelles, la CNIL alertait déjà sur la tentation de contrôle social et de surveillance des individus dans une cité gouvernée par les données, soulignant que *« la possibilité de l'anonymat dans la ville est en train de s'évanouir »*. La safe city ne fait qu'accentuer cette problématique.

Grégoire Allix

Révélations sur la détention des Ouïgours

Le plan chinois pour interner les Ouïgours
A Almaty, au Kazakhstan, en décembre 2018. Dans les locaux de l'association Atajurt, des familles brandissent le portrait de leurs proches retenus ou détenus dans le Xinjiang. ROMAIN CHAMPALAUNE POUR « LE MONDE »

Harold Thibault et Brice Pedroletti
Un consortium de 17 médias, dont « Le Monde », révèle les « China Cables », des directives secrètes pour placer des pans entiers de la minorité musulmane dans des camps de rééducation idéologique
Rétention arbitraire, conditions de détention extrêmes, autocritiques et lavage de cerveau… Une série de directives révélant le fonctionnement des camps d'internement des Ouïgours au Xinjiang et attribuées à l'Etat-Parti chinois, jettent une lumière inédite, car décrite de l'intérieur du régime, sur la politique de répression systématique et d'internement de masse menée par Pékin. Elles ont été obtenues par le Consortium international des journalistes d'investigation (ICIJ) et sont dévoilées par 17 médias internationaux dont*Le Monde.*
Les « China Cables », sur lesquels ont également travaillé la BBC, le *Guardian*, la*Süddeutsche Zeitung*, *El Pais*ou encore les agences Associated Press et Kyodo, confirment le caractère hautement coercitif des camps d'enfermement de la population ouïgoure, mis en place depuis 2017, et ce en contradiction directe avec le discours public de la Chine sur ce qu'elle nomme *« centres de formation et d'éducation »*. Au moins 1 million de Ouïgours, sur une population totale de 11,5 millions, et

d'autres membres de minorités musulmanes auraient été internés les trois dernières années, selon le décompte d'ONG repris par l'ONU.

Parmi ces documents, classés secrets et dont plusieurs experts de la région du Xinjiang et linguistes, contactés par l'ICIJ attestent l'authenticité, figure une longue liste d'instructions administratives. En tête des directives, datées de 2017, figure le nom de Zhu Hailun, le numéro deux du Parti communiste de la région autonome ouïgoure du Xinjiang. Ce dernier dirige la Commission politique et légale, l'organe exécutif suprême en matière de sécurité pour la région.

Les directives détaillent le fonctionnement des centres de rétention construits pour accueillir des centaines de milliers de membres des minorités musulmanes de la région du Xinjiang, dans l'extrême ouest chinois. Quatre autres circulaires, également à en-tête de M. Zhu, expliquent la mise en place d'une base de données de surveillance de la population, qui se veut exhaustive et qui fait remonter, chaque semaine, des dizaines de milliers de noms de personnes jugées*« suspectes ».* Ces personnes peuvent donc être interpellées, du seul fait qu'elles ont voyagé à l'étranger ou simplement utilisé une application de partage de fichiers.

Ce réseau de*« centres d'éducation et de formation »*, selon l'appellation officielle, constitue le cœur de la politique d'internement à grande échelle lancée en 2016 par la Chine. Ces camps sont la réponse du régime à la menace terroriste à laquelle il est confronté. Près d'une centaine de ces « centres »,fraîchement construits et ayant donné lieu à des appels d'offres publics, ont été géolocalisés en 2018, les barbelés et miradors étant visibles sur Google Earth. La plupart sont gigantesques, d'une capacité pouvant aller jusqu'à 20 000 personnes.

Les « China Cables » donnent des détails sur les critères d'internement de la population qui est déterminé grâce à un système de fichage ultra-détaillé. La *« plate-forme intégrée des opérations conjointes »* selon son nom administratif, sert à trier et faire ressortir des noms de personnes *« suspectes »* – 24 412 sur une seule semaine, dans quatre préfectures du sud-ouest du Xinjiang en juin 2017, dont les deux tiers ont été placés en *« centre de formation »*. Pour le chercheur allemand et spécialiste reconnu de la question ouïgoure Adrian Zenz, le réseau des camps *« est là pour endoctriner presque toute une minorité ethnique et changer une population entière »*.

Extrêmement coercitif

Adressée à toutes les villes et préfectures de la région, la première circulaire liste en 26 points les *« instructions pour renforcer et standardiser le fonctionnement »* de ces centres. Elle est typique des documents du Parti communiste, remplis de jargon, et confirme le caractère extrêmement coercitif de ces camps, qui constituent *« une mesure stratégique, critique et de long terme »* dans le combat contre le terrorisme. Leur fonctionnement est*« hautement sensible »* : il est ordonné de *« renforcer chez le personnel la conscience de*[les] *garder secrets »* et d'interdire d'y faire entrer tout matériel d'enregistrement vidéo, téléphones ou appareils photo.

La circulaire détaille les mesures de prévention des évasions par un fonctionnement typiquement carcéral. Il faut, préconise le document, *« améliorer l'installation de postes de police à l'entrée principale »*, mettre en place des*« enceintes parfaitement étanches »*. Et aussi s'assurer du système de *« double fermeture »* des portes des dortoirs, des couloirs et des étages – un procédé qui dans le jargon carcéral chinois implique deux clés détenues par deux gardes différents. Il faut encore s'assurer que les détenus, qualifiés d'*« étudiants »* car en phase de rééducation, *« ne s'échappent pas durant les cours, le traitement médical, les visites familiales »*. Tout « étudiant » qui quitte le centre pour une raison ou une autre *« doit être accompagné par du personnel qui le contrôle et le surveille »*.

Au chapitre *« prévention des troubles »*, les responsables des centres sont incités à*« repérer et remédier à toute violation de comportement* », et les officiers du renseignement, à s'assurer que *« personne ne se ligue pour créer des problèmes »*.

Une *« surveillance vidéo complète des dortoirs et des classes sans aucun angle mort doit être assurée »*. Le centre doit être subdivisé en une*« zone très stricte »*, une*« zone stricte »* et une *« zone normale »*. Chaque détenu sera *« affecté à l'une de ces zones après une sélection »*. La suite du document donne des consignes en matière de prévention des séismes, des incendies et des maladies – avec le souci

d'éviter tout incident et toute *« mort anormale »*. Il est strictement interdit à la police de « *pénétrer dans les zones d'études avec des armes* ». Les contacts avec la famille sont encouragés *« au téléphone une fois par semaine et par vidéo une fois par mois »*.
La plupart de ces instructions ont été corroborées par certains des détenus qui ont été libérés, ont gagné l'étranger et ont choisi de parler. Mais dans la réalité, les pratiques vont bien au-delà de ce qui est prescrit officiellement. Sayragul Sauytbay, une directrice d'école chinoise d'ethnie kazakhe, qui a été internée au motif que son mari et ses enfants étaient au Kazakhstan, a été choisie comme enseignante – une possibilité explicitement mentionnée dans la circulaire, qui préconise, en raison de la pénurie de professeurs, d'en choisir parmi les détenus.
Le centre dans lequel elle est restée quatre mois début 2018 ne permettait aucune visite des familles, ni aucun appel vocal ou vidéo : *« Si des proches venaient s'enquérir à votre sujet, ils étaient eux aussi détenus. Et vous ne les voyiez pas. C'était la règle dans ce centre »,* explique-t-elle. Les policiers en armes étaient présents partout : ils venaient régulièrement chercher des étudiants dans sa classe pour les interroger.Tursunay Ziavdun, une Ouïgoure libérée en décembre 2018 après onze mois d'internement dans un centre de formation et d'éducation de Kunès (ouest du Xinjiang), explique que les détenus de la zone dite *« très stricte »* étaient en uniforme rouge, ceux de la *« zone stricte »* en jaune, et ceux de la zone *« normale »* en bleu :*« Les uniformes rouges sont enchaînés quand ils sont emmenés dehors ou à des interrogatoires, chaque fois accompagnés par deux policiers en armes »,* explique-t-elle par vidéo depuis le Kazakhstan où elle a rejoint son mari. Comme Sayragul Sauytbay, Mme Ziavdun confirme que les salles de classes, qui contenaient une quarantaine de personnes, étaient entourées d'une grille qui séparait le professeur des « étudiants » et que des gardes en armes veillaient. Elle pouvait toutefois parler par vidéo à ses proches une fois par mois.
Les détenus sont soumis à une « *éducation idéologique »,*explique la circulaire. Ils doivent par ailleurs étudier le mandarin, les lois chinoises et acquérir certaines compétences professionnelles. Orinbek Koksebek, un Kazakh de Chine qui avait pris la nationalité du Kazakhstan et a été interné après être revenu en Chine, a raconté en 2018 au *Monde*avoir dû apprendre par cœur trois chansons communistes parce qu'il parlait très mal le chinois. Toute une partie des cours portaient sur la « *pensée de Xi Jinping et le XIXe congrès »*, explique Sayragul Sauytbay.
La circulaire mentionne l'importance de *« la repentance et de l'aveu »* des étudiants afin qu'ils comprennent *« le caractère illégal, criminel et dangereux de leur comportement passé »*. *« Cela s'appelait l'autoréflexion. Il fallait penser à ce que l'on avait pu faire de mal, à nos fautes, en mettant les mains sur le mur, pendant deux heures. Puis, après, il fallait l'écrire et le donner au professeur. Personne n'était coupable de quoi que ce soit. Mais tout le monde était forcé de trouver quelque chose, des fautes qui n'avaient pas été commises. Et ils étaient punis »*, poursuit Mme Sauytbay. Les témoignages confirment que tout acte religieux est entièrement proscrit : une parole, une prière, peut envoyer en détention.
Le document secret mentionne des punitions pour ceux *« qui ne comprennent pas, ont des attitudes négatives ou ont des velléités de résistance »*. Ils doivent être soumis à des méthodes appropriées de type*« tous contre un »*, pour s'assurer d'être *« transformés par l'éducation »*. Toute une rubrique porte également sur la discipline, le comportement et les manières, qui non seulement sont extrêmement strictes, mais donnent lieu à des évaluations, selon un système complexe de points.
En l'absence de toute possibilité de recours pour les détenus et leur famille, le système est d'une perversité extrême, un mélange de camp militaire et de prison secrète. A son arrivée en camp, Orinbek Koksebek a été enchaîné aux pieds pendant sept jours. Il a été envoyé à six reprises au cachot. Sayragul Sauytbay a décrit l'existence d'une *« chambre noire »,* une salle de torture dans le camp où elle a travaillé. Mme Sauytbay a été battue sur le corps et la tête avec une matraque électrique en caoutchouc dur – puis privée de nourriture pendant deux jours.
La chambre de torture comportait la classique « chaise du tigre » chinoise – qui maintient le prisonnier avec une barre de fer au-dessus des cuisses – mais celle-ci envoyait des chocs électriques. Plusieurs types d'instruments étaient à portée de main : une sorte de baïonnette, un bâton muni d'un

fil de fer à l'extrémité, un tabouret avec des pics. De nombreux détenus font par ailleurs état de viols de jeunes femmes par les gardes.

« Compléter l'éducation »

La circulaire établit également les conditions qui permettent à un *« étudiant »* de*« compléter »* son éducation : celle-ci doit durer *« au moins un an »* et ne s'applique qu'à ceux qui ont intégré la *« zone normale »*. Ensuite, plusieurs conditions simultanées doivent être réunies : le*« problème »* qui a donné lieu à l'*« éducation »* doit avoir été résorbé, les notes de*« transformation idéologique »,* de *« résultats scolaires »,* d'*« obéissance »* et de *« discipline »* répondre aux niveaux exigés.
Ces données sont ensuite*« entrées dans la plate-forme intégrée des opérations conjointes »* : *« si celle-ci ne détecte pas de nouveau problème »,* alors le dossier est transmis aux bureaux de la formation et de l'éducation des divers échelons régionaux. *« Ce sont des critères incroyablement stricts »,* note le chercheur Adrian Zenz, qui a été parmi les premiers à confirmer l'existence des centres d'éducation et leur caractère coercitif en épluchant les appels d'offres et les budgets officiels des localités du Xinjiang.
Tous les étudiants qui*« complètent leur formation »*, précise le document chinois, sont alors orientés vers une *« session intensive de renforcement des compétences »* de trois à six mois. Les préfectures sont encouragées à mettre en place des centres permettant*« le placement des étudiants »*. Des dizaines d'entreprises de l'intérieur de la Chine reçoivent des subventions pour s'installer dans des parcs industriels et recruter cette main-d'œuvre locale forcée.
Aucune statistique ne permet de savoir quel pourcentage d'« étudiants » ont été transférés vers de la formation professionnelle, libérés, ou condamnés à des peines carcérales à purger sur place – ou en prison, ou sous d'autres formes de détention. Les données officielles chinoises montrent toutefois que les arrestations au Xinjiang ont été multipliées par huit rien qu'entre 2016 et 2017 – pour atteindre 21 % du total de l'ensemble de la Chine.*« Plusieurs centaines de milliers de personnes ont été la cible de poursuites judiciaires ces deux dernières années et demie au Xinjiang »,*explique le chercheur Gene Bunin, créateur d'une base de données des victimes du Xinjiang, qui répertorie les cas connus de personnes disparues. *« On sait qu'il y a eu des libérations importantes des centres de formation et d'éducation. Le problème toutefois, c'est que ceux qui sont libérés et renvoyés chez eux sont loin d'être libres : ils sont sous des formes variées de contrôle, de résidence surveillée, se voient imposer des restrictions pour se déplacer de ville en ville. Beaucoup sont en piteux état psychologique et physique, ils vivent dans la peur d'être denouveau détenus »,* explique-t-il. Dans un nouveau rapport rendu public ce dimanche 24 novembre et intitulé « Laver les cerveaux, purifier les cœurs », le chercheur Adrian Zenz en étudiant les documents administratifs de plusieurs localités du Xinjiang a identifié quels individus étaient classés comme*« détenus pour rééducation »*, « *arrêtés »* ou *« en train de purger une peine »*.
Il s'agit d'une majorité d'hommes (six fois plus que de femmes), âgés de 25 à 50 ans. Ce *« qui confirme*, écrit Adrian Zenz, *que la campagne de rééducation et d'internement vise clairement les figures d'autorité, et non pas seulement la jeune génération censée avoir besoin de "formation", comme le prétend Pékin »*. Dans ses conclusions, M. Zenz incite à réévaluer le nombre de personnes qui ont été internées au Xinjiang à 1,8 million, soit environ 20 % de la population adulte ouïgoure et kazakhe.
Ce qu'il faut savoir
Le Consortium internationaldes journalistes d'investigation (ICIJ) et 17 médias partenaires révèlent une série de documents classés secrets internes à l'Etat-Parti chinois, les « China Cables » sur le fichage et la surveillance totale de la population du Xinjiang et la mise en place de camps d'internement.
Une circulaire décrit en 26 points l'univers carcéral et les méthodes d'endoctrinement et de filtrage mis en place depuis 2017.

Quatre directives portent sur la mise en place d'une base de données exhaustive sur les Ouïgours et les dizaines de milliers d'interpellations qu'elle permet.

La Chine souligne l'efficacité de ses mesures

Contacté par l'ICIJ et le *Guardian*, au nom de tous les médias partenaires, le gouvernement chinois a qualifié les documents de*« pure invention »* et de *« fake news »*. Il note que la région*« était devenue un champ de bataille – des milliers d'incidents terroristes se sont produits au Xinjiang entre les années 1990 et 2016, et des milliers de personnes innocentes ont été tuées. Donc il y a une demande énorme chez les habitants du Xinjiang pour que le gouvernement prenne des mesures résolues pour régler le problème »*. Le communiqué souligne que*« depuis que les mesures ont été prises ces trois dernières années, il n'y a pas eu un seul incident terroriste »* et soutient que la liberté de religion est pleinement respectée. *« Ces mesures ont été efficaces. Le Xinjiang est bien plus sûr. L'an dernier, le tourisme a progressé de 40 %, et le PIB local a augmenté de plus de 6 %. »*

Ailleurs dans le monde : En Chine, la reconnaissance faciale envahit le quotidien

De la sécurité publique au paiement en caisse automatique, la technologie est utilisée tous les jours dans la société chinoise.

Par Simon Leplâtre Publié le 09 décembre 2017 à 10h30 - Mis à jour le 10 décembre 2017 à 06h35

Shanghaï, un après-midi d'automne. Alors que l'agent qui fait la circulation a le dos tourné, un homme entre deux âges traverse au rouge. Quelques secondes plus tard, son visage apparaît sur les écrans installés dans les arrêts de bus du quartier. Il y restera, en alternance avec celui d'autres contrevenants, jusqu'à ce qu'il aille s'acquitter d'une amende de 20 yuans (2,60 euros) au commissariat du quartier.

D'autres villes de Chine ont adopté le système. Parfois moins discrètement, comme Shenzhen, la métropole qui fait face à Hongkong, où le visage des piétons trop pressés apparaît sur un écran géant au coin des carrefours.

La méthode ne dérange pas. *« Il ne faut pas traverser au rouge, donc je ne vois pas où est le problème »*, commente un jeune Shanghaïen en haussant les épaules. La plupart des passants ne sont pas dérangés par le caractère intrusif de la technologie, tant qu'elle vise à faire respecter la loi.

Cette acceptation du public est l'un des facteurs qui permet à l'empire du Milieu d'avoir une longueur d'avance dans le domaine de la reconnaissance faciale. *« En Chine, les gens sont moins préoccupés par les questions de vie privée, ce qui nous permet d'aller plus vite »*, déclarait Xian-Sheng Hua, directeur de la branche intelligence artificielle d'Alibaba, le leader chinois du commerce en ligne, début octobre lors d'un forum professionnel à Amsterdam.

Et la Chine va vite : aujourd'hui, la plupart des gouvernements locaux sont équipés de systèmes de reconnaissance faciale. De plus en plus d'institutions se laissent tenter. Installée dans les dortoirs d'universités, cette technologie remplace désormais les concierges, pour savoir à quelle heure rentrent les étudiants. De plus en plus, elle prend la place des badges pour rentrer dans les bâtiments d'entreprises.

Un système très bon marché

Cet été, une utilisation inattendue du système a fait les gros titres : des toilettes publiques à Pékin ont installé un distributeur de papier toilette à reconnaissance faciale pour lutter contre les abus : pas plus de 60 cm toutes les neuf minutes pour une même personne… D'autres toilettes « 2.0 » ont suivi dans le pays…

Si le système se fait si envahissant en Chine, c'est parce qu'il est désormais très bon marché. Pour les fonctions les plus basiques, une webcam équipée d'un logiciel simple suffit. *« L'important, ce sont les algorithmes*, explique Leng Biao, professeur de vision informatique à l'école d'ingénierie de l'université Beihang de Pékin. *Quand il s'agit de vérifier l'identité d'une personne dont on a la photo, la reconnaissance faciale est très fiable, on trouve même des logiciels gratuits sur Internet. »*

Reconnaître une personne parmi une base de données de millions d'individus est une autre affaire, a fortiori s'il s'agit de la population chinoise totale, qui compte 1,4 milliard d'habitants. *« Imaginez : même si vous n'avez que 10 % de marge d'erreur, appliqué à la population du pays, c'est énorme !* remarque Leng Biao. *Et sur une telle population, il y a forcément des gens tellement identiques que même leurs parents ne les reconnaîtraient pas ! »*

Aujourd'hui, c'est plutôt le premier type d'applications qui explose : au-delà des aéroports, des entreprises privées s'y mettent. En Chine, on peut ainsi retirer de l'argent dans les distributeurs de China Construction Bank avec son visage. Quant à Alipay, la branche financière d'Alibaba, elle teste en ce moment cette option pour payer dans ses petits supermarchés haut de gamme « Hema ».

Des courses sans téléphone, ni portefeuille

Dans l'un de ces magasins au nord de Shanghaï, les terminaux de paiement sont équipés de caméras 3D, comme sur le dernier iPhoneX. Après avoir enregistré votre visage, dont Alipay vérifie la conformité avec votre carte d'identité, vous pouvez faire vos courses sans votre téléphone, ni votre portefeuille. A la sortie de Hema, une jeune femme venue déjeuner dans cette épicerie restaurant, trouve cette fonction *« amusante »*, mais pas vraiment plus efficace que le paiement mobile, lui aussi rapide et déjà répandu en Chine.

