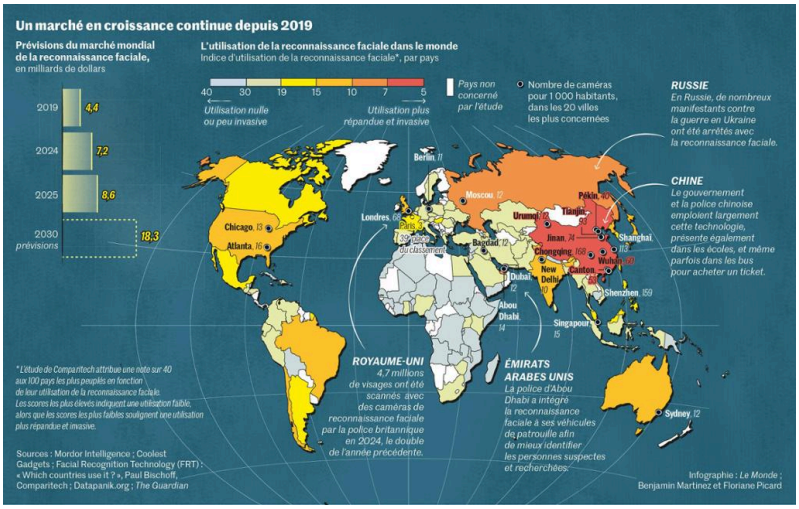
L'essor discret de la reconnaissance faciale



Marjorie Cessac

Portée par l'IA, cette technologie hautement sensible gagne du terrain en Europe et se banalise dans le monde

Entre le moment où vous arrivez à l'aéroport et celui où vous passez dans la salle d'embarquement, il ne se passe que dix minutes à peine. » Vincent Bouatou détaille la rapidité avec laquelle il est possible de prendre un avion à Singapour, sans exhiber de passeport ni de carte d'embarquement. Une facilité permise, selon le directeur de la technologie du groupe français Idemia Public Security, par la biométrie de l'iris et la reconnaissance faciale. *« Ce qu'ils ont fait à Changi est inégalé dans le monde »*, estime-t-il.

Cela se passe à Singapour, mais aussi en Chine, dans les pays du Golfe, aux Etats-Unis… Qu'il s'agisse d'aéroports, de transport, de contrôle aux frontières, d'affaires criminelles et bien plus encore, au fil des années, la reconnaissance faciale n'a cessé de se banaliser dans le monde. En témoignent les perspectives de ce marché qui pourrait peser 18 milliards de dollars (15,4 milliards d'euros) en 2030 contre 8 miliards aujourd'hui, selon plusieurs cabinets de conseil.

Côté pile, scanner un visage peut se faire à la volée, de manière plus fluide et pratique qu'un recueil d'empreintes digitales ou que l'encodage d'un iris. Mais côté face, c'est aussi la biométrie *« la plus hautement sensible »*, comme le rappelle la CNIL, l'autorité française de la protection de la vie privée. *« Si on vole votre Carte bleue, la banque peut vous redonner un code. Si vous vous faites pirater votre identité biométrique, vous ne pouvez pas changer de visage »*, insiste Thomas Dautieu, directeur de l'accompagnement juridique.

Sans compter qu'un faciès peut aisément être suivi dans l'espace public. A l'extrême, cette surveillance s'incarne dans le système de contrôle social des citoyens chinois, où la reconnaissance faciale est massivement utilisée dans les rues. Mais elle gagne aussi, de manière plus rampante, les pays occidentaux, comme le Royaume-Uni, où elle se développe à la sortie des boîtes de nuit ou dans les supermarchés.

Dans ce domaine, l'Union européenne (UE) oppose encore une certaine résistance. Elle s'est dotée de plusieurs garde-fous, comme le règlement général de protection des données (RGPD) et, depuis 2024, d'un règlement baptisé « AI Act ». Pour autant, *« les contextes de sécurité nationale ou de contrôle aux frontières font l'objet d'exceptions »*, souligne Katia Roux, chargée de plaidoyer chez Amnesty International France.

