THE CONVERSATION

L'expertise universitaire, l'exigence journalistique

Comment marche la reconnaissance faciale? En fonction de la réponse, les risques de surveillance varient beaucoup. Jan Canty, Unsplash, CC BY

La reconnaissance faciale, du déverrouillage de téléphone à la surveillance de masse

Publié: 10 juin 2022, 18:48 CEST

Elia Verdon

Doctorante en droit public et en informatique, CERCCLE (EA 7436) et LaBRI (UMR 5800), Université de Bordeaux

Les évènements intervenus au Stade de France dans le contexte de la finale de la Ligue des Champions en 2022 ont servi d'argument pour renouveler les discours prônant l'utilisation de la reconnaissance faciale pour la sécurisation de grands évènements, comme les Jeux olympiques ou la Coupe du Monde de rugby à venir en France.

Cette promotion de la reconnaissance faciale fait écho au dernier rapport du Sénat proposant le recours, à titre expérimental, à la reconnaissance « biométrique sur la voie publique en temps réel [...] à des fins de sécurisation des grands évènements ».

Ces propositions d'expérimentations soulèvent des risques d'accoutumance des populations, facilitant par la suite une pérennisation de cette technologie, qualifiée par le professeur de droit et d'informatique Woodrow Hartzog de « mécanisme de surveillance le plus dangereux qui ait été inventé ». Les risques en matière de surveillance des individus et de protection des libertés induits par la reconnaissance faciale sont assurément importants.

Identification et authentification, deux finalités aux enjeux bien différents

L'identification biométrique vise à retrouver un individu au sein d'un ensemble de personnes, au moyen de sa biométrie (par exemple son visage). On compare alors le visage de la personne recherchée à tous les autres visages inscrits dans une base de données constituée au préalable. Cet usage peut s'effectuer en temps réel, ou bien_ a posteriori_ sur des séquences d'images enregistrées.

A contrario, l'authentification vérifie qu'une personne est bien celle qu'elle prétend être. Pour cela, on compare en temps réel sa biométrie préalablement enregistrée – et seulement celle-ci – avec les caractéristiques biométriques de la personne. C'est le cas par exemple pour déverrouiller certains smartphones ou encore pour le contrôle aux frontières via le système PARAFE (où les données de la personne ont été préenregistrées dans une puce au sein du passeport lors de sa fabrication).

Ces deux finalités, authentification et identification, n'impliquent pas le même degré de surveillance des individus : l'identification des individus par un système de reconnaissance faciale, notamment sur la voie publique, a des potentialités de surveillance bien plus importantes que l'authentification, qui s'effectue pour accéder à un lieu précis.

Quelle surveillance l'identification faciale rend-elle possible ?

L'identification rend nécessaire la constitution d'une base de données centralisant les « gabarits », c'est-à-dire des modèles informatiques quantifiant les caractéristiques essentielles des visages préenregistrés : positions et tailles relatives des yeux, menton, bouche, etc. En France, l'identification faciale est permise depuis 2012 à des fins d'enquête judiciaire par les services de police dans la recherche d'auteurs d'infraction : les visages de personnes suspectées d'infraction peuvent être comparés aux visages inscrits dans le fichier du « traitement des antécédents judiciaires », ou « TAJ ».

À lire aussi : « Fichés S » et autres fichiers de police : de quoi parle-t-on vraiment ?

La centralisation des visages au sein d'une base de données soulève des risques de surveillance, car le couplage de ces données faciales avec des caméras de surveillance ou des drones est susceptible de permettre la mise en place d'un système de reconnaissance faciale à distance, en temps réel, dans l'espace public, et à l'insu des individus.

Cette technologie est particulièrement individualisante, au regard de la distinction qu'elle peut faire entre les individus au moyen de leurs caractéristiques faciales. Étant donné qu'il est interdit de dissimuler son visage dans l'espace public, le déploiement de caméras de surveillance à reconnaissance faciale automatique entraînerait le suivi continu et généralisé des populations. L'individu serait alors privé de son droit à la vie privée et à l'anonymat, tous deux des droits fondamentaux primordiaux en démocratie.

Bien que la reconnaissance faciale en temps réel dans l'espace public ne soit pas aujourd'hui autorisée en France, les diverses tentatives et expérimentations passées et à venir imposent de comprendre les risques de cette technologie. Si l'identification des individus par un système de reconnaissance faciale peut sembler louable pour des raisons de sécurité publique ou de résolution d'enquêtes, cela est plus discutable au regard de la généralisation de la surveillance faciale des individus.

Le choix d'une reconnaissance faciale protectrice

A contrario, l'utilisation de la reconnaissance faciale à des fins d'authentification d'un individu conduit à un degré de surveillance moindre, car il est alors possible de ne pas centraliser les visages au sein d'une base de données. En effet, l'authentification peut être effectuée en comparant le visage photographié en temps réel au gabarit du visage préalablement enregistré, soit dans un support physique (son passeport, sa carte d'identité, son téléphone, etc.), soit dans une base de données.

Système automatisé de contrôle des passeports à l'aéroport Charles de Gaulle, en 2016.
0x010C/Wikipedia, CC BY-SA

Utiliser une base de données centralisée pour l'authentification induit les mêmes enjeux que l'identification. En revanche, si le gabarit est inscrit au sein d'un support physique, il sera plus aisé d'écarter les risques d'une société de surveillance en redonnant à l'individu le contrôle sur sa biométrie (on parle alors de « biométrie à la main de l'usager »).

Légiférer pour mieux protéger les libertés

Au vu des risques de surveillance que fait peser cette technologie, il semble nécessaire de ne pas éroder nos libertés. Si le rapport du Sénat se veut force de propositions en la matière, il est parfois ambigu. En effet, il propose d'interdire « l'utilisation de la reconnaissance biométrique à distance en temps réel dans l'espace public », tout en posant directement des exceptions à ce principe (proposition 22).

Par ailleurs, dans un souci de préservation des libertés, il aurait pu préciser, voire imposer, l'authentification biométrique à la main de l'usager, lorsqu'il évoque l'utilisation de l'authentification biométrique à des fins de fluidification des flux de certains évènements (proposition 16).

Enfin, une interdiction de l'utilisation de la reconnaissance faciale dans l'espace public, comme à San Francisco, permettrait d'amoindrir les risques d'une société de surveillance. Le rapport du Sénat propose à plusieurs reprises des expérimentations (propositions 7, 14 et 22). Or, les expérimentations ont tendance à se généraliser. Tel fut le cas de PARAFE : il s'agissait à l'origine d'une expérimentation visant le passage rapide aux frontières extérieures par reconnaissance automatisée des empreintes digitales. Ce système a par la suite été pérennisé et s'est vu doter de nouvelles capacités d'authentification par reconnaissance faciale. Ces expérimentations, motivées par des arguments de praticité (fluidifier les accès et améliorer l'« expérience utilisateur »), entraînent des risques d'accoutumance et qui ne sont pas sans risque pour les libertés. Une légère facilité du quotidien permise par cette technologie vaut-elle le prix de nos libertés fondamentales (droit à la vie privée, liberté d'aller et venir anonymement, etc.) ?