Pour l'instant, une fois votre identité reconnue par la machine, il faut encore entrer votre numéro de téléphone, une *« double vérification »* imposée par la loi chinoise, explique une communicante d'Alipay, qui rappelle qu'il s'agit là d'un projet pilote.

Mais Alibaba, et son concurrent le plus proche, JD.com, travaillent tous deux sur un projet de supérettes entièrement automatisées. Il est encore en phase de tests dans les locaux des deux leaders du commerce en ligne, où l'on entre et où l'on paie grâce à la reconnaissance faciale uniquement.

JD.com s'apprête aussi à vendre un service fondé sur la vision artificielle, permettant aux exploitants de supermarchés d'analyser le comportement de leurs clients, d'afficher des publicités ciblées grâce à des écrans munis de caméras, et même d'analyser la population qui passe devant leurs magasins…

Un marché à la croissance exponentielle

D'après une étude du cabinet Analysys, le marché de la reconnaissance faciale dépassait le milliard de yuans en 2016 (128 millions d'euros), et devrait être multiplié par cinq d'ici à 2021. Pour autant, si nombre d'entreprises s'y mettent, rares sont celles qui ont de réelles capacités dans le domaine, pointe le professeur Leng Biao. *« Une dizaine tout au plus, ont les moyens de créer leurs propres algorithmes, et de les faire évoluer »*, estime-t-il.

Deux sociétés, en particulier, ont pris de l'avance : Sensetime, et Megvii sont devenues des licornes en 2017, dépassant le milliard de dollars de valorisation. Les deux entreprises utilisent l'intelligence artificielle pour

affiner leur analyse d'image, et elles ne cessent d'étendre leurs activités, au fil de tours de table qui rassemblent géants de la tech et fonds d'investissements gouvernementaux.

Sensetime, installée à Hongkong, collabore avec une quarantaine de gouvernements locaux, et elle fournit en parallèle des logiciels permettant d'améliorer les photos aux principales marques chinoises de smartphones, Huawei, Oppo, Vivo et Xiaomi.

Même schéma pour Megvii, dont le siège est à Pékin, qui travaille avec Alibaba sur des systèmes de paiement d'un côté, et revendique 3 000 arrestations grâce à sa technologie, de l'autre. *« Nous voulons être les yeux et le cerveau des villes, afin que toutes les prises de vue urbaines deviennent des données sur la ville »*, détaille un de ses porte-parole.

90 % de précision en quelques secondes

En matière de sécurité publique pourtant, le leader est une petite société de Shanghaï. Malgré ses technologies de pointe, IsVision n'a ni « showroom » ni écrans plats pour impressionner les visiteurs. A la place, le mur de l'entrée est recouvert de plaques officielles dorées célébrant, par exemple, *« la meilleure entreprise informatique de Shanghaï »*. Pour ses clients, des responsables de polices locales, ces distinctions valent bien des discours.

Fondée en 1999, l'entreprise sert aujourd'hui vingt-deux provinces et municipalités indépendantes chinoises, sur trente-quatre, dont le Tibet et le Xinjiang. Dans les locaux, des ingénieurs montrent l'application qui équipe les smartphones de la police, permettant d'effectuer des contrôles d'identité rapides. Un autre outil équipe les caméras de surveillance : une fois votre visage ajouté à une « liste noire », impossible de passer devant la caméra sans déclencher une alarme !

IsVision a remporté son plus gros contrat en 2015 : le ministère de la sécurité publique lui a commandé un système de reconnaissance faciale national. Objectif : 90 % de précision en quelques secondes. *« Nos capacités sont les plus importantes du monde, tout simplement parce que personne n'a affaire à une telle quantité d'informations ! »*, explique fièrement Liu Shuchang, le directeur des ventes.

« Pour la police, la reconnaissance faciale est très pratique. Elle ne possède pas les empreintes digitales de tous les Chinois, alors que grâce aux cartes d'identité, tous les visages sont connus. Notre algorithme peut comparer 1,4 milliard de personnes en 2 ou 3 secondes ! », poursuit-il.

« Prévenir le crime »

Pour les autorités, la reconnaissance faciale s'inscrit dans un système plus large visant, affirment-elles, à *« prévenir le crime »*. *« En utilisant des systèmes et des équipements intelligents, on peut savoir à l'avance qui pourrait être un terroriste, qui pourrait faire quelque chose de mal »*, avait ainsi décrit sans fard Li Meng, vice-ministre des sciences et des technologies, à la mi-juillet.

Grâce à l'intelligence artificielle, les autorités peuvent analyser de plus en plus de données à la fois publiques et provenant d'entreprises privées, contraintes par la loi de livrer leurs données sur demande. *« Nous sommes en train de passer d'une approche passive, réactive, de la sécurité, à une approche active : maintenant, grâce à des listes noires de suspects, on peut agir avant que les crimes ne soient commis »*, assure Liu Shuchang. Vertigineux.

Simon Leplâtre (Shanghaï, correspondance)

Est-il possible d'échapper à la vidéosurveillance en Chine ?

Big Browser

La BBC a tenté l'expérience, qui n'a bien sûr pas duré longtemps dans un pays équipé de millions de caméras fonctionnant à l'intelligence artificielle, dont la reconnaissance faciale.

Publié le 11 décembre 2017 à 17h00 - Mis à jour le 11 décembre 2017 à 17h04 Temps deLecture 1 min.

Dans la ville de Guiyang, à chaque feu rouge, les caméras scannent les visages des conducteurs. Damir Sagolj / REUTERS

En Chine, l'omniprésence des caméras CCTV – 170 millions à travers le pays, et 400 millions de plus prévues dans les trois ans –, ajoutée au développement de technologies de reconnaissance faciale et d'intelligence artificielle a abouti à ce que la BBC décrit comme *« le réseau le plus étendu et sophistiqué de vidéosurveillance au monde »*.

Le correspondant de la BBC en Chine, John Sudworth, a voulu illustrer le fonctionnement de ces caméras (à voir en intégralité ici). Il a pu accéder aux locaux de la police de la ville de Guiyang, où les près de 3 millions de citoyens sont constamment sous l'œil des caméras installées par la municipalité, comme c'est le cas dans presque toutes les grandes villes chinoises.

How long can a BBC reporter stay hidden from CCTV cameras in China? @TheJohnSudworth has been given rare access to… https://t.co/vZB8T28rLW
— BBCWorld (@BBC News (World))

Avec la complicité des policiers de Guiyang, Sudworth accepte d'être un cobaye dans une expérience pour que chacun comprenne l'efficacité, et l'omniprésence, de la vidéosurveillance. Il se fait prendre en photo dans les locaux de la police et son visage est ajouté à la base de données où figurent ceux de tous les autres habitants de la ville. Pas besoin d'organiser de séances photo, ce sont celles de leurs cartes d'identité.

Combien de temps le journaliste pourra-t-il marcher dans la ville avant d'être repéré ? En descendant de sa voiture, près du centre-ville, il tente d'aller jusqu'à la station de bus. Dès le premier pont, il repère trois caméras. Et constate :

« Ça ne sert à rien d'essayer de se cacher ici. »

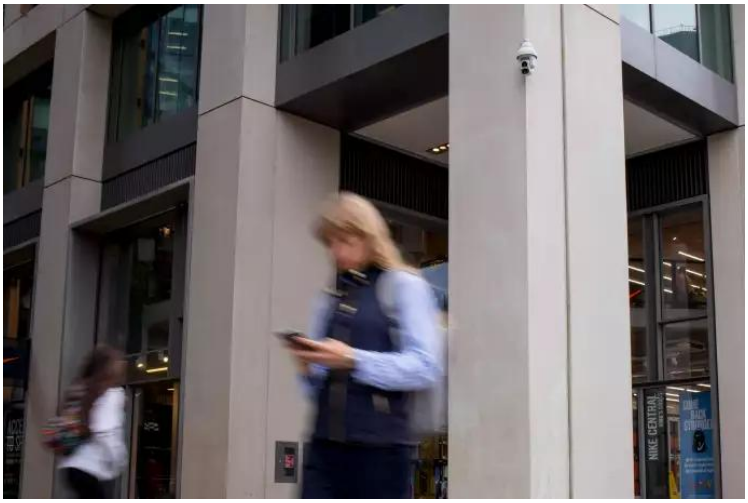
Sept minutes après avoir posé un pied sur le trottoir de Guiyang, plusieurs policiers l'entourent. Même s'il n'avait pas quitté sa voiture, Sudworth ne serait pas resté incognito beaucoup plus longtemps. A chaque feu rouge, les caméras scannent les visages des conducteurs.

Dans d'autres villes, comme Shanghaï ou Shenzhen, les visages des piétons qui traversent au rouge sont projetés sur les abribus, ou sur des panneaux géants, tant qu'ils n'ont pas payé leur amende…

En catimini, le Royaume-Uni s'impose en champion de la reconnaissance faciale

En quelques années, et en toute discrétion, le pays est devenu l'un des plus en pointe dans cette technologie. Les logiciels ont tant progressé qu'ils inquiètent les défenseurs des libertés individuelles pour leurs capacités de surveillance de masse inégalées.

Par Cécile Ducourtieux Publié le 03 septembre 2019 à 02h27 - Mis à jour le 03 septembre 2019 à 10h55



Une caméra CCTV à la gare de King's Cross Saint Pancras, à Londres, le 16 août. TOLGA AKMEN / AFP

Beaucoup d'usagers de l'Eurostar connaissent King's Cross Saint Pancras. La gare terminus par laquelle ils débarquent à Londres se situe au cœur de ce quartier en pleine ébullition. Google y a déplacé son siège, la fameuse école d'art Central Saint Martins se trouve à deux pas, comme la boutique de souvenirs Harry Potter devant laquelle les fans du petit sorcier patientent dans la file d'attente pour s'offrir une réplique de son écharpe ou un selfie devant l'entrée du quai 9 3/4 d'embarquement vers Poudlard.

Personne, avant des révélations du *Financial Times*, mi-août, ne soupçonnait qu'en ce lieu grouillant de monde une expérience de reconnaissance faciale était menée. Depuis quand, dans quel objectif et avec combien de caméras activées ? Mystère. Interrogée par le quotidien britannique, l'agence Argent, chargée de la mise en valeur du site, s'est contentée d'affirmer que la technologie *« vise à assurer la sécurité du public ».* Jointe quinze jours plus tard, une porte-parole de l'agence ajoute : *« King's Cross collabore activement avec les bureaux* [du régulateur britannique des données personnelles] *Information Commissioner's Office* [ICO]. *»*

Ce dernier a en effet annoncé l'ouverture d'une enquête, dès la publication de l'article du quotidien économique. *« Scanner les visages des gens quand ils vaquent en toute légalité à leurs activités quotidiennes, avec l'objectif de les identifier, peut représenter un danger potentiel pour la vie privée, et cela doit tous nous concerner,* a déclaré, mi-août, Elizabeth Denham, la patronne de l'ICO, dans un communiqué. *Spécialement si ces technologies sont utilisées sans que les gens soient tenus au courant ni n'en comprennent le fonctionnement. »*

D'autres révélations, toutes aussi troublantes, ont suivi au cœur de l'été. Canary Wharf, l'énorme quartier d'affaires de l'est de Londres, serait lui aussi sur le point de s'équiper, toujours selon le *Financial Times*. Le 16 août, l'ONG Big Brother Watch listait les lieux, un peu partout au Royaume-Uni, où la technologie était désormais utilisée, à l'insu de *« millions de consommateurs » : « Il s'agit d'une vraie épidémie »,* concluait l'association londonienne.

Visages scannés

Des essais ont ainsi été menés en 2018 dans l'enceinte du Meadowhall, à Sheffield, l'un des plus vastes centres commerciaux du nord de l'Angleterre. Mais aussi au Trafford Center de Manchester, un autre temple du shopping, qui a potentiellement pu concerner 15 millions de personnes. A Birmingham, le centre de conférences Millennium Point est également concerné, tout comme des casinos et des maisons de paris (la chaîne Ladbrokes). Plus surprenant, le Word Museum, à Liverpool, a utilisé la technologie en 2018, au sein d'une exposition consacrée au premier empereur de Chine et à son armée de terre cuite.

Fin août, le *Sunday Times* racontait encore que Manchester City, le club de Premier League, comptait lui aussi utiliser la technologie pour limiter les files d'attente les jours de match à l'entrée de l'Etihad Stadium. Fournie par la société texane Blink Identity, elle permettrait de scanner 50 visages à la minute et de distinguer les détenteurs de billets des autres.

En quelques années, et en toute discrétion, le Royaume-Uni est devenu l'un des pays du monde les plus en pointe dans cette technologie permettant d'identifier automatiquement des personnes à partir de captures de leur visage. Les logiciels concernés ont tant progressé qu'ils inquiètent au plus haut point les défenseurs des libertés individuelles pour leurs capacités de surveillance de masse inégalées. Surtout quand les caméras de reconnaissance sont couplées à d'énormes bases de données de visages enregistrés. Les médias occidentaux ont rapporté, début 2019, que la Chine en faisait usage à l'encontre des populations musulmanes ouïgoures.

C'est d'abord la police britannique, qui, ces trois dernières années, a procédé à de nombreux tests, notamment la police du Grand Londres (lors des carnavals de Notting Hill en 2016 et en 2017) et la police du Pays de Galles du Sud. Officiellement, pour améliorer la sécurité des citoyens britanniques. Mais, désormais, nombre d'opérateurs privés s'y mettent, en toute impunité. *« En principe, les caméras dotées d'un système de reconnaissance faciale scannent les visages, puis les confrontent à des bases de données,* explique Pete Fussey, professeur de sociologie à l'université d'Essex. *Le problème, c'est que, bien souvent, nous ignorons de quelles bases de données il s'agit et quel est le véritable objectif de la surveillance* [commercial ? sécurité ?]. *En grande partie parce que ces technologies sont vendues à des sociétés privées qui les déploient dans des espaces privés. »*

420 000 caméras à Londres

Comment un pays réputé pour son absence de carte d'identité peut-il être à ce point en pointe ? L'énorme réseau de caméras de vidéosurveillance déjà existant (les « CCTV ») aide considérablement au déploiement de la nouvelle technologie. Londres en compte ainsi 420 000 dans le métro, les écoles, les supermarchés, les entrées d'immeuble… Grâce à elles, la capitale britannique est la ville au monde la plus surveillée après Pékin (470 000 caméras), selon une étude du think tank américain Brookings Institution datant de 2017. *« La reconnaissance faciale est pour l'essentiel une technologie logicielle, elle peut donc être installée sur les caméras existantes. Pour bien fonctionner, elle nécessite cependant une haute qualité d'optique, donc elle est souvent utilisée avec des caméras haut de gamme »,*précise néanmoins Pete Fussey.

Ces caméras ont été déployées massivement à partir des années 1990, notamment pour prévenir les attentats de l'Armée républicaine irlandaise (l'IRA). Le réseau s'est densifié après les attentats de Londres de 2005. *« 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. Il semble qu'aujourd'hui il n'y ait pas d'autre pays, à part la Chine, qui fasse une utilisation aussi inconsidérée de la reconnaissance faciale »,* déplore Silkie Carlo, directrice de Big Brother Watch.

Qu'en pensent les citoyens, pour la plupart dans l'ignorance de ces expériences tous azimuts ? Le seul sondage sérieux, encore que très restreint, date de mai. Il a été mené par le London Policing Ethics Panel (un organe indépendant censé organiser le dialogue entre la police de Londres et ses habitants), auprès d'un panel de 1 092 Londoniens.

Que révèle-t-il ? Un peu plus d'un tiers seulement des personnes interrogées s'inquiètent des expérimentations menées par la police du Grand Londres depuis 2016. Mais la préoccupation monte chez les jeunes (16-24 ans), les habitants*« d'origine asiatique ou noire »*. Et 38 % des jeunes du panel déclarent qu'ils éviteraient de participer à une manifestation si la police y utilisait la reconnaissance faciale. Hannah Couchman, membre de l'association britannique Liberty, en est convaincue : *« Le public est de plus en plus concerné. Le fait que San Francisco, en Californie, aux portes de la Silicon Valley, ait choisi d'interdire l'usage de la reconnaissance faciale est un signal important. »*

Absence de cadre juridique spécifique

Les militants sont d'autant plus inquiets qu'au Royaume-Uni la technologie prospère en l'absence de tout cadre juridique spécifique. Les lois existantes ne sont pas adaptées, estime Daragh Murray, chercheur, comme M. Fussey, au Centre des droits humains de l'université d'Essex. *« Le règlement européen RGPD*[règlement général de protection des données, entré en vigueur en mai 2018]*s'applique au traitement des données privées, comment elles sont stockées ou partagées. Il ne porte pas sur le fait de savoir s'il est approprié ou non d'utiliser la reconnaissance faciale. »*

Donner aux citoyens le droit de ne pas être « flashé » par des caméras biométriques ? La Commission européenne y réfléchit, assurait le *Financial Times,* fin août. C'est illusoire, estime M. Murray : comment s'exclure volontairement d'une expérimentation de reconnaissance faciale, quand elle est pratiquée dans un lieu public comme King's Cross ? A part en évitant le quartier ou en dissimulant systématiquement son visage ? *« Pour que les citoyens soient protégés, la loi ne doit pas viser à leur donner un droit individuel de retrait, mais à encadrer les pratiques des acteurs choisissant de déployer cette technologie »,*explique M. Murray. Liberty et Big Brother Watch prônent une interdiction totale dans les lieux publics.

Encore faudrait-il que les politiques s'en mêlent. Mais, au pays du Brexit, *« les députés n'ont pas le temps pour des débats sérieux à Westminster »,* déplore Silkie Carlo. Certains ont émis des réserves, comme la chef du Parti vert, Caroline Lucas, et le conservateur David Davis. En attendant qu'ils prennent le sujet à bras-le-corps, c'est la justice qui pourrait trancher. Pour la première fois, un cas a été porté devant les tribunaux. Ed Bridges, un résident de Cardiff (Pays de Galles), a déposé plainte en mai contre la police du Pays de Galles du Sud, auprès d'un tribunal local, après avoir été flashé durant une manifestation contre le commerce des armes.

Cécile Ducourtieux (Londres, correspondante)

Comment fonctionnent les technologies de reconnaissance faciale ?

Les principaux moyens techniques actuels

Il est trompeur de parler de reconnaissance faciale au singulier : il existe plusieurs modes de fonctionnement différents, qui n'ont pas tous le même impact sur la vie privée.

Par Martin Untersinger , Marianne Boyer et Romain Imbach Publié le 15 novembre 2019 à 10h22 - Mis à jour

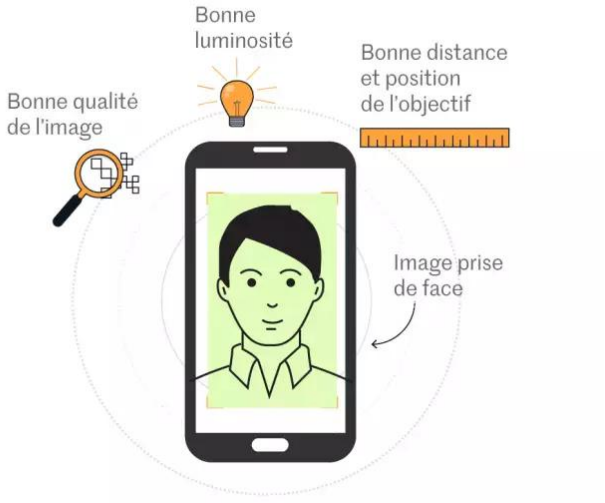
On parle de plus en plus, en France, des technologies de reconnaissance faciale. Le secrétaire d'Etat au numérique, Cédric O, aimerait que la loi permette de mener davantage d'expérimentations, tandis que la Commission nationale de l'informatique et des libertés (CNIL) a publié son « code de la route » en la matière.

Derrière le terme passe-partout de « reconnaissance faciale » se cachent des technologies différentes. Techniquement voisines, elles ne soulèvent pas du tout les mêmes enjeux en matière de protection des données et de libertés publiques.