« Effet de contagion possible »

Des dérives sont possibles suivant l'usage que l'on décide de faire de ces technologies. En Hongrie, le recours à la reconnaissance faciale a été autorisé par le Parlement en mars pour identifier les personnes qui organisent ou assistent à la Marche des fiertés, désormais interdite par la loi. *« L'AI Act encadre partiellement la reconnaissance faciale en temps réel, mais on voit bien que son usage peut être aussi problématique a posteriori, quand des manifestants sont arrêtés plusieurs jours après. C'est ce qui s'est passé en Russie en 2021 »*, ajoute Katia Roux.

A mi-chemin entre le régalien et le domaine privé, les aéroports sont en Europe l'un des rares lieux où elle est à ce jour autorisée. Du moins lors des contrôles d'identité aux frontières. Contrairement à d'autres régions du monde, son usage y est cependant restreint. En 2024, le comité européen de la protection des données a pointé le fait que dans un tel dispositif, les données biométriques ne devaient pas être centralisées. *« L'utilisation abusive de ce système peut avoir de graves conséquences telles que la fraude ou l'usurpation d'identité »*, a alerté Anu Talus, la présidente du comité, précisant que les passagers doivent *« garder un contrôle maximal sur leurs données »*. Au risque sinon, selon elle, de faux négatifs et de discrimination. A ce titre, les pays qui avaient entamé des tests les ont arrêtés, mais cela ne pourrait être que partie remise. *« Nous essayons de proposer des solutions techniques qui protègent les données, y compris en cas de fuite »*, rétorque Vincent Bouatou chez Idemia, jugeant la législation européenne *« trop stricte »*. Des arguments auxquels la Commission n'est pas insensible.

En octobre 2024, cette dernière a proposé la création d'une *« application de voyage digitale »* au sein de l'UE afin que les passagers puissent stocker sur leur mobile les informations de leur passeport ou de leur carte d'identité et une image faciale. *« Cela nous inquiète »*, insiste Ella Jakubowska, responsable des politiques au sein du réseau European Digital Rights, qui fédère des associations de défense des droits numériques : *« Cette proposition implique la création de 27 nouvelles bases de données biométriques contenant les données faciales de potentiellement tous les voyageurs, ainsi qu'une forme inédite de traitement de données sensibles aux frontières européennes »*, ajoute-t-elle.

La généralisation de ces outils requiert l'attention. *« Il y a un effet de contagion possible*, concède Thomas Dautieu. *Plus on admet de cas de reconnaissance faciale, plus on est tenté de développer de nouveaux usages. »* Des champs d'application inédits sont envisagés. *« La vérification d'identité pourrait s'étendre aux gares ferroviaires, routières ou maritimes, où il existe aussi un enjeu de sécurité publique*, explique Benoît Jouffrey, directeur technique pour la cybersécurité et l'identité numérique chez Thales. *Ce sont des sujets sur lesquels nous travaillons. »*

La France n'est pas en reste. Les annonces de Gérald Darmanin ne laissent guère de doute à ce sujet. Le 23 mai, le garde des sceaux a annoncé le lancement d'un *« groupe de travail »* sur la reconnaissance faciale, qu'il souhaite mettre en place dans l'espace public et les aéroports. L'objectif étant de *« créer un cadre légal »* permettant d'*« introduire cette mesure dans notre législation »*, alors qu'il est interdit d'identifier et de suivre quelqu'un en direct. Sur son compte X, le 5 mai, l'ancien ministre de l'intérieur avait déjà indiqué qu'à son sens la reconnaissance faciale constituait une solution *« pour lutter drastiquement contre l'insécurité »* et que, *« malheureusement, le Parlement s'y [était] toujours opposé jusqu'à présent »*.

Des digues sautent. *« Considérée naguère comme une ligne rouge, la reconnaissance faciale est assumée par des membres du gouvernement alors que les risques sont documentés »*, déplore Katia Roux. Preuve en est, lors des Jeux olympiques (JO) et paralympiques de Paris, seule la vidéosurveillance algorithmique (VSA) avait été autorisée. L'expérimentation a permis le recours à des logiciels qui automatisent le visionnage d'images collectées au moyen de caméras ou de drones, et lancent des alertes en cas de situations *« suspectes »*. Mais elle s'est achevée en mars.

Depuis, le gouvernement fait du zèle pour la prolonger. Après avoir déposé un amendement visant à étendre le dispositif jusqu'en 2027, que le Conseil constitutionnel a censuré en avril, l'exécutif tente de faire adopter la prorogation de l'article 10 de la loi JO 2024 jusqu'en 2027. Chose faite par le Sénat, le 24 juin, dans le projet de loi visant à faciliter les préparatifs des Jeux d'hiver 2030 dans les Alpes.