Le premier usage, le moins conséquent en matière de protection des données personnelles, consiste en la vérification de l'identité en comparant l'image d'une personne avec celle qui est stockée, par exemple dans son passeport. Dans ce cas, il n'y a pas obligatoirement constitution d'une base de données, simplement une comparaison. Pour la CNIL, la solution à privilégier est justement celle de stocker le gabarit du visage sur des *« supports possédés par les individus et leur en assurant la maîtrise »* (par exemple leur téléphone) et qui permet à l'utilisateur de ne pas diffuser l'image de son visage à des tiers. C'est ce type de mécanisme qui permet de déverrouiller certains téléphones.

Techniquement, c'est le dispositif de reconnaissance faciale le plus au point, même s'il n'est pas fiable à 100 %. Mais comme pour tous les usages de cette technologie, la fiabilité du dispositif dépend directement de la qualité de l'image prise comme de celle à laquelle on la compare.

Conditions de paramètres à prendre en compte pour une optimisation de réussite :

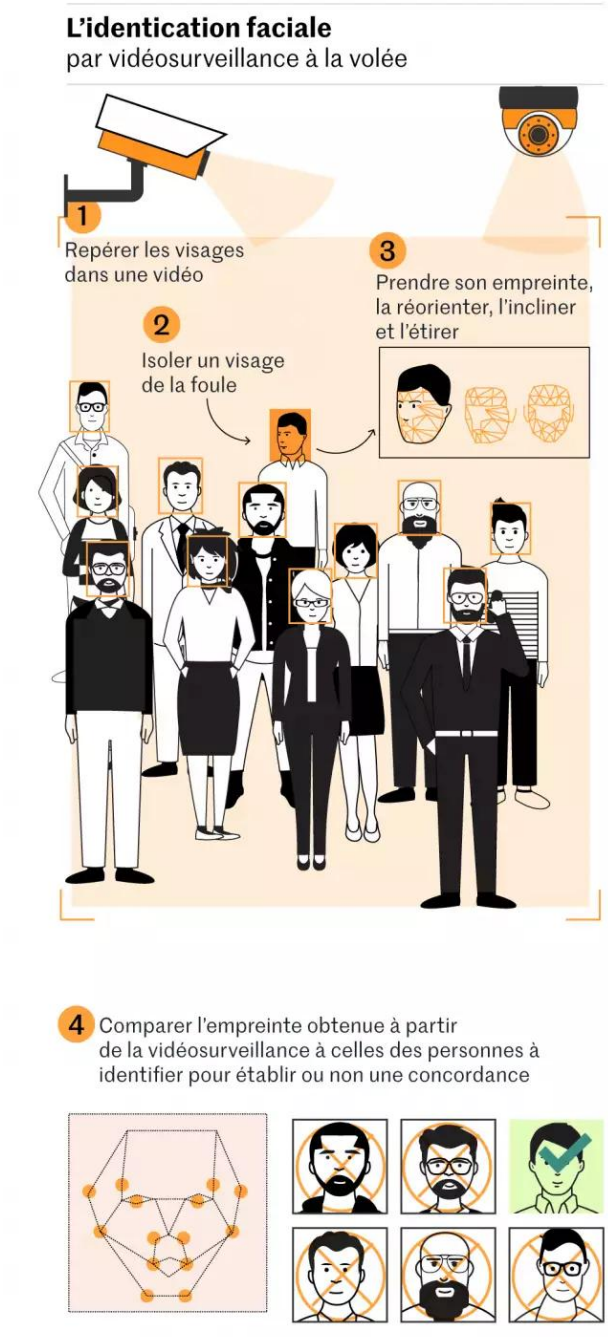


Il est également possible de comparer l'image d'un individu avec une base de données préalablement constituée, par exemple dans le cadre d'un portique de sécurité biométrique dans une entreprise qui compare chaque personne se présentant à une base de personnes autorisées à pénétrer dans l'enceinte de la société.

La CNIL, chargée de la protection des données personnelles, est beaucoup plus pointilleuse dans ce cas. L'image du visage est en effet une donnée biométrique : à l'inverse d'un mot de passe, on ne peut pas en changer si la base de données est piratée ! Le droit européen accorde une protection très importante à ces données, qualifiées de « sensibles ». Pour avoir le droit de les manipuler, il faut une très bonne raison (une exigence de sécurité par exemple), ne pas avoir la possibilité de recourir à une autre technologie, prendre des mesures drastiques pour sécuriser la base de données…

Il est aussi possible, dans le cadre de procédures judiciaires, de recourir à la reconnaissance faciale : les enquêteurs peuvent comparer une photo (issue d'un réseau social, d'une vidéosurveillance…) à celles contenues dans le fichier de traitement d'antécédents judiciaires, le seul actuellement à pouvoir être interrogé pour la reconnaissance faciale.

A l'autre bout du spectre, se trouve la reconnaissance faciale à la volée, dans l'espace public, couplée à la vidéosurveillance. Actuellement, ce type de technologie n'est pas employé en France, mais pourrait peut-être l'être dans le futur. C'est l'utilisation la plus problématique de la reconnaissance faciale car elle se fait à l'insu des passants, et nécessite pour fonctionner de traiter les données biométriques – et potentiellement d'identifier – de toutes les personnes passant dans le champ de la caméra. Certains responsables politiques, comme Valérie Pécresse, présidente de la région Ile-de-France, la réclament.



C'est ce mode de reconnaissance faciale qui est, à l'heure actuelle, le moins fiable car la prise de vue se fait dans un environnement dit « non contrôlé » (avec des variations de lumière, d'orientation, des caméras basse définition, des personnes en mouvement), qui nécessite de lourds traitements. Les technologies d'apprentissage automatique ont

permis cependant d'importants progrès ces dernières années et c'est ce type de dispositif qui est déployé dans certaines zones de Chine.

Martin Untersinger , **Marianne Boyer** et **Romain Imbach**

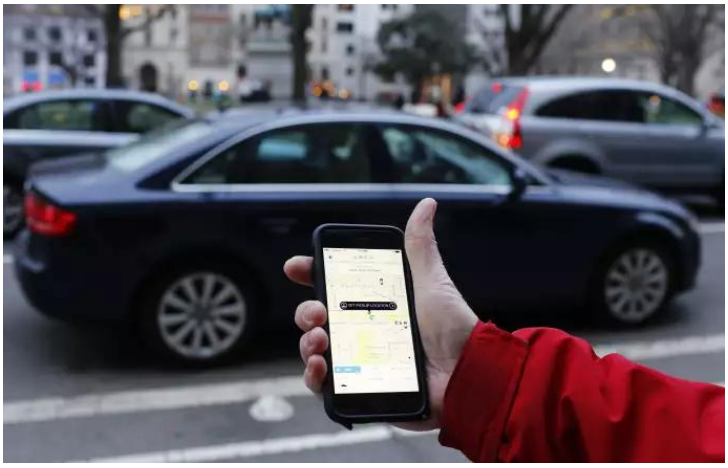
Quelles images sont utilisées ?

Les images captées dans les aéroports, les rues et tous les espaces publics, les téléphones et les réseaux numériques

Transport, santé, sécurité... le grand bazar des données urbaines

Numériser la ville ne suffit pas à la rendre intelligente. Dans une société de la connexion permanente, le big data urbain inquiète les citoyens.

Par Claire Legros Publié le 04 février 2018 à 17h00 - Mis à jour le 05 février 2018 à 11h31



Commande d'un VTC sur l'application Uber. Andrew Caballero-Reynolds / AFP

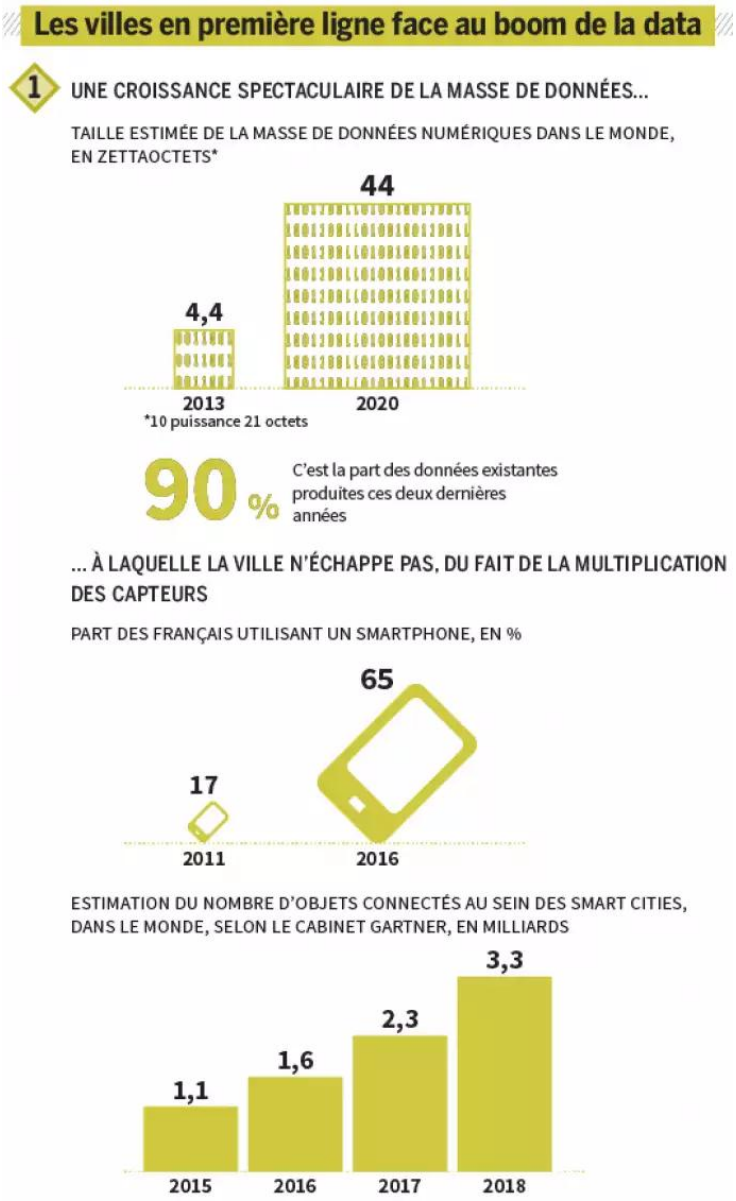
Les joggers adorent Strava. Cette application d'origine américaine leur permet d'échanger leurs performances et de se retrouver sur les lieux de course en ville, puisque tout le monde est géolocalisé. Un réseau social du footing, avec cartes à l'appui, pour aider les collectivités à repérer les aménagements nécessaires aux pratiques sportives dans la ville. Seul problème, dévoilé le 27 janvier par un étudiant en sécurité internationale : on peut aussi y repérer les parcours des militaires qui font du sport près de leur base, au Mali ou en Afghanistan, ce qui n'est pas vraiment du goût des généraux.

Bienvenue dans le grand bazar des données urbaines. Issu des multiples capteurs disséminés dans nos véhicules, nos appartements et jusqu'au fond de nos poches avec nos smartphones, le déluge ininterrompu de données refonde les villes en profondeur. En échange de services de plus en plus efficaces, acteurs publics et privés amassent des informations sur nos trajets et habitudes.

Alors que responsables politiques et entreprises plébiscitent l'avènement des cités numériques, les habitants restent méfiants

Certains y voient la promesse réjouissante d'un trafic plus fluide, d'un habitat économe en énergie, d'une transparence des marchés publics, de relations plus étroites entre membres d'une communauté – comme les adeptes du jogging… Pour d'autres, c'est le cauchemar de cités panoptiques, façon Big Brother, qui est en train de se concrétiser.

Aucun secteur n'échappe à cette transformation radicale : consommation d'eau et d'énergie, mobilité, commerce, santé, sécurité… Mais numériser la ville ne suffit pas à la rendre intelligente. Dans une société de la connexion permanente, le big data urbain représente aussi une source d'inquiétudes. Alors que responsables politiques et entreprises plébiscitent l'avènement des cités numériques, les habitants restent méfiants, comme l'a montré une enquête, publiée en novembre 2017, de l'Observatoire société et consommation (L'Obsoco) et du cabinet d'études Chronos. Moins d'une personne interrogée sur trois souhaite partager ses données pour contribuer au bon fonctionnement de la « smart city ».

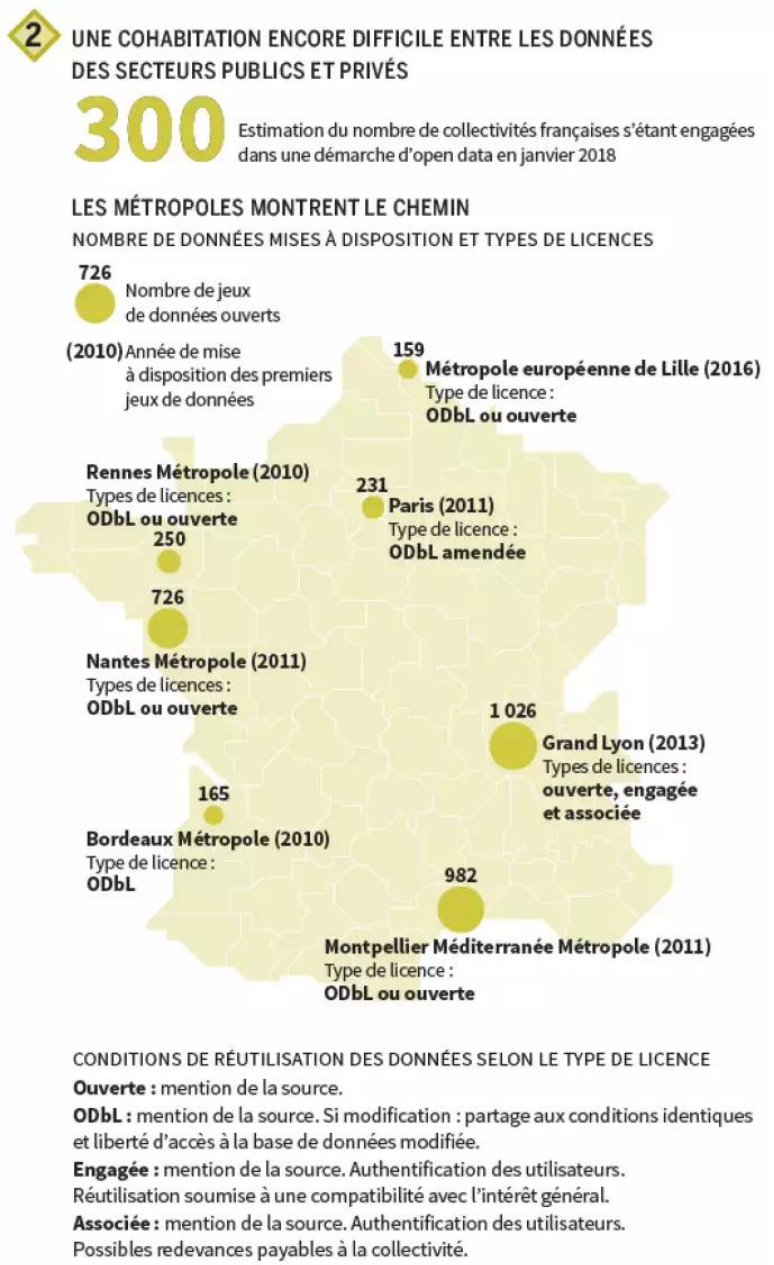


La ville connectée est-elle compatible avec la protection des libertés individuelles ? Doit-on soumettre les politiques publiques à la régulation statistique ? L'intérêt général peut-il se résumer à la somme des intérêts des utilisateurs d'applications ? Le citoyen est-il condamné à rester un pourvoyeur de données que l'on traque pour mieux l'orienter ? A la croisée du juridique, du politique et de l'éthique, ces questions sont au cœur du projet de la « smart city ».

Ouverture des données

Sur la plate-forme de données de la Ville de Paris, ouverte à tous sous certaines conditions, on trouve à la fois la liste des livres les plus réservés dans les bibliothèques, les marchés publics de plus de 20 000 euros ou les subventions accordées aux associations. Depuis une dizaine d'années, les grandes villes françaises ont basculé progressivement vers l'open data : après les avoir anonymisées et agrégées, elles publient les données collectées par leurs administrations. L'objectif de ce partage est double. Il s'agit à la fois de faire preuve de transparence et de stimuler l'innovation en suscitant de nouveaux services.

A Montpellier, la start-up LKSpatialist fait figure de modèle du genre. A partir des données cadastrales ouvertes par la ville, elle développe des logiciels d'aide aux agents immobiliers pour repérer en quelques clics les caractéristiques d'un logement : proximité d'une école, réglementations particulières… Elle est passée de 3 à 38 salariés en trois ans.



En théorie, la loi impose aux villes de plus de 3 500 habitants d'ouvrir leurs données en octobre 2018, de même qu'aux entreprises qui gèrent un service public – transports ou réseau d'eau. A ce jour, selon l'Observatoire de l'open data en France, qui doit être lancé le 8 février, environ 300 des 4 000 collectivités concernées sont passées à l'acte. *« On est loin du compte,* estime Jacques Priol, fondateur d'une société de conseil aux collectivités et auteur du *Big Data des territoires* (FYP Editions, 2017). *Les petites communes n'ont pas les moyens techniques de l'open data. »*

« Chef d'orchestre du territoire »

L'autre grand chantier de la ville connectée concerne la cohabitation avec le secteur privé. Airbnb, Google, Uber… Les plates-formes de partage, en lien direct avec les usagers, bousculent le modèle classique de gouvernance urbaine, dépossédant au passage les acteurs publics de leur capacité à organiser une partie des services. Les collectivités cherchent à reprendre la main.

A Rennes, la métropole vient de lancer un *« service public métropolitain de la donnée »* pour *« une gouvernance commune de l'information, qu'elle soit publique ou privée »*, indique Bernadette Kessler, responsable de l'innovation numérique de Rennes Métropole. Pionnière de l'open data, la collectivité veut aller plus loin. Elle étudie avec des partenaires privés les conditions juridiques d'un partage*« pour améliorer les services existants et en créer de nouveaux ». « Tout le monde, ou presque, utilise Uber, Google Map ou Waze, pour ne citer que les plus connus. Est-ce que ce seul critère suffit pour définir les services publics de demain ? »,*s'interroge Marion Glatron, directrice déléguée à l'innovation et à la smart city.

A Lille, la métropole se positionne, elle, en régulateur des services numériques.*« Nous voulons mettre en place une supervision, être le chef d'orchestre du territoire au nom de l'intérêt général,* affirme Akim Oural, conseiller métropolitain aux nouvelles technologies. *On ne veut plus subir, comme on l'a fait avec Airbnb ou Uber. »*

« Quatre minutes avant les services d'urgence »

Depuis juillet, la Métropole européenne lilloise (MEL) dispose d'informations sur le trafic en temps réel, issues des milliers d'utilisateurs de l'appli Waze, qui l'alerte sur les accidents et les bouchons. *« En échange, la collectivité nous apporte des informations prévisibles qui peuvent avoir un impact sur l'état de la route – événements sportifs, brocantes, travaux »*, détaille Jérôme Marty, directeur général France de Waze, qui travaille aussi avec l'agglomération Versailles Grand Parc et le département du Loiret. *« On a calculé qu'en moyenne, Waze alerte quatre minutes avant que les services d'urgence ne soient au courant, avec une mise à jour toutes les cinq minutes. Ces informations sont précieuses pour un service public »*, assure Etienne Pichot-Damon, chargé de l'open data à la MEL.

De son côté, la métropole de Montpellier a choisi de miser sur ses propres ressources afin de limiter la dépendance aux plates-formes privées

L'expérience est suivie avec attention par de nombreux services urbains, même si tous ne sont pas enclins à pactiser avec les producteurs de données. Le Grand Lyon a décliné les avances de Waze au motif que *« les conditions d'un partenariat ne sont pas réunies*, explique Karine Dognin-Sauze, vice-présidente de la métropole de Lyon. *Nous ne pouvons pas accepter un accord avec une société qui incite ses usagers à emprunter à 8 h 30 des rues tranquilles bordées par une école. »*

De son côté, la métropole de Montpellier a choisi de miser sur ses propres ressources afin de limiter la dépendance aux plates-formes privées. *« Nous voulons rester autonomes en utilisant nos propres capteurs,* expose Jérémie Valentin, responsable de l'open data à la métropole. *Qui nous dit que l'offre de Waze sera durable ? »*

Données au compte-gouttes

Du côté des plates-formes, les opérations de séduction se multiplient. Ces derniers mois, des acteurs majeurs ont ouvert des informations destinées aux pouvoirs publics. Uber affiche sur sa plate-forme Uber Movement, depuis le 20 octobre 2017, les temps de trajet calculés à partir des parcours de ses conducteurs. Le service de VTC veut *« aider les villes à prendre des décisions »*, selon Alexandre Droulers, le directeur des projets pour l'Europe de l'Ouest. Ce qui ne l'empêche pas de livrer ses données au compte-gouttes…

« Les stratégies des plates-formes ne doivent rien au hasard. Elles se mettent en ordre de bataille en vue des discussions à venir, notamment sur la régulation » Simon Chignard conseiller à Etalab

Uber a travaillé en collaboration avec l'Institut d'aménagement et d'urbanisme (IAU) de la région Ile-de-France, dont le directeur du département mobilité, Dany Nguyen Luong, reconnaît que l'offre*« apporte des informations inédites. Nous pouvons par exemple comparer les temps de parcours à différentes heures de la journée ».* Pour autant, ces informations restent trop limitées, selon lui : *« On aurait besoin du volume du trafic : nombre de passagers, de VTC en circulation… Ces données restent confidentielles, alors qu'elles relèvent autant de l'intérêt général que celles des opérateurs traditionnels de délégations de service public. »*

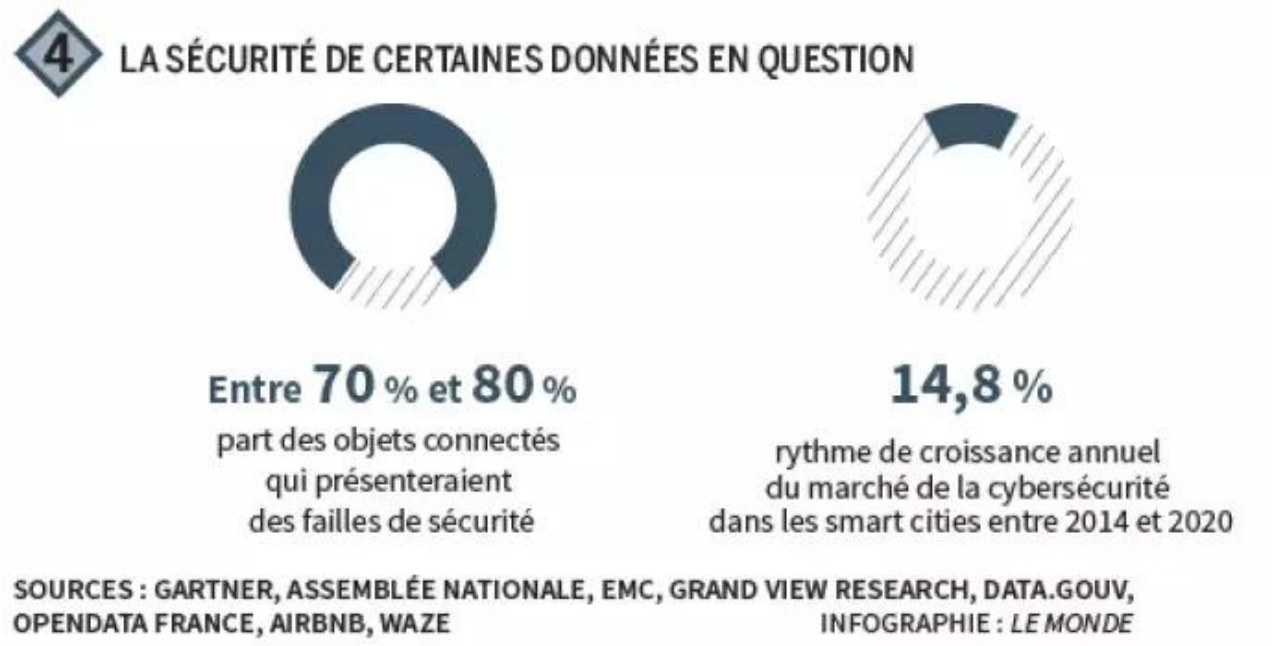
Même déception après l'ouverture, le 21 novembre 2017, du portail DataVille d'Airbnb, la plate-forme de données du site de location de logements de particuliers. Les revenus médians des utilisateurs affichés par ville ne permettent pas de comprendre, à l'échelle d'un quartier, l'impact des réservations sur l'offre de logement. *« C'est tout sauf de l'open data ; on ne peut pas réaliser nos propres analyses »*, estime Jérémie Valentin, à Montpellier, tandis qu'à Bordeaux, le conseiller municipal Matthieu Rouveyre a entrepris de géolocaliser tous les logements loués sur Airbnb, au nom du *« droit à la ville ».*

Pour Simon Chignard, conseiller à Etalab, la mission du gouvernement relative au partage de données publiques, *« les stratégies des plates-formes ne doivent rien au hasard. Elles se mettent en ordre de bataille en vue des discussions à venir, notamment sur la régulation ».*

Enjeux éthiques

Entre les collectivités, auxquelles la loi impose l'open data, et les acteurs privés, pour qui la donnée représente un trésor économique, l'échange reste donc largement inéquitable. Certains veulent aller plus loin, en créant un statut de « données d'intérêt territorial », comme le préconise l'ex-député Luc Belot dans son rapport sur la smart city remis en avril 2017.

De son côté, la Commission nationale de l'informatique et des libertés (CNIL) analyse les conditions d'un *« open data du secteur privé »* dans un cahier publié par son laboratoire d'innovation en novembre 2017. Quant à la ministre des transports, Elisabeth Borne, elle a évoqué, le 13 décembre 2017, à l'issue des Assises de la mobilité, la *« mise à disposition des données »* de l'ensemble des opérateurs, *« non seulement publics mais aussi privés, à l'instar de l'autopartage, des VTC ou encore des vélos en libre-service ».*



L'année 2018 sera-t-elle celle de la régulation de la data urbaine ? Un premier pas s'apprête à être franchi le 25 mai en France, avec l'entrée en vigueur du nouveau règlement européen général pour la protection des données (RGPD), qui prévoit des devoirs plus stricts, assortis de sanctions, pour les acteurs qui collectent de la donnée personnelle, et des droits plus importants pour les citoyens.

Conditions d'utilisation illisibles, défauts de consentement, manque de transparence… Le citoyen reste le grand oublié de la smart city, souvent considéré comme un smartphone ambulant et insuffisamment consulté. Or la masse croissante des informations collectées et la porosité entre les différents usages renouvellent les possibilités de surveillance. *« Un panneau indique à l'entrée des villes la présence de caméras de surveillance mais rien ne permet aujourd'hui de savoir que vos données y sont captées »*, regrette Jacques Priol.

Temps démocratique

Le vaste chantier des villes intelligentes est d'abord un projet politique. En témoigne l'annonce, à Marseille, de la création d'un nouveau centre de supervision consacré à la tranquillité publique, avec comme objectif de croiser les données de la ville avec celles achetées à des acteurs privés, comme les opérateurs de téléphonie mobile.

« La vraie question n'est plus comment on construit la ville connectée, mais pour en faire quoi », estime le sociologue Bruno Marzloff, du cabinet Chronos. *« Il ne faudrait pas que la vitesse des algorithmes remplace le temps démocratique, où la participation du citoyen est indispensable »*, renchérit Jacques Priol.

Encore timides, des initiatives commencent à voir le jour pour associer plus étroitement les habitants à l'utilisation de leurs données. A Lyon, la métropole teste depuis 2017 le dispositif « Mes infos », initié par la FING (Fondation Internet nouvelle génération) pour redonner aux citoyens le contrôle de leurs données personnelles. Le projet associe à la fois des particuliers, une collectivité locale et des entreprises, dont la compagnie d'assurances MAIF et l'opérateur de télécoms Orange.

Ces partenaires imaginent de nouveaux services selon des règles définies préalablement ensemble. Un dispositif qui s'inscrit dans la volonté de*« construire un environnement de confiance, et qui passe par l'éducation à la donnée »*, résume Karine Dognin-Sauze. Chaque individu a accès aux informations collectées à son sujet et peut décider pour quels services il est prêt à en autoriser l'usage. Une façon de replacer le citoyen au centre du débat.

Claire Legros

Smartphones Pixel 4 à reconnaissance faciale, enceintes visiophones… Google dévoile de nouveaux appareils

Les nouveaux smartphones Pixel 4 pourront être déverrouillés par un système de reconnaissance faciale comparable à celui d'Apple et pilotés en esquissant des gestes de la main.

Par Nicolas Six Publié le 15 octobre 2019 à 17h23 - Mis à jour le 16 octobre 2019 à 05h58

Présentation du Google Pixel 4 à New York le 15 octobre. DREW ANGERER / AFP

Nouveaux smartphones et nouvelles enceintes, dotés de fonctionnalités inédites : Google a dévoilé ses prochains appareils, mardi 15 octobre, lors d'une conférence à New York.

Pas de technologie révolutionnaire en vue, mais certaines améliorations pourraient tout de même faciliter le quotidien des utilisateurs. L'entreprise de Mountain View (Californie) en a également profité pour révéler la date précise de commercialisation de Stadia, son service de jeu vidéo en ligne, qui sera disponible le 19 novembre.

Des Pixels 4 dotés de reconnaissance faciale

Deux nouveaux smartphones haut de gamme ont été dévoilés, les Pixel 4 et Pixel 4 XL, qui sortiront le 24 octobre. Le premier dispose d'une qualité devenue rare : un gabarit compact. Son prix est aussi plus accessible que le modèle XL : environ 770 euros, contre 900 euros pour son grand frère.

Les deux appareils sont équipés d'un intrigant arsenal de capteurs logés dans un bandeau noir, au-dessus de leur écran. On y trouve un système de reconnaissance du visage, conçu pour déverrouiller le téléphone, qui fonctionne de façon assez similaire à celui de l'iPhone. Selon Google, il permettra de réveiller les Pixel 4 de façon simple, rapide et sûre, même dans le noir complet, ce dont les smartphones Android sont presque tous incapables, à commencer par les modèles du groupe sud-coréen Samsung.

Radar de mouvement

Plus étonnant : les Pixel sont équipés d'un radar de mouvement qui permet de commander leurs applications sans les toucher, pour décrocher, raccrocher, baisser le volume, zapper les titres des chansons… et faire coucou au personnage de jeu vidéo Pikachu qui trône sur l'écran d'accueil des Pixel, animé en 3D.

Des smartphones d'autres marques sont déjà capables de reconnaître les commandes gestuelles, mais ils s'appuient généralement sur une caméra. Selon Google, ce radar présente deux avantages : il fonctionne dans toutes les conditions de lumière et repère les mouvements sur un plan plus large.

Nous avons pu tester cette fonction pendant quelques minutes. Elle est relativement efficace à condition de passer la main à quelques centimètres du téléphone. Quand le Pixel détecte un mouvement, il en affiche une représentation graphique en haut de l'écran qui donne chair à la technologie : c'est un retour visuel commode.

Amusante, mais limitée à quelques commandes pour le moment, cette fonction nous a paru un peu gadget. Toutefois, certains utilisateurs pourraient y trouver une réelle utilité dans leur voiture ou leur cuisine.

Deux capteurs photo… seulement

Côté photo, Google fait actuellement partie des marques de smartphone les plus recommandables, et les Pixel 4 devraient prendre de fort beaux clichés. La prise de photos très contrastées progresse : le filtre HDR, qui permet de capturer des parties d'images très lumineuses sans négliger les parties sombres, fonctionnera désormais en direct ; on verra donc immédiatement son effet. Il sera aussi possible d'ajuster manuellement le niveau des ombres et des lumières vives en temps réel.

Ils intègrent désormais un second capteur photo, un zoom x 2 utile pour voir plus loin, mais font l'impasse sur le troisième capteur qui équipe bon nombre de concurrents, l'« ultra grand angle » qui permet notamment de capturer des photos de paysage spectaculaires.

Le Pixel 4 XL et le Pixel 4. NICOLAS SIX

Les Samsung S10 et Note 10 – de redoutables concurrents aux tarifs proches – en sont équipés, comme beaucoup d'autres mobiles à ce niveau de prix. Les Samsung sont aussi dotés d'un écran aux bords incurvés qui les rendent plus confortables à manipuler.

Une enceinte visiophone

Du côté des enceintes connectées, autre produit hautement stratégique pour Google, la nouvelle Nest Hub Max, commercialisée le 4 novembre pour 230 euros, intrigue.

Cette enceinte connectée est non seulement dotée d'un grand écran dix pouces qui permet de visualiser beaucoup d'informations d'un coup (la météo de la semaine par exemple), sans attendre que l'enceinte égrène ces infos à voix haute. Mais surtout, elle embarque une caméra pour passer des appels vidéo. Celle-ci voit très large, peut repérer les interlocuteurs présents dans la pièce pour zoomer sur eux, et même suivre leurs déplacements – un peu comme le vidéophone concurrent de Facebook, le Portal.

Que fait-elle quand plusieurs personnes sont présentes à l'écran ? Selon un porte-parole de Google, elle tente de tous les loger dans l'image, y compris les personnes silencieuses. Cette fonction ambitionne de rendre les conversations de famille moins contraignantes qu'avec un smartphone, un ordinateur ou une tablette classique, qui forcent à rester attentif au cadrage et ont tendance à filmer le menton.

L'enceinte Nest Hub Max est dotée d'un écran. NICOLAS SIX

Quid de la protection de la vie privée ? Selon Google, un bouton situé juste derrière le capteur permet de couper physiquement la caméra et les micros, ce qui devrait empêcher l'appareil de filmer le domicile jour et nuit. Même si, au besoin, on pourra utiliser l'appareil comme caméra de surveillance.

Google explique que cette caméra sert aussi à reconnaître les utilisateurs qui ont enregistré leur visage. Cela permet à son écran d'afficher des informations personnalisées, comme les rendez-vous de la journée par exemple.

Mais si plusieurs personnes sont présentes dans la même pièce, la Hub Max affichera les rendez-vous de la personne qu'il reconnaît, et tant pis s'ils sont dérangeants… *« Il s'agit là d'une fonction de personnalisation, pas de vie privée »*, reconnaît un porte-parole de Google. Qui ajoute qu'on peut échapper à ce problème en passant ces rendez-vous en privé – une manœuvre assez pénible.

Nicolas Six

Reconnaissance faciale : une start-up analyse les photos des réseaux sociaux pour la police américaine

Le « New York Times » a publié une enquête sur cette entreprise financée par Peter Thiel (Palantir, Facebook) qui fournit son logiciel à la police américaine.

Publié le 20 janvier 2020 à 12h41 - Mis à jour le 20 janvier 2020 à 15h05

Pouvoir comparer en quelques instants une photographie avec une base de données de plus de trois milliards de photographies publiées par tout un chacun sur les réseaux sociaux : la promesse a séduit six cents services de police aux Etats-Unis. Cet outil est proposé par Clearview, discrète start-up américaine à laquelle le *New York Times* a consacré une longue enquête, parue le 18 janvier.

Fondée par Hoan Ton-That, 31 ans, l'entreprise a, pour faire fonctionner son logiciel, discrètement copié des milliards d'images publiées sur les plates-formes sociales les plus courantes du monde occidental : profils Facebook ou LinkedIn, photos Instagram ou Twitter… Elle a ainsi pu constituer une gigantesque base de données, dans laquelle un moteur de recherche par reconnaissance faciale permet ensuite d'identifier des suspects ou des témoins. Des visages

qui auraient été par exemple enregistrés par des caméras de surveillance pourraient conduire à l'identification d'une personne grâce aux informations présentes dans cette base de données.

« Les utilisateurs de Clearview peuvent potentiellement identifier de la sorte toutes les personnes qu'elles ont vues. L'outil pourrait être utilisé pour identifier des militants dans des manifestations, ou un bel inconnu dans le métro, ne révélant pas seulement leur nom mais aussi leur lieu de vie, ce qu'ils ont fait précédemment, et quelles sont leurs fréquentations », écrit le *New York Times.*

L'outil est populaire auprès des forces de police locales, qui, aux Etats-Unis, disposent de leurs propres budgets et sont libres d'utiliser les logiciels et équipements de leur choix. Clearview a par ailleurs aussi fourni ses solutions à des entreprises privées de sécurité, rapporte le *New York Times.* Pour certains enquêteurs, Clearview complète utilement les bases de données locales ou fédérales contenant les photos de personnes condamnées ou les portraits des permis de conduire. *« Avec Clearview, on peut utiliser des photos qui ne sont pas parfaites ; la personne peut porter un masque ou des lunettes, et cela fonctionne même avec les images partielles d'un visage »*, témoigne ainsi un policier dans le quotidien new-yorkais.

Amazon : les actionnaires soutiennent la vente d'un logiciel de reconnaissance faciale à la police

Publié le 23 mai 2019 à 10h05 - Mis à jour le 23 mai 2019 à 10h15

L'assemblée générale d'Amazon a décliné, mercredi 22 mai, deux résolutions au cœur de tensions au sein de l'entreprise. La première, portée par certains actionnaires et soutenue par des organisations non gouvernementales, visait à interdire au grand groupe du numérique de fournir sa technologie de reconnaissance faciale, Rekognition, aux forces de l'ordre. En vain. L'an dernier, une trentaine d'associations américaines de défense des libertés avaient dénoncé, dans une lettre ouverte, un logiciel *« puissant »* et *« dangereux »*, qui *« se prête à tous les abus »*.

La seconde résolution portait, quant à elle, sur l'impact environnemental d'Amazon, exigeant que l'entreprise soit plus active dans la lutte contre le changement climatique. 7 642 salariés d'Amazon avaient signé une lettre ouverte en ce sens publié le 10 avril. Là encore, les actionnaires ont voté contre.

Danger majeur pour les libertés individuelles

Cette efficacité affichée inquiète fortement les défenseurs des libertés individuelles ; l'entreprise affirme que son système trouve une correspondance dans 75 % des cas, mais ne donne pas le taux de « faux positifs » – le nombre de personnes identifiées par erreur. Or, plus la base de données est importante, plus les chances d'y trouver plusieurs personnes dotées d'une forte ressemblance augmentent, a fortiori lorsque l'image utilisée pour la recherche est de mauvaise qualité. Plusieurs études ont également montré que les logiciels de reconnaissance faciale, s'ils sont en progrès constant, sont loin d'être précis à 100 %.

L'histoire de Clearview suscite également des inquiétudes en raison de sa coloration très politique. Elle a ainsi été financée initialement par le multimilliardaire Peter Thiel, fondateur de Palantir, membre du conseil d'administration de Facebook et réputé proche de Donald Trump.

La société a aussi fait appel à plusieurs républicains ultraconservateurs pour assurer sa promotion auprès des services de police du pays. Entreprise privée, Clearview n'est par ailleurs pas soumise aux mêmes types de contrôles pointilleux que les bases de données classiques des forces de l'ordre – les photos ne sont par exemple jamais effacées de ses archives.

Mais au-delà du cas spécifique de Clearview, la crainte est grande de voir ce type de services se multiplier. Clearview a établi son prototype original avec deux ingénieurs seulement, et un budget très réduit. *« Sans une loi fédérale très stricte sur la vie privée* [qui interdirait ces collectes massives d'images]*, nous sommes foutus »*, a résumé au *New York Times* Al Gidari, professeur de droit de la vie privée à l'université Stanford.

Facebook met à jour sa fonction de reconnaissance faciale

Le géant des réseaux sociaux subit une pression des institutions pour mieux protéger la vie privée et les données, y compris biométriques, de ses utilisateurs.

Le Monde avec AFP Publié le 04 septembre 2019 à 01h20 - Mis à jour le 04 septembre 2019 à 09h25

Facebook devra clarifier son utilisation de la technologie de reconnaissance faciale. Jenny Kane / AP

Les utilisateurs de Facebook devront désormais choisir d'activer la reconnaissance faciale s'ils veulent s'en servir pour être identifiés sur les photos postées sur le réseau social, a annoncé la plate-forme mardi 3 septembre. Dans le cas contraire, la fonctionnalité restera désactivée par défaut.