Pour l'heure, l'utilisation de la VSA reste interdite, sauf dans le cadre d'enquêtes policières, donc a posteriori, ou à des fins purement statistiques. *« La VSA n'est pas de la reconnaissance faciale, mais on peut, à bien des égards, lui porterles mêmes critiques comme de pouvoir suivre des gens dans la rue*, relève Assia Wirth, doctorante en sociologie. *Il n'y a pas que le visage qui permet de nous identifier. Nous pouvons tout aussi bien l'être par un vêtement que par notre démarche. »* Autre risque, *« le flou qui entoure la manière dont les municipalités, les forces de l'ordre et même les groupes privés utilisent ces outils »*, observe Myrtille Picaud, chercheuse au CNRS.

Coudées franches dans le privé

En novembre 2023, le média *Disclose* révélait que la police nationale avait eu recours au logiciel Video Synopsis, de BriefCam, pour traquer des personnes. *Cette société israélienne, filiale du groupe Canon, n'a pas souhaité nous répondre. « Des entreprises comme BriefCam continuent de vendre dans leur vidéosurveillance algorithmique, et ce qui se passait avant les JO se poursuit dans l'impunité la plus totale »,* pointe Noémie Levain, juriste au sein de La Quadrature du Net. En janvier, le tribunal administratif de Grenoble a donné raison à cette association de

défense des droits fondamentaux dans l'affaire qui l'opposait à la ville de Moirans (Isère), en reconnaissant l'illégalité du logiciel de BriefCam utilisé par de nombreuses communes.

De plus, ces technologies sont encore loin d'être au point. Les résultats de la VSA pendant les JO de Paris 2024 sont par exemple peu probants. Selon le rapport d'évaluation, sur 270 alertes envoyées à la SNCF par le logiciel, 62 % étaient erronées et seulement 21 ont été jugées *« pertinentes »*. *« Les entreprises disent ne pas avoir eu assez de temps pour calibrer leurs algorithmes »*, note Florent Castagnino, maître de conférences de l'Institut Mines-Télécom, en précisant qu'*« en situation réelle s'il y a beaucoup de monde, ces derniers peuvent être perturbés »*.

En attendant, les groupes sélectionnés ont pu mettre à profit les Jeux de Paris pour élargir leurs bases de données. C'est le nerf de la guerre. *« Si on veut faire de l'Europe un continent IA* [intelligence artificielle]*, rivaliser avec la Chine et les Etats-Unis, il faut s'emparer de manière responsable de la question des bases de données »,* insiste Benoît Jouffrey chez Thales, estimant que l'Europe devrait réaliser *« des collectes auprès des citoyens européens sur consentement »*.

Pour se développer, les entreprises ont les coudées plus franches dans le secteur privé. Pour elles, *« promouvoir des applications qui permettent de réaliser de l'authentification d'identité pour ne pas se faire hacker son compte bancaire ou sa ligne de téléphone est plus simple, car moins contesté »*, note Assia Wirth. D'autant que ces activités permettent de financer leurs innovations et d'entraîner leurs algorithmes. *« Il y a plus de demandes du côté des entreprises, et nous pouvons remonter les alertes en temps réel aux opérateurs de sécurité »*, confirme Alan Ferbach, président de Videtics, une start-up spécialisée dans l'analyse vidéo par l'IA. La société compte dans sa clientèle *« des industriels, comme Veolia et Suez, qui souhaitent protéger l'accès de leurs sites, ou des centres commerciaux qui veulent mieux comprendre le parcours de leurs clients »*. Auprès des collectivités, Videtics se bornerait en revanche à du *« comptage de personnes, voitures ou bateaux »*, ce qui constitue déjà, selon des ONG, un *« doigt dans l'engrenage »*.

Promue au nom de la sécurité, et de la facilité, la reconnaissance faciale progresse au sein des agences d'intérim ou des chauffeurs Uber, qui revendiquent le besoin de lutter contre l'usurpation d'identité. A la lisière de l'illégalité, elle s'invite à bas bruit dans des logiciels de recrutement pour mesurer les émotions. Et se banalise à travers des gestes du quotidien en déverrouillant son smartphone. Une manière discrète de faciliter son acceptabilité sociale.