Ce changement intervient alors que le groupe subit une pression des institutions pour mieux protéger la vie privée de ses usagers.

La technologie de reconnaissance faciale identifie automatiquement les personnes présentes sur les photos mises en ligne sur Facebook, si ce sont des contacts des utilisateurs. Ceux-ci peuvent alors choisir de légender la photo avec leur nom. Depuis près de deux ans, cette fonctionnalité va plus loin, en signalant aux usagers quand ils apparaissent sur des images postées sur le réseau par leurs contacts.

Désormais, les personnes qui utilisaient cette option ou qui rejoignent le réseau à partir de mardi se verront proposer l'activation, ou non, de cette technologie. En dehors de ce bouton on/off, les principes qui la régissaient auparavant restent inchangés.

Amende record de 5 milliards de dollars

La fonctionnalité *« ne vous identifie toujours pas [auprès de personnes qui ne font pas partie de vos contacts] »*, rappelle Srinivas Narayanan, chercheur de la division d'intelligence artificielle de Facebook, dans un communiqué en ligne. *« Nous ne partageons pas vos informations liées à la reconnaissance faciale avec des tiers. Et nous ne vendons pas notre technologie. »*

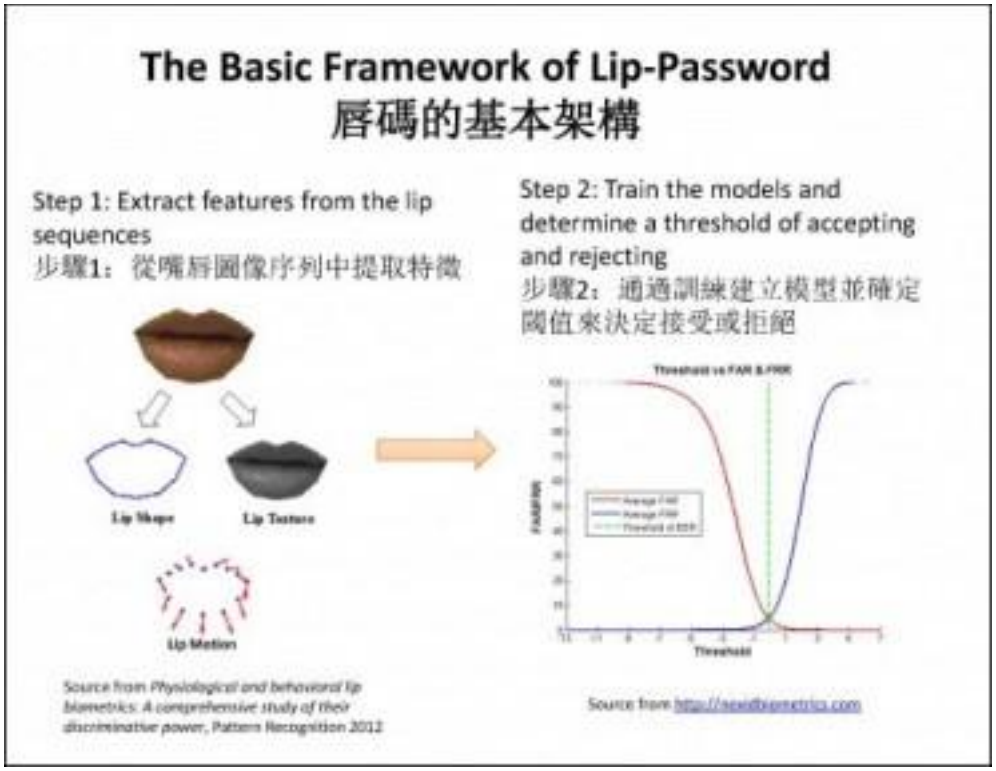
A la fin juillet, l'agence américaine de protection des consommateurs a infligé au groupe une amende record de 5 milliards de dollars pour avoir *« trompé »* ses usagers sur leur capacité à contrôler leurs informations personnelles.

Elle a aussi passé un accord avec le réseau social pour modifier sa façon de traiter les données, lui imposant notamment de fournir des éléments clairs sur son utilisation de la technologie de reconnaissance faciale et d'obtenir le consentement explicite des utilisateurs pour tout usage non défini au préalable.

Les données des usagers constituent un moteur essentiel du modèle économique de Facebook, fondé sur la personnalisation à très grande échelle des publicités.

Des images pour entendre, en l'absence de tout son, à distance dans l'espace ou le temps (cas des films muets) des paroles inaudibles

Une université asiatique a élaboré une technique reconnaissance de mots de passe via le mouvement des lèvres. Une nouvelle voie crédible pour l'authentification des utilisateurs ?
Le département informatique de l'université baptiste de Hong Kong a mis au point une technique pour déchiffrer les mots de passe avec le simple mouvement des lèvres. Cette solution se nomme LMP pour Lip Motion Password. La solution se veut agnostique par rapport à la langue utilisée.
Concrètement, la reconnaissance se base sur des caméras intégrées dans les smartphones ou les tablettes reconnaissant les différents types de lèvres et la façon dont elles bougent quand le mot de passe est prononcé. Le professeur Cheung Yiu-Ming explique : « *le même mot de passe énoncé par deux personnes est différent et un système d'apprentissage peut les distinguer* ».
Utilisant le Machine Learning, LMP est capable de prendre en compte plusieurs éléments : la texture des lèvres (y compris quand elles sont gercées), les mouvements des lèvres, et le son (capacité à reconnaître un accent ou une spécificité de langage). D'après la recherche, les bruits de fonds ne sont pas un handicap, car le service se focalise sur les mouvements des lèvres. Par ailleurs, la technique utilisée résiste bien à l'imitation d'une voix.



Les avantages à la reconnaissance labiale

LMP comporte plusieurs avantages selon les universitaires. En premier lieu, la technique n'oblige plus les utilisateurs à imaginer un mot de passe avec des majuscules, des minuscules ou des caractères spéciaux. Elle résout en partie le problème de la réutilisation des mots de passe en y ajoutant un élément de biométrie. Autre intérêt, elle est capable de stocker les

mots de passe sous forme d'ondes sonores avec une signature propre. On évite ainsi les risques de duplication qui existent avec les empreintes digitales par exemple.
Pour les scientifiques de l'université de Hong Kong, la LMP devrait servir à l'avenir pour assurer la sécurité des transactions financières. La reconnaissance labiale s'inscrit en tout cas dans un écosystème de solutions biométriques en pleine croissance. On recense déjà, par exemple, des services s'appuyant sur le **rythme cardiaque** ou **la tension veineuse**.
(article réalisé en collaboration avec Esteban Martin-Fréour)

Entendre ce que disent des personnes dans une voiture ou derrière une fenêtre. Faire piloter une voiture à la voix.

SenseTime, la start-up chinoise en pointe dans la reconnaissance faciale

La jeune pousse, qui a levé plus de 1 milliard de dollars en deux mois, s'impose comme une championne de l'intelligence artificielle.

Par Simon Leplâtre Publié le 04 juin 2018 à 11h20 - Mis à jour le 04 juin 2018 à 11h20

SenseTime fournit la technologie de reconnaissance faciale des principaux constructeurs chinois de smartphones – Huawei, Oppo, Xiaomi et Vivo. LLUIS GENE / AFP

Vous n'avez sans doute pas encore entendu parler de SenseTime, mais l'entreprise chinoise, elle, vous connaît peut-être déjà. Du moins, de vue. Si vous avez voyagé en Chine, ou si vous utilisez un smartphone chinois, de la marque Huawei par exemple, il est probable que votre visage soit enregistré dans la base de données du leader chinois de la reconnaissance faciale.

SenseTime travaille aussi bien avec des firmes privées de haute technologie qu'avec les services de police pour surveiller la population. Fondée en 2014 par un ancien du Massachusetts Institute of Technology (MIT), elle n'en finit pas de croître. Preuve en est, elle a annoncé, jeudi 31 mai, la levée de 620 millions de dollars (environ 531 millions d'euros), après presque autant mi-avril (600 millions de dollars). Grâce à ce nouvel apport, elle conforte sa place de start-up de l'intelligence artificielle (IA) la plus cotée du monde, avec une valorisation de 4,5 milliards de dollars.

La société prévoit de se renforcer dans son secteur d'origine, la reconnaissance faciale, et de se diversifier parallèlement dans d'autres activités. Ainsi, elle a signé un partenariat avec Honda pour développer des capacités d'identification d'objets pour des voitures autonomes. La start-up propose aussi ses services à des entreprises de robots industriels, qui doivent eux aussi « lire » leur environnement pour se déplacer de manière autonome dans des usines. L'entreprise collabore également avec les forces de police d'une quarantaine de localités chinoises afin d'identifier des personnes recherchées, y compris au Xinjiang (nord-ouest), région autonome instable, où un contrôle très strict de la population a été mis en place.

Le dernier tour de table de SenseTime a rassemblé des fonds d'investissements chinois et étrangers, tels que Fidelity International, Hopu Capital, Silver Lake et Tiger Global Management. Ils rejoignent des grands noms de la technologie qui soutenaient déjà la firme, comme Alibaba, qui a mené la dernière levée de fonds de l'entreprise en avril, Qualcomm, le leader américain des puces électroniques, ou encore le fonds souverain de Singapour, Temasek.

Débloquage des smartphones

Le logo de SenseTime est rarement visible, même en Chine, où l'entreprise est pourtant la plus active. Sa technologie se trouve cependant derrière nombre de logiciels et d'applications populaires. Suning, un vendeur de produits électroménagers chinois à succès, a lancé l'année dernière des magasins autonomes, sans vendeurs. Le paiement par reconnaissance faciale y est possible grâce à SenseTime. Le spécialiste de l'IA aide aussi l'opérateur du métro de Shanghaï à analyser les flux de passagers.

Mais le chiffre d'affaires de SenseTime provient essentiellement d'applications moins impressionnantes. L'entreprise fournit la technologie de reconnaissance faciale des principaux constructeurs chinois de smartphones – Huawei, Oppo, Xiaomi et Vivo. Celle-ci permet à la fois de débloquer les smartphones, de ranger les photos en fonction des personnes présentes sur les clichés, ou de prendre des selfies plus avantageux grâce aux fonctions « embellissement », très prisées des utilisateurs chinois.

SenseTime est certes un poids lourd de l'intelligence artificielle en Chine, mais elle est loin d'être la seule. Alibaba, Tencent et Baidu, qui dominent le Web chinois, investissent lourdement pour se conformer aux directives de Pékin. En juillet 2017, la Chine a publié sa feuille de route, avec l'objectif de dominer le secteur d'ici à 2030. A chacun son rôle : smart city (« ville intelligente ») pour Alibaba, véhicules autonomes pour Baidu… L'Etat encourage la création de fonds d'investissements spécialisés. Les autorités espèrent que cette industrie générera 150 milliards de dollars de chiffre d'affaires dans le pays.

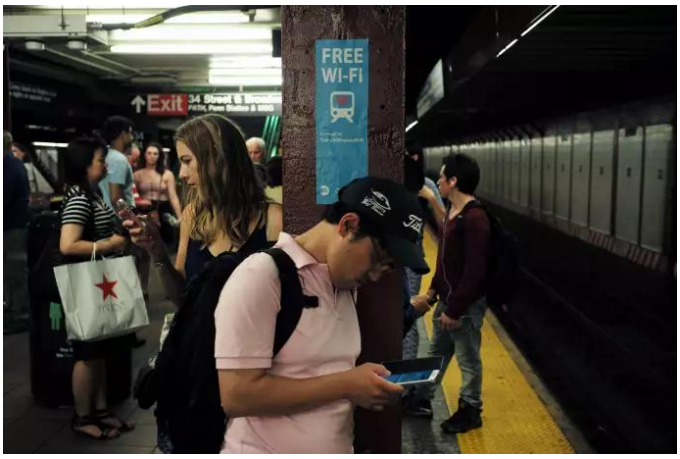
Simon Leplâtre (Shanghaï, correspondance)

Des menaces contre la démocratie sous prétexte de sécurité

Les libertés individuelles, oubliées de la smart city

La ville connectée est-elle compatible avec le respect de la vie privée ? La CNIL souligne les dérives liées à la collecte massive des données et propose de nouvelles formes de gouvernance.

Par Claire Legros Publié le 13 octobre 2017 à 18h31 - Mis à jour le 13 octobre 2017 à 18h31



Si le concept de smart city fait l'objet de multiples publications, son impact sur la vie privée reste peu exploré : la protection des données personnelles demeure « le parent pauvre de ces travaux ». JEWEL SAMAD / AFP

C'est un chantier titanesque qui se construit chaque jour à l'aide de capteurs discrets, disséminés dans les quartiers, les immeubles, et jusqu'au fond de nos poches. Avec la promesse réjouissante d'une cité fluide, optimisée, assainie, sécurisée. Mais la ville connectée est-elle compatible avec la protection des droits et libertés des individus ? Qu'en est-il de l'intérêt général lorsque la donnée se concentre, un peu plus chaque jour, entre les mains de quelques grands acteurs privés ?

Soucieuse d'apporter sa pierre à l'édifice de la smart city, la Commission nationale de l'informatique et des libertés (CNIL) a publié, mardi 10 octobre, une riche synthèse des travaux de son laboratoire d'innovation numérique, intitulée « La plate-forme d'une ville, les données personnelles au cœur de la fabrique de la smart city ». La gardienne des données personnelles y explore les enjeux politiques et sociaux de la cité numérique et souligne les dérives à l'œuvre dans des villes dévoreuses de données.

L'individu, « smartphone ambulant »

Avec un premier constat : si le concept de smart city fait l'objet de multiples publications, son impact sur la vie privée reste peu exploré : la protection des données personnelles demeure *« le parent pauvre de ces travaux ». « L'individu reste un problème à régler, ou au mieux* (…) *un smartphone ambulant dont les données seraient essentielles à la bonne conduite de la ville »,* notent les auteurs.

Google, Facebook, mais aussi Uber et AirBnb… Les industriels de la donnée ont établi de nouveaux rapports de force, sans égard pour les principes d'information et de consentement, pourtant inscrits dans la loi mais *« particulièrement affaiblis dans les technologies de la smart city ».* Cette masse grandissante de données renouvelle les possibilités de

surveillance dans l'espace urbain, comme l'ont montré les travaux de la chercheuse Liesbeth van Zoonen sur la porosité entre les différents usages.

Or, collectivités et entreprises n'ont plus que quelques mois pour se mettre en conformité avec le nouveau règlement européen général pour la protection des données (RGPD), qui prévoit des sanctions plus importantes et de nouveaux droits pour les citoyens.

L'instance le rappelle et préconise la création de « comités consultatifs sur la vie privée » dans les collectivités. Elle souhaite aussi encourager le développement de technologies protectrices de la vie privée, comme par exemple des dispositifs du type « Do not track » adaptés aux objets connectés en milieu urbain.

Des flux de plus en plus privatisés

En remodelant la ville, l'économie des plates-formes rebat aussi les cartes du pouvoir. De nouveaux équilibres se mettent en place où les géants numériques contournent les acteurs publics, dépossédés de leur capacité à organiser le marché des services urbains, au risque de perdre de vue l'intérêt général au profit des intérêts particuliers.

C'est dans le domaine des mobilités que se posent les questions les plus aiguës. Des applications qui, comme Waze, fluidifient le trafic, peuvent aller à l'encontre des politiques publiques. Les urbanistes qui *« cherchent à redessiner le réseau routier afin de supprimer les raccourcis »* doivent désormais lutter contre des algorithmes *« qui font de la satisfaction de leur utilisateur un optimum absolu »*. Quitte à conseiller des rues tranquilles bordées par une école ou une crèche. A l'inverse, des quartiers défavorisés, signalés « à risque » par les applications, voient leur trafic diminuer alors qu'*« injecter du flux dans ces zones pourrait les déghettoïser ».*

Comment redonner la main aux autorités garantes de l'intérêt général ? Pour y répondre, les auteurs de l'étude ont adopté une démarche originale. Pendant trois mois, de novembre 2016 à janvier 2017, ils ont mené des ateliers de « design fiction » pour explorer des problématiques imaginaires à l'horizon 2026, ces scénarios servant à documenter des propositions.

Portabilité citoyenne de la donnée

Les pistes proposées sont ambitieuses. Elles portent sur l'ouverture des données, y compris celles d'acteurs privés peu disposés en général à partager le trésor sur lequel ils sont assis. La CNIL imagine des mécanismes qui, chacun à leur niveau, contribueraient à rééquilibrer les pouvoirs entre acteurs publics et privés : élargir par exemple le périmètre des « données d'intérêt général » consacrées par la loi « République numérique », ou encore généraliser un « open data du secteur privé ». Une façon de changer les règles du jeu au nom de l'intérêt général.

Les auteurs accordent une place toute particulière à une forme de gouvernance innovante, celle des communs urbains, inspirés par les travaux de l'économiste Elinor Ostrom et développés depuis plusieurs années par Valérie Peugeot, elle-même membre de la CNIL. Des données produites par des acteurs publics ou privés seraient gérées comme une ressource communautaire selon un mode de gouvernance partagée déjà à l'œuvre dans le domaine du logiciel libre ou des licences Créative Commons.

L'idée pourrait s'appuyer sur l'un des dispositifs majeurs du nouveau RGPD, le*« droit à la portabilité »*, mis en place au printemps 2018. Il permettra aux personnes qui le souhaitent de récupérer leurs données personnelles dans un format ouvert et lisible par une machine. Pourquoi ne pas en confier une partie, dans un cadre précis, à un acteur public afin de participer à des missions d'intérêt général ?

Reste à savoir comment les pouvoirs publics s'empareront de ces travaux. *« Le numérique exige plus que des solutions ponctuelles*, note Isabelle Falque-Pierrotin, présidente de la CNIL, dans son introduction au dossier. *C'est bien un nouveau design de la ville qu'il nous impose d'imaginer. »*

Royaume-Uni : bilan catastrophique pour une expérience de vidéosurveillance « intelligente »

Toutes les personnes identifiées comme recherchées par le logiciel l'ont été par erreur.

Publié le 01 septembre 2017 à 16h29 - Mis à jour le 01 septembre 2017 à 16h40

Au carnaval de Notting Hill à Londres, le 28 août. Cette gigantesque fête est l'une des plus grandes d'Europe. Tim Ireland / AP

Trente-cinq cas de « faux positif », et une arrestation d'un innocent : c'est le bilan catastrophique d'une expérience de « vidéosurveillance intelligente », menée à la fin d'août durant le carnaval de Notting Hill à Londres, selon une enquête de la télévision nationale Sky News.

Le carnaval de Notting Hill, le plus grand événement populaire de la capitale britannique, attire chaque année environ un million de personnes sur deux jours. Cette année, il était encadré par un dispositif de sécurité exceptionnel, après les attentats de Londres et de Manchester. La police londonienne utilisait notamment un système de caméras capable de reconnaître des visages en les comparant à une base de données, qui devait permettre d'identifier les personnes recherchées par la police.

Les limites de ces systèmes automatisés sont connues depuis longtemps : malgré les progrès de la technologie, ils donnent toujours une grande proportion de « faux positifs » – des personnes identifiées comme suspectes par le logiciel, qui sont en réalité innocentes. C'est précisément ce qui s'est passé durant le carnaval : dans 35 cas, le programme a cru reconnaître une personne recherchée, mais il s'est trompé.

La base de données utilisée par le logiciel était également mal mise à jour : une personne, correctement identifiée par le programme, a été interpellée, avant d'être remise en liberté. Elle avait, en effet, déjà été mise hors de cause dans l'affaire pour laquelle elle était recherchée, mais son visage était resté dans la base de données. Aucune arrestation de personne réellement recherchée n'a été rendue possible par les caméras.

Plusieurs associations britanniques dénoncent l'utilisation de ces systèmes de vidéosurveillance, déjà expérimentés l'an dernier lors du carnaval. Elles estiment que les bases de données biométriques utilisées par ces caméras sont illégales, et que leur utilisation est une violation des droits fondamentaux.

« La reconnaissance faciale s'avère inefficace pour enrayer la violence »

L'authentification biométrique, testée par des entreprises, aura pour conséquence d'instaurer un « contrôle permanent et généralisé » au nom du « solutionnisme technologique », déplorent le juriste Martin Drago et le chercheur Félix Tréguer, dans une tribune au « Monde ».

Par Félix Tréguer et Martin Drago Publié le 24 octobre 2019 à 06h15

Article réservé aux abonnés

Tribune. L'inévitable débat sur la reconnaissance faciale arrive enfin en France, et le gouvernement esquisse sa réponse. Dans un entretien paru dans Le Monde du 15 octobre, le secrétaire d'Etat au numérique Cédric O, ancien cadre du groupe Safran, a notamment estimé qu'*« expérimenter »* la reconnaissance faciale était *« nécessaire pour que nos industriels progressent »*.

Mais cette prise de parole au plus haut niveau politique n'est que la partie émergée de l'iceberg. Car depuis des mois, notes et rapports officiels se succèdent pour souligner le défi que constitue l'*« acceptabilité sociale »* de ces technologies. Pour leurs auteurs, l'objectif est clair : désarmer les résistances à ces nouvelles modalités d'authentification et d'identification biométriques dont la prolifération est jugée inéluctable, et permettre à des industriels français comme Thales ou Idemia *[une entreprise de sécurité numérique]* de se positionner face à la concurrence chinoise, américaine ou israélienne.

L'enjeu est d'autant plus pressant que, contrairement à ce que laisse entendre Cédric O, les dispositifs de reconnaissance faciale sont déjà en place sur le territoire français. Depuis plusieurs années, des entreprises développent et testent ces technologies grâce à l'accompagnement de l'Etat et l'argent du contribuable. Le tout sans réel encadrement ni transparence.

La campagne participative de recherche-action Technopolice.fr, lancée début septembre par des associations de défense des libertés, a commencé à documenter les projets lancés au niveau national et local – à Paris, Nice, Marseille, Toulouse, Valenciennes et Metz notamment. Outre la reconnaissance faciale, d'autres applications greffées aux flux de vidéosurveillance et fondées elles aussi sur des techniques d'« intelligence artificielle » font également l'objet d'expérimentations, comme l'analyse des émotions ou la détection de « comportements suspects ».

« Rassurer » l'opinion publique

Alors, face aux oppositions portées sur le terrain et jusque devant les tribunaux par les collectifs mobilisés contre ces déploiements, les représentants de l'Etat et les industriels font front commun. Leur but n'est pas tant d'expérimenter que de tenter de « rassurer » l'opinion publique, le temps d'œuvrer à la banalisation de ces technologies et de mettre la population devant le fait accompli.

Les garanties mises en avant dans la communication gouvernementale – instance de supervision sous l'égide de la Commission nationale de l'informatique et des libertés (CNIL), pseudo-consultation et adoption future de règles juridiques qui dessineraient un modèle « acceptable » de reconnaissance faciale « à la française » – sont tout bonnement illusoires. L'histoire récente l'illustre amplement. La loi « informatique et libertés », adoptée en 1978 en réaction aux premiers scandales liés au fichage d'Etat, n'a de toute évidence pas permis, comme c'était pourtant son objectif, de juguler l'avènement d'une société de surveillance.

« Si nos grands-parents avaient vécu au début des années 1940 dans un monde saturé de tels dispositifs, ils n'auraient pas pu tisser des réseaux clandestins capables de résister au régime nazi »

Pire, dans ce domaine, la CNIL a vu ses pouvoirs systématiquement rognés depuis quinze ans, donnant le change à des présidents successifs ayant souvent contribué à cette impuissance. Quant à l'exemple des fichiers de police, il suffirait à démontrer que, même une fois inscrites dans la loi, les dispositions destinées à protéger les droits fondamentaux sont systématiquement contournées.

Or ces technologies biométriques augurent un changement de paradigme dans l'histoire de la surveillance. A terme, elles reviennent à instaurer un contrôle d'identité permanent et généralisé, exigeant de chaque personne qu'elle se promène en arborant une carte d'identité infalsifiable, qui pourra être lue sans qu'elle ne le sache par n'importe quel agent de police. L'histoire devrait nous servir de leçon : si nos grands-mères et nos grands-pères avaient dû vivre au début des années 1940 dans un monde saturé de tels dispositifs, ils n'auraient pas pu tisser des réseaux clandestins capables de résister au régime nazi.

Déshumaniser les rapports sociaux

En dépit de leurs effets politiques délétères, ces coûteuses machines seront incapables d'apporter la sécurité vantée par leurs promoteurs. Les milliards d'euros dépensés depuis plus de vingt ans au nom du « solutionnisme technologique » en vogue dans les milieux de la sécurité devraient là encore nous en convaincre : la technologie s'est avérée inopérante pour enrayer les formes de violence qui traversent nos sociétés. Sous couvert d'efficacité et de commodité, elle conduit à déshumaniser encore davantage les rapports sociaux, tout en éludant les questions politiques fondamentales qui sous-tendent des phénomènes tels que la criminalité.

C'est pourquoi, contre cette offensive concertée de l'Etat et des industriels qui, à tout prix, cherchent à imposer la reconnaissance faciale, nous devons dire notre refus. Aux Etats-Unis, après les mobilisations citoyennes, plusieurs municipalités, ainsi que l'Etat de Californie, ont commencé à en proscrire les usages policiers. A notre tour, nous appelons à l'interdiction de la reconnaissance faciale.

Martin Drago est juriste au sein de l'association La Quadrature du Net, spécialisée dans la défense « des libertés fondamentales dans l'environnement numérique ». Félix Tréguer est chercheur postdoctorant au Centre de recherches internationales (CERI) de Sciences Po.
Félix Tréguer (chercheur au CERI) et **Martin Drago** (juriste)

Nice va tester la reconnaissance faciale sur la voie publique

La municipalité, adepte de la vidéosurveillance, a décidé d'expérimenter un dispositif de reconnaissance faciale à l'occasion du carnaval de Nice.

Le Monde avec AFP Publié le 18 février 2019 à 21h46 - Mis à jour le 19 février 2019 à 14h24

Le maire de Nice, Christian Estrosi, a poussé à l'installation de caméras de surveillance dans sa ville, qui en compte une pour 145 habitants. ÉRIC PIERMONT / AFP

Ce sera une première en France. Lundi 18 février, le maire Les Républicains (LR) de Nice, Christian Estrosi, a annoncé lors d'une conférence de presse que sa municipalité allait tester un système de reconnaissance faciale sur la voie publique via ses caméras de vidéosurveillance. Le test va durer deux jours dans une partie de l'enceinte du carnaval de Nice, dont la 135e édition a commencé samedi. Il concerne exclusivement des personnes volontaires.

L'expérimentation permettra de tester différents scénarios, comme celui d'un enfant perdu dans la foule, d'une personne âgée vulnérable elle aussi égarée ou encore d'une personne dite « d'intérêt », c'est-à-dire recherchée, en utilisant six caméras de vidéosurveillance positionnées sur le périmètre de test.

Une participation volontaire

Un millier de volontaires venant au carnaval vont être amenés à jouer le rôle de cobaye et à accepter le principe de la reconnaissance faciale, ce qui permettra ensuite de rechercher parmi eux des personnes dont les opérateurs de vidéosurveillance auront la photographie. Les personnes qui ne seront pas volontaires auront le visage flouté et ne seront pas reconnaissables sur les images.

Prévenue au début du mois par l'équipe de Christian Estrosi, la Commission nationale de l'informatique et des libertés (CNIL) a accompagné l'expérimentation, mais n'a pas eu à donner une autorisation préalable : celle-ci n'est plus obligatoire pour les dispositifs biométriques depuis l'entrée en application du Règlement général pour la protection des données (RGPD) européen.

Dans une série de messages postés sur Twitter, mardi 19 février, la Commission a dit regretter *« l'urgence dans laquelle ses services ont été sollicités »*, son accompagnement ayant été demandé par la municipalité moins d'un mois avant le carnaval, et souhaite un *« bilan de cette expérimentation »* dans les deux mois suivant la manifestation.

#Nice06 #ReconnaissanceFaciale Depuis l'entrée en application du #RGPD, les dispositifs biométriques ne sont plus… https://t.co/nrt3fzoXNn
— CNIL (@CNIL)

Par ailleurs, la CNIL rappelle que la reconnaissance faciale sur la voie publique ne peut, dans le cadre législatif actuel, *« aller au-delà du simple test »*, puisque aucune loi n'est aujourd'hui adaptée spécifiquement aux *« dispositifs de reconnaissance faciale »*. Elle a demandé aux équipes de Christian Estrosi d'installer des panneaux informatifs expliquant clairement aux participants aux festivals les conditions et l'obligation de consentement de l'expérimentation.

La licence du logiciel employé, AnyVision, appartient à l'entreprise Confidentia. Selon son président, Jean-Philippe Claret, il permet *« de reconnaître quelqu'un même si la photo a trente ans »* ou encore de reconnaître une personne passant de profil près d'une caméra, même si la photo fournie est de face.

Obtenir la liste des « fichés S »

Nice compte une caméra pour cent quarante-cinq habitants. Par le passé, la municipalité s'était déjà montrée encline à doubler son important parc de caméras de procédés de cette nature. Quelques semaines avant l'attentat de la promenade des Anglais (86 morts), lors de l'Euro 2016 de football, M. Estrosi avait déjà demandé sans succès au gouvernement l'autorisation d'utiliser la reconnaissance faciale à l'entrée de la fan-zone installée dans sa ville.

Plus récemment, en décembre 2018, il avait demandé au préfet de lui fournir la liste des « fichés S » (pour sûreté de l'Etat) de sa ville, afin de *« pouvoir suivre toutes les allées et venues, dans les transports en commun, dans les artères, dans les lieux publics, des individus en question »*, à l'aide d'un logiciel de reconnaissance faciale qui serait relié à l'ensemble des caméras de la ville.

Reconnaissance faciale : la CNIL tique sur le bilan de l'expérience niçoise

Pour la mairie de Nice, le test de la reconnaissance faciale mené en février est très satisfaisant. Mais le gendarme de la vie privée dit manquer de détails pour un véritable diagnostic.

Par Martin Untersinger Publié le 28 août 2019 à 12h15 - Mis à jour le 29 août 2019 à 10h07

Temps deLecture 4 min.

Durant trois jours en février, quelques milliers de Niçois ont été les cobayes d'une expérience unique en France : leurs visages captés par la vidéosurveillance ont été analysés en temps réel par un logiciel de reconnaissance faciale.

Comme demandé à l'époque par la Commission nationale de l'informatique et des libertés (CNIL), compétente en matière de vidéosurveillance, un rapport tirant le bilan de cette expérience, dont *Le Monde* a obtenu copie, a été rédigé par la mairie de Nice et transmis à la CNIL.

La mairie de Nice très satisfaite

Le dispositif conçu par la ville de Nice était relativement simple : les images de vidéosurveillance de l'une des entrées du carnaval passaient à la moulinette d'un logiciel développé par l'entreprise israélienne AnyVision. Le but : en évaluer la pertinence et la fiabilité.

Deux grandes situations ont été mises en place. Sur les files d'attente, d'abord, où le logiciel devait détecter la présence d'un volontaire ayant préalablement fourni une photographie de son visage. Cela a fonctionné, affirme la mairie, y compris avec une photographie vieille de plusieurs décennies. Sur la foule en mouvement, ensuite, où le logiciel était chargé de reconnaître une personne recherchée, là encore volontaire. Carton plein pour le logiciel, selon la mairie, qui a passé ce test avec succès, même lorsque la personne était en mouvement ou camouflée par une casquette ou des lunettes de soleil. Le logiciel, affirme le rapport, est même parvenu à distinguer deux jumeaux monozygotes (il n'a pas détecté celui qui n'était pas recherché).

L'entrée de la zone d'expérimentation de reconnaissance faciale. Mairie de Nice

Un dispositif d'information avait été mis en place à l'entrée de la zone vidéosurveillée et seules les personnes ayant accepté de participer à l'expérience (un peu plus de 5 000 personnes) ont été passées au tamis du logiciel. *« Aucune plainte quelconque* [*sic*] *de la part des usagers »,* n'a été recensée, écrit la mairie. Du côté des agents de la police municipale, c'est, semble-t-il, l'unanimité. *« La reconnaissance faciale est perçue par les agents ayant participé à l'expérimentation comme un outil fiable et pertinent »*, écrit la municipalité, qui reproduit à l'appui de sa démonstration plusieurs rapports rédigés par ses agents, tous positifs.

La CNIL tique et demande des précisions

Le rapport est pourtant avare de détails, notamment techniques, sur le mode de fonctionnement exact du logiciel. A-t-il détecté par erreur des personnes qui n'étaient pas recherchées, ce qu'on appelle un « faux positif », l'un des principaux défauts de cette technologie ? A-t-il manqué dans la foule une personne pourtant recherchée ? Qu'a-t-il été fait des données biométriques (captation du visage des 5 000 participants) à l'issue de l'expérience ?

Sollicitée, la mairie de Nice nous a assuré qu'*« aucun faux positif n'était remonté »,*que *« l'ensemble des scénarios déployés avait permis d'obtenir une détection et une reconnaissance des personnes d'intérêt dans 100 % des cas »* et que la durée de conservation des données avait été communiquée à la CNIL dans un précédent document.

Ce rapport est en tout cas loin d'avoir contenté la CNIL, à qui il a été présenté début juillet. Le texte, trop imprécis et manquant d'éléments techniques, n'a pas permis d'avoir *« une vision objective de cette expérimentation et un avis sur son efficacité »,* fait-on ainsi savoir. L'autorité administrative a donc demandé, par un courrier du 16 juillet, de nombreux compléments d'informations, en particulier des éléments chiffrés sur l'efficacité du dispositif technique ou sur les conséquences concrètes d'un possible biais (lié au genre, à la couleur de peau…) du logiciel.

La CNIL expliquait, mardi, ne pas avoir reçu de réponse de la mairie de Nice. Cette dernière nous a fait savoir, mercredi après-midi, que ce courrier était *« en cours d'instruction »* par ses services et que l'expérience avait été trop courte pour répondre à certaines questions de la CNIL. Si la loi ne permet pas en l'état à la mairie d'aller plus loin que son test de février, elle ne donne pas non plus à la commission de pouvoir coercitif lorsqu'il s'agit d'une simple expérimentation.

Les relations entre l'autorité administrative et la ville dirigée par Christian Estrosi étaient déjà fraîches : le maire s'était vanté d'avoir obtenu une autorisation de la CNIL pour cette expérimentation, avant d'être publiquement démenti par l'institution. Le gendarme de la vie privée avait aussi déploré *« l'urgence dans laquelle ses services ont été sollicités »* – moins d'un mois avant l'expérimentation prévue – et des *« circonstances n'étant pas de nature à favoriser un travail d'analyse approfondie du dispositif projeté »*.

Un cadre juridique insatisfaisant

La mairie de Nice et la CNIL sont, cependant, d'accord sur un point : la France doit rénover son cadre juridique et se poser sérieusement la question des nouvelles technologies de vidéosurveillance. La mairie azuréenne regrette ainsi dans son rapport *« l'absence de loi encadrant l'expérimentation de nouvelles technologies en conditions réelles »*, ce qui l'a contrainte, assure-t-elle, à se limiter : elle aurait aimé tester cette technologie sur toute l'emprise du carnaval, et non seulement à l'une de ses entrées. La mairie veut même voir plus loin et assure que les*« résultats de cette expérimentation vont être utilisés dans le cadre d'une réflexion visant à aboutir à la rédaction d'un projet/proposition de loi »*.

De son côté, la CNIL réclame depuis plusieurs mois que le législateur se penche sur les nouvelles utilisations sécuritaires de la vidéosurveillance afin de compléter le cadre légal existant et de le doter de garde-fous. L'offre – de la part des industriels – et la demande – venant des services de sécurité et des municipalités – existent et les Jeux olympiques de 2024, organisés en France, sont dans toutes les têtes.

Ces derniers représenteront un enjeu en matière de sécurité et pourraient être l'occasion pour les pouvoirs publics de légiférer sur la reconnaissance faciale. En juin, le ministre de l'intérieur, Christophe Castaner, justement venu prendre connaissance des résultats de l'expérience niçoise, avait jugé important *« d'ouvrir le débat »* sur le sujet. Dans son rapport, la mairie de Nice a en tout cas arrêté sa position : il faudrait que les Jeux olympiques puissent *« accueillir une technologie mature »* de reconnaissance faciale.

Martin Untersinger

« Cette reconnaissance faciale, c'est trop » : dans un quartier de New York, des locataires en colère

Des résidents ont attaqué en justice la décision du gérant de leur immeuble, qui souhaite installer des caméras à reconnaissance faciale.

Par Arnaud Leparmentier Publié le 05 juillet 2019 à 10h01 - Mis à jour le 05 juillet 2019 à 17h01

« Je ne peux pas vous laisser entrer. » La gardienne de l'Atlantic Plaza Towers est à son poste, derrière son pupitre, mais elle est inaccessible. Pour pénétrer dans cet immeuble au cœur d'un quartier noir de Brooklyn, à New York, le visiteur doit franchir une première porte vitrée, sonner à l'interphone de son hôte pour se faire ouvrir une seconde porte. Enfin, on arrive devant la gardienne, qui vous observe, ainsi que sa caméra à peine dissimulée. Si vous prouvez votre identité, peut-être vous laissera-t-elle franchir la troisième porte vitrée et accéder aux appartements. Du reste, on ne sait rien, si ce n'est que l'immeuble à loyer réglementé est rempli de caméras, y compris dans les ascenseurs.

Les locataires, eux, pénètrent dans l'immeuble avec des badges électroniques. Dans quelques semaines, ce sera sans doute pire. Le gérant de l'immeuble, Nelson Management Group, veut installer des caméras à reconnaissance faciale pour pallier la faiblesse des badges, qui peuvent être volés ou copiés. Tous les locataires devront s'y plier pour franchir la deuxième porte, celle qui mène au gardien. C'est la goutte d'eau qui a fait déborder le vase : quelque 134 locataires se sont mobilisés et ont attaqué en justice cette décision, début mai. Ils attendent un jugement des autorités de New York.

En attendant, l'ambiance est tendue. On est le seul Blanc dans ce quartier en voie de légère gentrification. Des Afro-Américains et des Africains, quelques Latinos. On se fait sèchement rembarrer, avant de trouver quelques interlocuteurs bienveillants. *« C'est un bon endroit »*, estime Nicole Dunkin, qui vient de rendre visite à son père. *« Tout le monde se connaît, il n'y a pas besoin de reconnaissance faciale »*, assure la jeune femme. Même discours de Jeff Cervois, de lointaine origine haïtienne, qui se promène avec ses deux enfants.

« Cette reconnaissance faciale, c'est trop. Ce bâtiment n'est pas dangereux, c'est très familial. Peut-être n'était ce pas le cas il y a quelques années. Ce sont sûrement des partisans de Donald Trump qui ont eu cette idée. »

Abus de pouvoir

L'idée a irrité, car cette « première », comme par hasard, vise des pauvres, des personnes de couleur (90 % de la population de l'immeuble) et des femmes (80 %). Le sujet est encore plus sensible, car la technologie n'est pas au point… pour les Noirs. Une étude réalisée par le Massachusetts Institute of TechnologyMedia Lab, de Boston, a montré que les systèmes de reconnaissance faciale étaient efficaces pour les hommes blancs à 99 %, mais que le taux d'erreur atteignait 35 % pour les femmes à peau noire. L'association American Civil Liberties Union a fait passer les membres du Congrès à la moulinette du logiciel d'Amazon, en comparant leur photo à un fichier de 25 000 portraits de délinquants pris par la police : 28 membres du Congrès ont été, à tort, identifiés comme délinquants.

Les locataires craignent des abus de pouvoir du propriétaire, et la plainte déposée insiste sur le côté racial

Outre le débat sur l'atteinte à la vie privée et le fichage de ses visiteurs, le sujet peut avoir des conséquences fâcheuses : que le système ne fonctionne pas, et ce sont des locataires et leurs visiteurs qui risquent de se voir dénier le droit d'entrer dans leur appartement. Les locataires craignent des abus de pouvoir du propriétaire, et la plainte déposée en leur nom insiste sur le côté racial.

Dans sa plainte l'avocate militante Samar Katnani écrit :

« Cette technologie va seulement servir à contrôler encore plus un groupe de locataires noirs et à la peau foncée, pour qui les atteintes à la vie privée sont une vraie menace. »

Elle estime que ces communautés sont *« poussées encore plus aux marges de la société, parce que la surveillance et le sentiment d'être observé génère de la peur et de l'incertitude, ce qui conduit les gens à se faire leur propre police et inhibe leur activité dans l'espace public ».*

Un débat public qui prend de l'ampleur

Ce genre de cas reste marginal pour l'instant. Un immeuble de Detroit (Michigan) a été équipé par la police, mais la ville est – avec Chicago (Illinois) et Baltimore (Maryland) – une des capitales du crime aux Etats-Unis. Pour autant, on se fait déjà très régulièrement photographier à l'entrée des immeubles de bureaux de Manhattan, et la reconnaissance faciale, qui est utilisée par la police des frontières pour les étrangers arrivant sur le territoire américain, devrait se généraliser pour les vols domestiques dans les aéroports. Le débat public sur l'utilisation de cette technologie prend de l'ampleur.

Bradford Smith, président de Microsoft, avait appelé, en 2018, le Congrès a se saisir du dossier pour légiférer, estimant que l'affaire ne pouvait être laissée à la seule autorégulation des entreprises. En 2012, la Federal Trade Commission, le régulateur américain du commerce, avait recommandé qu'un système permettant facilement à l'usager ou au consommateur de ne pas être l'objet de reconnaissance faciale soit généralisé, mais le Congrès n'a jamais légiféré. Résultat, comme souvent, ce sont les collectivités locales qui agissent – San Francisco a banni son usage en mars – ou les entreprises, qui font mine de prévenir leurs clients. La compagnie aérienne Delta indique ainsi que son terminal F d'Atlanta organise les contrôles de sécurité par le biais de la reconnaissance faciale. Officiellement, on peut ne pas s'y soumettre – (2 % des passagers le font chez Delta). Pour l'instant.

San Francisco interdit la reconnaissance faciale

Huit des neuf membres du conseil municipal de la ville se sont prononcés en faveur d'un texte interdisant aux services de police et à la municipalité d'utiliser cette technologie.

Par Corine Lesnes Publié le 15 mai 2019 à 08h17 - Mis à jour le 15 mai 2019 à 11h18

A tout seigneur, tout honneur. Par un vote quasi-unanime de ses conseillers municipaux, San Francisco est devenue la première ville des Etats-Unis à imposer des limites à la pratique de reconnaissance faciale. « *La propension de la technologie de reconnaissance faciale à mettre en danger les libertés civiles surpasse substantiellement ses bénéfices supposés*, indique le texte adopté mardi 14 mai. *La technologie va exacerber les injustices raciales et menacer notre capacité à vivre libres de la surveillance permanente du gouvernement ».*

Les défenseurs de la vie privée, de l'Electronic Frontier Foundation à l'ACLU (association de défense des libertés civiles) avaient fait campagne contre cette technologie – largement utilisée en Chine – qui permet d'identifier les passants dans la rue, les magasins, les aéroports, les stades, et potentiellement les manifestants.

Les forces de l'ordre l'utilisent depuis longtemps pour passer en revue des banques d'images à la recherche de suspects, mais les progrès de l'intelligence artificielle font craindre la généralisation de la pratique. Déjà, certaines chaînes de magasins l'utilisent pour deviner l'âge ou le sexe des consommateurs et analyser leur expression alors qu'ils passent les produits en revue, le but étant de leur diffuser des publicités ou des promotions ciblées.

Potentiel dystopique

De nombreuses compagnies, d'Amazon à FaceFirst et Microsoft, offrent des produits ou services de reconnaissance faciale. Le géant de Seattle a d'ailleurs lui-même appelé le Congrès à réglementer le secteur, au regard de son potentiel dystopique.

La circulaire sur « l'arrêt de la surveillance » adoptée à San Francisco ne s'applique qu'aux services municipaux et à la police – qui a cessé de tester la reconnaissance faciale depuis une vague de protestations en 2017. Elle ne concernera pas le secteur privé ni l'aéroport où la sécurité est du ressort de l'Etat fédéral. Mais elle requiert un

processus d'information et de contrôle public pour l'acquisition de technologies de surveillance telles que les lecteurs automatisés de plaques minéralogiques.

La quasi-unanimité des membres du conseil municipal de San Francisco (8 à 1) illustre à quel point la suspicion s'est propagée dans la capitale des technologies. La plateforme de stockage de photos Ever a dû reconnaître qu'elle rentabilisait les photos de famille postées par les usagers sans les en informer explicitement. Elle s'est défendue en expliquant qu'elle ne vend pas directement les informations mais les utilise pour développer son propre algorithme de reconnaissance faciale. Dont elle vend ensuite les services à ses clients.

Les mesures de protection

La reconnaissance faciale pour s'identifier en ligne inquiète les défenseurs des libertés numériques

Un recours a été déposé devant le Conseil d'Etat pour faire annuler le décret autorisant l'application AliceM.

Par Léa Sanchez Publié le 27 juillet 2019 à 08h51 - Mis à jour le 29 juillet 2019 à 07h15

BORIS SEMENIAKO

Scanner la puce de son passeport biométrique à l'aide de son téléphone et prendre une vidéo de soi pour créer son compte et pouvoir accéder à des services administratifs en ligne : c'est le principe de l'application « Authentification en ligne certifiée sur mobile », surnommée « AliceM ». Ce système, présenté commetrès sécurisé par le ministère de l'intérieur et utilisable uniquement sur Android, devrait permettre de s'authentifier sur les sites liés au portail d'accès FranceConnect : celui des impôts, de la Sécurité sociale…

Mais AliceM, qui est encore en phase de test, suscite des interrogations et des inquiétudes, venant notamment des défenseurs des libertés numériques.

Le 15 juillet, l'association spécialisée La Quadrature du Net a déposé un recours devant le Conseil d'Etat pour annuler le décret du 13 mai autorisant le dispositif. Elle dénonce un traitement intrusif de données biométriques *« ayant pour objectif avoué d'identifier chaque personne sur Internet pour ne plus laisser aucune place à l'anonymat ».*

« Prémices » d'une politique publique de l'identité numérique

Le projet des pouvoirs publics de développer des solutions d'identité numérique n'est pas nouveau. Si, en 2012, le Conseil constitutionnel avait jugé inconstitutionnel la création d'une base de données biométriques, l'Agence nationale des titres sécurisés (ANTS) et le ministère de l'intérieur travaillentdepuis plusieurs années sur AliceM. En septembre 2017, la feuille de route du ministère de l'intérieur mentionnait sa volonté de se positionner *« comme maître d'ouvrage et maître d'œuvre de l'élaboration de solutions d'identité numérique ».*

En mai, à l'occasion de la publication du rapport « Etat de la menace liée au numérique en 2019 », le locataire de Beauvau, Christophe Castaner, affirmait vouloir que *« chaque Français, dès 2020, puisse prouver son identité »* en ligne pour, notamment, *« bâtir la sécurité du XXIe siècle »* et lutter contre les contenus haineux sur Internet. Il affirmait à cette occasion qu'AliceM constituait l'un des*« prémices d'une politique publique de l'identité numérique ».*

Dans le recours qu'elle a déposé, La Quadrature du Net centre son argumentaire sur le caractère obligatoire de la reconnaissance faciale dans le fonctionnement de l'application.

Dès octobre 2018, dans un avis portant sur le projet de décret visant à autoriser AliceM, la Commission nationale de l'informatique et des libertés (CNIL) émettait aussi des doutes sur ce point et proposait des alternatives, comme un face-à-face en préfecture. *« 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 »,* écrivait-elle, rappelant les exigences du Règlement général sur la protection des données (RGPD) en la matière.

« Normaliser » la reconnaissance faciale

Pour La Quadrature du Net, maintenir ce système dans ces conditions renforce une *« normalisation »* de la reconnaissance faciale. *« C'est un bras d'honneur à la CNIL »*, s'insurge Martin Drago, juriste pour l'association.

Le militant pointe les limites techniques de la reconnaissance faciale, mais surtout les conséquences sur la société liées à l'utilisation de ces données sensibles : *« Le danger, c'est que notre visage ne devienne plus qu'un outil d'identification, un outil utilitaire. »* Il regrette l'absence de débat public en France sur cette question, malgré les expérimentations ayant déjà eu lieu. A Nice, par exemple, la municipalité a décidé en février de tester un dispositif de reconnaissance faciale sur la voie publique.

En plus des informations biométriques, le décret autorisant AliceM indique que de nombreuses données à caractère personnel sont susceptibles d'être enregistrées : nom, prénom, adresse postale, sexe, informations relatives au titre d'identité utilisé…

Une partie d'entre elles seront uniquement stockées, de manière chiffrée, sur le téléphone de l'usager. D'autres, notamment celles liées à *« l'historique des transactions associées au compte AliceM »*, seront également conservées dans un*« traitement centralisé »* mis en œuvre par l'ANTS et supprimées *« à l'issue d'une période d'inactivité du compte de six ans ».* Une durée supérieure à celle que préconisait la CNIL : dans son avis rendu en 2018, elle recommandait une conservation de ces données *« pour une durée maximale de six mois ».*

Léa Sanchez

« Big Brother » : quand les Chinois se rebiffent

L'annonce d'une prochaine mise en place d'un système de reconnaissance faciale dans le métro de Pékin a suscité un réel débat dans le pays, jusque dans la presse officielle.

Par Frédéric Lemaître Publié le 27 décembre 2019 à 02h47 - Mis à jour le 31 décembre 2019 à 05h35

Des caméras d'intelligence artificielle (IA) lors d'une exposition sur la sécurité publique, à Pékin, en octobre 2018. NICOLAS ASFOURI / AFP

LETTRE DE PÉKIN

Trop, c'est trop. L'annonce d'une prochaine mise en place d'un système de reconnaissance faciale dans le métro de Pékin a fait sortir Lao Dongyan de ses gonds. Professeure de droit à l'université de Tsinghua, la plus prestigieuse du pays, cette juriste a, malgré les risques pour sa carrière, rédigé fin octobre un long article sur les réseaux sociaux chinois pour dire tout le mal qu'elle pense de cette décision.

« C'est fou, écrit-elle. *Vous avez besoin de montrer votre carte d'identité quand vous entrez ou sortez du campus universitaire, d'enregistrer votre carte d'identité quand vous ouvrez un compte e-mail, de scanner votre visage quand vous réservez une chambre d'hôtel. De passer un portique de sécurité pour prendre le métro. Et ce n'est pas suffisant. Maintenant il va falloir aller encore plus loin et utiliser la prétendue nouvelle technologie pour continuer de renforcer le niveau de sécurité. Je pose la question : quand cela cessera-t-il ? »*Avant de *« solennellement recommander au comité permanent du bureau politique »* du Parti communiste chinois, soit aux plus hauts dirigeants du pays, de s'emparer du sujet, Lao Dongyan commence par réfuter quatre contre-arguments. Le premier : il faudrait plutôt remercier le gouvernement, « figure paternelle », pour sa protection. Réponse cinglante : *« Les personnes qui contrôlent nos données ne sont pas Dieu. Elles ont leurs propres désirs et leurs propres faiblesses. De plus, on ne sait pas comment elles vont utiliser nos données personnelles ni comment elles veulent manipuler nos vies. »*

« Sans vie privée, pas de liberté »

Deuxième contre-argument : si on ne fait rien de mal, on n'a rien à craindre. Réponse de Lao Dongyan : *« Dans une société normale, les individus devraient avoir le droit de s'opposer à l'accès arbitraire de quelque organisation que ce soit à leurs données biométriques personnelles.* (…) *Sans vie privée, il n'y a pas de liberté. »*

Troisième contre-argument : les gens pas importants ne sont pas concernés. Réponse : *« Quand vous comptez sur la négligence d'autrui pour assurer votre sécurité personnelle* (…), *vous ne pariez pas seulement sur votre chance, mais*

également sur le fait que la personne qui contrôle vos données est un ange. (…)*J'admire votre politique de l'autruche. »*

Quatrième contre-argument : tout cela ne sert à rien. Réponse : *« Même si, à la fin, cela ne sert à rien, ça vaut mieux que d'accepter docilement d'avoir des chaînes au pied. Au moins, on a lutté. »*

Dans un second temps, cette juriste argumente sur les raisons pour lesquelles elle s'oppose à la reconnaissance faciale dans le métro de Pékin : vu l'importance des données biométriques pour les individus, *« les organisations ou les institutions compétentes doivent prouver la légitimité de leur méthode avant* [le] *recueil* [de données]. *La mise en place dans le métro sans avoir écouté le public enlève toute légitimité au processus. Ensuite, nul ne sait selon quels critères les autorités de transports vont se permettre de classer les voyageurs en différents groupes. Cela va à l'encontre de l'article 37 de la Constitution »*, dit-elle. Enfin *« rien ne prouve que la reconnaissance faciale rende les transports plus efficaces et, même si c'était le cas, ce ne serait pas un critère suffisant. »*

Même la presse officielle en parle

Agée d'une quarantaine d'années, cette femme – qui ne répond pas aux journalistes – fait preuve d'un courage inouï. Mais tout aussi étonnant est le fait que ses propos aient pu être rendus publics et qu'ils aient suscité un réel débat.

Un avocat de Pékin, Lu Liangbiao, va même encore plus loin : *« Le peuple est un maniaque de l'ordre. Il ne se sent en sécurité que lorsque l'Etat s'occupe de lui. Mais le pouvoir est encore plus maniaque et veut tout contrôler. Cela le rassure.* (…) *Les caméras feraient mieux de surveiller les fonctionnaires et les dirigeants sur l'emploi qu'ils font de l'argent public, plutôt que de contrôler les simples citoyens. »*

Signe que le sujet est sensible, même la presse officielle en parle. *« La reconnaissance faciale provoque un débat national »*, constate en première page le*China Daily,* le 19 novembre. Si le quotidien ne mentionne pas le texte – trop sulfureux – de M^me^ Lao, il évoque longuement un autre cas : la plainte déposée en octobre 2019 par un juriste du Zhejiang contre un parc animalier. Cet homme qui, en avril, avait payé un droit d'entrée annuel et laissé ses empreintes digitales, réclame le remboursement de sa cotisation parce que le parc exige désormais que les clients acceptent le mécanisme de reconnaissance faciale. Même le journal télévisé national en a parlé. Une étude publiée fin décembre par la très officielle Académie chinoise des sciences sociales révèle que 90 % des 3 200 personnes interrogées par celle-ci s'inquiètent de l'utilisation de leur données par un tiers.

Contrairement aux Occidentaux qui essaient de fixer un cadre juridique en amont des innovations technologiques, la Chine fait l'inverse. Elle incite chercheurs et entrepreneurs à innover et, une fois que le processus est mature et que ses premiers effets se font sentir, elle commence à réguler. Il semble donc que le temps d'un débat contrôlé sur le sujet soit venu. Mais celui-ci ne devrait pas s'éterniser. C'est en 2020 que le « crédit social », accordant une note à chaque citoyen, devrait être généralisé.

Reconnaissance faciale : « Il existe encore en France des garde-fous en matière de données biométriques »

Claire Gerardin

Consultante en communication

Si la loi française garantit la liberté des personnes « contre une reconnaissance faciale encore trop peu performante », il faut questionner les usages futurs de cet outil, notamment en termes de surveillance sécuritaire, souligne, dans une tribune au « Monde », la consultante en communication Claire Gerardin.

Publié hier à 05h00, mis à jour hier à 08h09 Temps deLecture 4 min.

Depuis plus d'un siècle se pose la question de savoir jusqu'où l'objectif de garantir la sécurité des personnes n'empiète pas, ou pas trop, sur leur liberté, et sur leur vie privée. La technologie de la reconnaissance faciale relance de nouveau le débat.

Aujourd'hui, dans un contexte de menace terroriste, mais aussi de certaines rhétoriques anxiogènes, garantir la sécurité des citoyens est au cœur des préoccupations publiques et électorales. Cela représente une opportunité pour les industriels, qui développent des outils de plus en plus performants en matière de surveillance sécuritaire comme ceux de la reconnaissance faciale.

Authentifier, identifier

Basée sur des techniques de biométrie – qui permettent d'extraire des caractéristiques physiques, biologiques et comportementales d'un individu, cette technologie consiste à filmer ou photographier une personne pour constituer un gabarit, c'est-à-dire sa signature biométrique. La plupart des usages de la reconnaissance faciale aujourd'hui poursuivent des objectifs d'authentification ou d'identification de personnes.

Pour ce faire, on doit pouvoir faire correspondre une image captée en temps réel à un gabarit enregistré dans une base de données. Ce qui implique d'avoir accès à une telle base de données, et qu'elle soit constituée d'images acquises dans les mêmes conditions qu'en situation de captation afin de permettre l'appariement. Pour les applications du type de la reconnaissance des personnes aux aéroports, on approche, en comparant une photo de passeport à une photo posée prise au guichet du douanier, les 100 % de succès.

« En France, l'identification automatique sur les voies publiques par des caméras de surveillance et son croisement avec une base de données sont formellement interdits »

Mais pour toutes les situations de mobilité (lorsqu'une personne marche dans la rue, par exemple), l'efficacité de ces techniques est encore très limitée. Car les capteurs sont vite pris en défaut par de nombreuses variations telles que la rotation du visage, son expression – le visage comportant 40 muscles, on imagine le nombre de combinatoires*[regroupement de phénomènes]* liées à leur activation simultanée ou non – l'éclairage, la pilosité, le port d'un chapeau ou de lunettes, le maquillage, etc. Dans de tels cas, on observe des taux d'erreurs qui atteignent souvent… 100 %. Ces capteurs devraient évoluer avec l'émergence de la technologie de la 3D et des capteurs de flux thermiques qui fonctionnent grâce au thermogramme *[carte thermique]* facial, déterminé par la graisse, les muscles et les os.

On cite souvent la Chine comme exemple de cauchemar en matière de reconnaissance faciale, avec la mise en place de son système de « crédit social ».Mais, d'une part, ce programme n'est pas entériné, il est encore en test dans 43 villes ; et, d'autre part, les technologies utilisées ne sont pas aussi performantes qu'on l'imagine. Par ailleurs, la notion de citoyenneté selon le régime chinois ne relève pas de la même logique qu'en Occident, et le système de notation des citoyens n'a pas attendu la reconnaissance faciale pour être institué.

Cette notation est en fait déjà pratiquée sous diverses formes depuis de nombreuses années dans ce pays (« China's Social Credit System : A Chimera with Real Claws », Séverine Arsène, *Visions* n°110, IFRI, novembre 2019). Enfin, la collecte de données biométriques suscite actuellement une vague d'oppositions qui a incité le gouvernement à préparer une loi sur la protection des données personnelles.

Vide juridique

En France, presque toutes les villes sont équipées de systèmes de caméras de surveillance, mais quasiment aucun n'est couplé ni à une technologie de reconnaissance faciale, ni à une base de données. La loi actuelle laissant un certain vide juridique en matière d'expérimentations d'identification par reconnaissance faciale, certaines collectivités (comme Nice ou Marseille) ont lancé des initiatives mais la Commission nationale de l'informatique et des libertés (CNIL) s'y est opposée. Le projet gouvernemental d'authentification Alicem – qui

prévoyait de donner accès à différents services publics en ligne au moyen d'une authentification par reconnaissance faciale – a fait l'objet d'un avis critique de la CNIL et d'un recours déposé par l'association La Quadrature du Net. Le décret autorisant sa création a été publié en mai dernier, mais le projet est toujours en phase de test. Le secrétaire d'Etat au numérique, Cédric O, a indiqué fin décembre 2019 qu'aucune date de déploiement n'était encore fixée et qu'un *« travail de consultation »* était en cours *« par le Conseil national du numérique ainsi qu'une mission parlementaire »*.

Il existe en Europe et en France des garde-fous protégeant la liberté des personnes contre la reconnaissance faciale. L'identification automatique sur les voies publiques d'un individu par des caméras de surveillance et son croisement avec une base de données sont formellement interdits, sauf en cas de demande par un juge pour un délit criminel. Pour les systèmes d'authentification, le règlement général sur la protection des données (RGPD) impose d'obtenir le consentement préalable de l'individu, de lui proposer une autre solution que la reconnaissance faciale, et ses données personnelles ne peuvent être conservées.

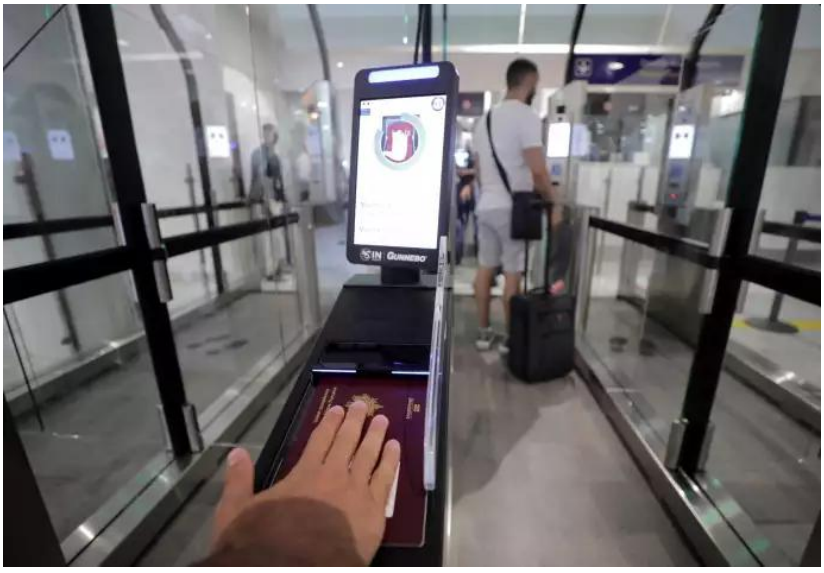
La reconnaissance faciale est déjà utilisée pour favoriser des conforts d'usage comme passer plus rapidement le contrôle des douanes, déverrouiller son smartphone, ou retrouver des amis sur Facebook. Ces usages anodins nous accoutument à son utilisation, nous la rendent acceptable. Néanmoins, cette technologie est encore une « chimère », car elle n'est pas performante pour des usages plus élaborés. Mais puisqu'elle le sera un jour, il faut questionner dès aujourd'hui les objectifs de ses futurs usages : sécurité, surveillance, confort d'usage ?

Claire Gerardin est consultante en communication, spécialiste des nouvelles technologies.

La CNIL plaide pour un « code de la route » de la reconnaissance faciale

Même si le gendarme français de la vie privée n'exclut aucun usage de cette technologie, y compris les plus intrusifs, il défend, dans une note inédite, une utilisation minimale et très encadrée.

Par Martin Untersinger Publié le 15 novembre 2019 à 05h59 - Mis à jour le 16 novembre 2019 à 08h57



A l'aéroport de Nice, en juillet 2018. La reconnaissance faciale est déjà utilisée au sein des portiques de sécurité biométriques. ERIC GAILLARD / REUTERS

Alors que les questions sur la reconnaissance faciale se font plus prégnantes et les velléités gouvernementales en la matière plus précises, le gendarme français de la vie privée cherche à se faire entendre. La Commission nationale de l'informatique et des libertés (CNIL) publie, vendredi 15 novembre, un document inédit dans lequel elle détaille ce qu'elle estime être les règles du jeu du débat public à venir autour de cette technologie.

L'autorité indépendante chargée de la protection des données personnelles sent que les choses s'accélèrent et n'aimerait pas être ignorée. A l'échelon local, des expérimentations ont déjà été menées à Nice ou Marseille. Dans les colonnes du*Monde,* le secrétaire d'Etat au numérique, Cédric O, s'est déclaré favorable à la multiplication des expériences. L'Etat travaille également, en dépit des réserves exprimées par la CNIL, sur un dispositif d'identification par reconnaissance faciale, Alicem, destiné aux sites Internet de service public.

Lors d'un colloque organisé le 7 novembre à Paris, le préfet responsable de l'intelligence artificielle (IA) au ministère de l'intérieur, Renaud Vedel, a plaidé en faveur d'*« un cadre juridique pour la recherche et le développement »* en matière d'IA, sujet qui inclut la reconnaissance faciale. Les industriels, quant à eux, souhaiteraient trouver des débouchés pour leurs technologies et lorgnent la Coupe du monde de rugby de 2023 ainsi que les Jeux olympiques de 2024, tous deux organisés en France. Le cadre juridique en vigueur demeure cependant très rigide : il interdit la manipulation de données biométriques (l'image du visage en fait partie), interdiction qui ne peut être contournée que de manière très limitée.

Avec ce document, la CNIL escompte *« définir le code de la route des usages de la reconnaissance faciale »,* explique au *Monde* sa présidente, Marie-Laure Denis. Ces grands principes sont destinés à accompagner un éventuel texte de loi plus permissif. L'institution redoute les expérimentations ponctuelles et plaide depuis longtemps pour que l'Etat mette au clair – définitivement et après un débat législatif – ce qu'il est possible de faire ou non avec cette technologie. Faute de quoi *« le risque est grand que ces choix nous échappent, que des glissements progressifs conduisent à un changement de société non anticipé et non souhaité, et que nous soyons, un jour, devant un fait accompli »,* écrit-elle dans sa note.

« Changement de paradigme »

Pour la CNIL, cette technologie est très loin d'être anodine. Les images du visage d'une personne sont en effet *« une réalité biologique qui lui est propre, permanente dans le temps et dont elle ne peut s'affranchir »*. De plus, *« les données*(…) *sont potentiellement disponibles partout »*, depuis que le recours à la vidéosurveillance et aux réseaux sociaux s'est généralisé.

Ses usages sont par ailleurs très variés. Entre le déverrouillage d'un téléphone sans que l'image du visage quitte la mémoire de l'appareil, l'identification d'un suspect sur une image de vidéosurveillance grâce à un fichier de police et la reconnaissance faciale à la volée dans l'espace public, toutes les utilisations ne se valent pas en termes de libertés publiques. Cette dernière possibilité, déjà pratiquée en Chine, *« appelle une vigilance toute particulière »*. Selon la commission, elle représente *« un changement de paradigme de la surveillance* (…) *: le passage d'une surveillance ciblée de certains individus à la possibilité d'une surveillance de tous aux fins d'en identifier certains »*.

Pour l'autorité indépendante, *« les atteintes à cet anonymat, par les pouvoirs publics ou par des organismes privés, sont ainsi susceptibles de remettre en cause certains de nos principes fondamentaux »*, car l'espace public est le lieu où s'exercent de nombreuses libertés (expression, réunion, manifestation…).

Malgré ces paroles fortes, la CNIL n'exclut aucun usage, y compris ce modèle hautement intrusif. *« Compte tenu de son ampleur et du degré de surveillance qu'il induit, ce type de cas d'usage appelle une analyse approfondie, dans chaque contexte d'utilisation et objectif par objectif »,* souligne l'institution dans son texte. Même s'il *« pose des questions préoccupantes pour les libertés publiques »*, ce mode de reconnaissance faciale peut avoir *« des usages légitimes »* et *« il n'y a pas de position tranchée de la part du collège de la CNIL »*, confirme Marie-Laure Denis.

Des choix « politiques »

Entre les lignes, on devine pourtant que l'institution plaide en faveur d'une utilisation minimale et très encadrée de cette technologie. *« Il ne faudrait pas que l'expérimentation ait pour objectif d'être un faux nez d'une généralisation de cette technologie. Les voitures peuvent rouler à 250 ou 300 km/heure, ce n'est pas pour autant qu'il est souhaitable qu'elles roulent à cette vitesse »*, précise Mme Denis.

Pour l'institution, la sécurité des données biométriques représentera « une priorité impérieuse »

La CNIL aimerait que certaines utilisations soient purement et simplement interdites, et ce, préalablement à tout essai. *« Il est important, compte tenu des risques, de définir des lignes rouges avant toute expérimentation »*, estime Mme Denis, citant, à titre d'exemple, le cas des mineurs dont les données sont étroitement protégées. Pour l'institution, la reconnaissance faciale ne doit être utilisée que lorsqu'il existe *« un impératif particulier d'assurer un haut niveau de fiabilité de l'authentification ou de l'identification »* des personnes et que son usage est le seul moyen d'y parvenir.

Par ailleurs, la sécurité des données biométriques représentera *« une priorité impérieuse »*. Un stockage *« sur un support individuel détenu par l'utilisateur, à la main de ce dernier, doit toujours être privilégié aux solutions de stockage en base centrale »*, juge la CNIL. Toute expérimentation devra aussi *« se prémunir de tout effet cliquet »*, en intégrant des limites claires *« dans le temps et dans l'espace »*,ainsi que des objectifs et des modalités d'évaluation bien définis, assortis de bilans d'étape adressés à la CNIL, suivant *« une méthode expérimentale rigoureuse »*.

Avec cette note, la CNIL entend lancer le débat politique qu'elle appelle de ses vœux depuis plus d'un an. Elle n'a pour l'heure été saisie d'aucun texte gouvernemental. *« Derrière les aspects techniques, il s'agit de procéder à des choix politiques, et de dessiner certains contours du monde de demain »*, assure l'institution. Avant de conclure : *« De tels choix ne peuvent être opérés à l'abri des regards ou du contrôle démocratique. »*

Martin Untersinger

Caroline Lequesne Roth : « L'encadrement des technologies de surveillance est une condition de la démocratie »

Caroline Lequesne Roth

Maître de conférences en droit public à l'université Côte d'Azur, cofondatrice du projet de recherche « Deep Law for Technologies » et responsable du Master 2 Droit algorithmique et gouvernance des données

La généralisation de la reconnaissance faciale à des fins de surveillance serait attentatoire aux libertés, estime, dans une tribune au « Monde », la juriste Caroline Lequesne Roth, qui plaide pour un large débat public afin de distinguer les usages acceptables ou non.

A l'ère des technologies de surveillance, où les scénarios dystopiques prennent forme dans l'espace public, l'actualité place la reconnaissance faciale au cœur des débats. Le déploiement accéléré de cette technologie constitue un phénomène authentiquement global. Plébiscitée par les régimes libéraux comme autocratiques, de Londres à Pékin, la reconnaissance faciale est progressivement érigée en outil incontournable de l'arsenal sécuritaire. Elle suscite également l'intérêt croissant du secteur privé : identification des personnes condamnées pour vol dans les commerces, identification des mineurs pour la vente d'alcool ou la consultation de sites pornographiques, contrôle à l'entrée des casinos… Autant d'expérimentations qui dessinent les contours des modèles de consommation de demain.

La France n'échappe pas au phénomène. Alors que la ville de Nice, très motivée en ce domaine, a testé un système de reconnaissance faciale en février 2019 à l'occasion de son carnaval, le gouvernement prévoit de faire reposer sur la reconnaissance faciale l'accès au système Alicem (Authentification en ligne certifiée sur mobile). Ce système doit permettre à tout citoyen de se connecter aux services publics en prouvant de manière sécurisée son identité à partir d'un smartphone. Le secrétaire d'Etat chargé du numérique, Cédric O, encourage en outre les expérimentations, dans un contexte où l'industrie européenne est fortement concurrencée par les géants sino-américains.

L'introduction de ces dispositifs n'emporte toutefois pas le plein assentiment de la société civile. Celle-ci y entrevoit, tour à tour, le spectre du Léviathan technocratique ou du Big Brother que constituent les géants mondiaux du numérique. La multiplication des usages liberticides au-delà de nos frontières alimente déjà un bilan à charge : répression de la minorité des Ouïgours en Chine, arrestation de manifestants à Hongkong, traque de militants palestiniens en Cisjordanie sont autant d'exemples d'usages de la reconnaissance faciale fermement condamnés par les associations de défense des droits de l'homme. Dans l'Hexagone, le dispositif Alicem a donné lieu à l'introduction d'un recours devant le Conseil d'Etat, et les expérimentations conduites dans les lycées de la région Sud (Provence-Alpes-Côte d'Azur) ont été désavouées par la Commission nationale informatique et libertés (CNIL).

A pluralité des usages, pluralité des effets

Dans une société démocratique, l'interdiction de la surveillance de masse doit demeurer le principe. La généralisation de l'outil de reconnaissance faciale à des fins de surveillance serait manifestement attentatoire aux libertés et disproportionnée au regard de l'objectif de maintien de l'ordre public. Rappelons qu'un tel dispositif repose sur la captation continue de milliers de visages, sans le consentement des individus et en dehors de toute procédure les mettant en cause. La CNIL rappelle en ce sens que *« 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 »*.

Les usages de cette technologie ne font pas, à ce jour, l'objet d'une législation idoine. Le Règlement général sur la protection des données comme la directive européenne « Police Justice » interdisent le traitement des données biométriques aux fins d'identification, sauf exception circonstanciée, fondée sur la nécessité publique. Ces exceptions doivent être strictement encadrées et prévoir les mesures appropriées et spécifiques à la sauvegarde des droits fondamentaux.

Si, en France, les textes requièrent l'adoption d'un décret en Conseil d'Etat, le pluralisme des intérêts qui s'expriment et le choix de société que l'adoption de ces dispositifs implique appellent à notre sens une intervention du législateur et un large débat public. Celui-ci permettrait de distinguer les usages « acceptables » au regard de nos valeurs démocratiques, et ceux qui doivent être résolument bannis, à l'instar du fichage des migrants ou de l'identification de suspects dans les délits mineurs. A pluralité des usages, pluralité des effets.

Repenser notre rapport à l'objet technique

Les appels en faveur de moratoires se multiplient déjà outre-Atlantique au sein de la communauté universitaire. Plusieurs propositions de loi ont parallèlement été introduites, en Grande-Bretagne et dans divers Etats américains, pour engager une telle démarche. En France, le secrétaire d'Etat chargé du numérique plaidait, en octobre 2019, en faveur d'expérimentations *« pour que nos industriels progressent »*. Il proposait la création d'une instance de supervision de ces expérimentations, mais n'envisageait que *« dans un deuxième temps »* l'ouverture d'un *« débat citoyen »* sur *« l'équilibre entre usages, protection et libertés »,*position réaffirmée à l'occasion d'un entretien au *Parisien,* le 24 décembre.

Contestable dans la méthode – comment faire l'économie d'un débat dans un Etat de droit ? –, la position de Cédric O fait fi de l'acceptabilité sociale de ces dispositifs, qui rencontrent des résistances nombreuses. Elle se heurte également à « l'effet cliquet » technologique qui menace nos administrations : comment justifier le démantèlement a posteriori de dispositifs coûteux qui ne donneraient pas satisfaction ?

Ce chantier invite plus fondamentalement à repenser notre rapport à l'objet technique. La présomption d'efficacité et de neutralité, dont bénéficie souvent la technologie dans le discours de nos responsables, en occulte les lacunes : erreurs, biais et failles de sécurité obèrent encore son fonctionnement vertueux. Nous plaidons aussi pour une « méfiance institutionnalisée », qui opposerait au secret des affaires une obligation d'audit et envisagerait le standard technique sous l'angle des droits fondamentaux. L'encadrement des technologies de surveillance en général, de la reconnaissance faciale en particulier, s'impose aussi comme une condition et une urgence de la démocratie « technologique ».

Caroline Lequesne Roth (Maître de conférences en droit public à l'université Côte d'Azur, cofondatrice du projet de recherche « Deep Law for Technologies » et responsable du Master 2 Droit algorithmique et gouvernance des données)

« Pour une reconnaissance faciale éthique »

Didier Bachère

Député (LRM) des Yvelines

Stéphane Séjourné

Député européen (Renew Europe)

Oui, cette techniologie représente des opportunités commerciales multiples, mais il est nécessaire d'entamer une réflexion sur les modalités de son utilisation, estiment les députés Didier Baichère et Stéphane Séjourné, dans une tribune au « Monde ».

Publié le 24 octobre 2019 à 06h00

Tribune. Si la reconnaissance faciale appartenait hier aux films de science-fiction, elle est aujourd'hui une dimension méconnue de la compétition géopolitique et industrielle mondiale. Or la souveraineté européenne dépend des efforts que nous déployons pour garantir notre indépendance en matière de technologies hautement stratégiques. Le risque de décrochage, s'agissant de l'intelligence artificielle en général et de la reconnaissance faciale en particulier, confronte l'Europe à un triple défi : un défi d'innovation technologique et industrielle, un défi d'appropriation citoyenne et un défi de régulation juridique.

Terre technologique et puissance de marché, l'Union européenne sait imposer au reste du monde ses valeurs. En témoigne l'influence internationale du règlement général sur la protection des données (RGPD), conçu contre l'utilisation inopinée de nos données personnelles. Alors que les géants du numérique américains et chinois développent de gigantesques bases de données au détriment de la vie privée de leurs citoyens, il est temps pour l'Europe d'établir des standards exigeants en matière de consentement et de créer un espace de données répondant aux besoins d'innovation du secteur public et de nos entreprises.

Comme souvent, les nouveaux usages s'accompagnent de mythes et de fantasmes qui oblitèrent la possibilité d'organiser une réflexion éthique sérieuse. En tête des secteurs intéressés par la reconnaissance faciale viennent la sécurité, avec la délivrance de documents d'identité et la réalisation de contrôles, et la santé, pour laquelle elle constituerait un appui au diagnostic.

« Si nous n'y prenons garde, la reconnaissance faciale s'imposera d'elle-même, avec ses biais sur lesquels il sera bien difficile de revenir, malgré les discriminations engendrées »

La technologie représente également des opportunités commerciales multiples que le législateur doit anticiper. Les utilisateurs des smartphones les plus récents en font déjà usage pour déverrouiller leur appareil ou effectuer des paiements. Certaines entreprises voudraient également s'en servir à des fins de ciblage marketing par l'identification de l'âge et du genre de leurs clients.

L'expérimentation conduite par certaines collectivités locales montre là encore un éventail d'applications possibles : retrouver des personnes perdues ou optimiser la gestion de flux lors de grands événements. Se pose alors la question de la formation des élus sur ces sujets pointus et le risque de se voir imposer des dispositifs couplés à la vidéo protection déjà largement répandue.

Si nous n'y prenons garde, la reconnaissance faciale s'imposera d'elle-même, avec ses biais sur lesquels il sera bien difficile de revenir, malgré les discriminations engendrées, alors même que cette technologie n'est pas entièrement fiable sur le plan technique. Son efficacité diffère selon les conditions d'utilisation mais également selon les populations (sexe, ethnie…).

Une consultation citoyenne

Entre rejet en bloc de la reconnaissance faciale et usage débridé, il y a un chemin à définir dont la responsabilité incombe à la puissance publique. En Europe, la France pourrait se positionner en exemple pour développer une reconnaissance faciale éthique bénéficiant à tous sans créer de nouvelles inégalités, sans empiéter sur nos libertés publiques, sans poser de nouveaux risques sur notre sécurité individuelle et collective. Pour cela, organisons une consultation citoyenne qui s'appuierait sur le travail engagé par le Forum économique mondial et le Conseil national du numérique (CNNum). Nous fixerions nos priorités, nos limites, et réaffirmerions la responsabilité de l'ensemble des acteurs scientifiques, industriels et politiques. La création d'un comité d'éthique, tel qu'envisagé par le secrétaire d'Etat au numérique Cédric O, permettrait de piloter le débat et de répondre aux préoccupations exprimées en coordination avec la Commission nationale de l'information et des libertés (CNIL). A l'issue de cette première phase, une loi d'expérimentation au niveau national participerait à la réflexion entamée au niveau européen sur les implications éthiques de l'intelligence artificielle et contribuerait à façonner un cadre assurant la souveraineté industrielle de l'Union dans le respect de ses valeurs.

Didier Baichère est député (LRM) des Yvelines, vice-président de l'Office parlementaire d'évaluation des choix scientifiques et technologiques. Stéphane Séjourné est député européen (Renew Europe), président de la délégation française Renaissance au Parlement européen.
Didier Bachère (Député (LRM) des Yvelines) et **Stéphane Séjourné** (Député européen (Renew Europe))