La vérité sur...

les failles de la biométrie faciale

Vols d'identité, surveillance de masse... les logiciels de reconnaissance de visages comportent de vrais risques. Pourtant, ils se généralisent sans cadre précis.

Pour retrouver les assaillants du Capitole, à Washington, le FBI a dégainé une arme redoutable : le logiciel Clearview. Soutenue financièrement par Peter Thiel, cette start-up créée par Hoan Ton-That – un ex-mannequin australien d'origine vietnamienne – a développé une application permettant d'identifier n'importe qui à l'aide d'un simple cliché. Les 600 services de police américains qui l'utilisent sont déjà accros : le logiciel retrouve des suspects ne figurant dans aucune base de données. Mais cet exploit a été accompli en franchissant une ligne jaune que même Google ou Facebook n'avaient encore jamais osé passer : Clearview a collecté illicitement plus de 3 milliards de photos sur les réseaux sociaux, dont LinkedIn et Instagram.

Clé vulnérable

L'intrusion ne concerne pas que les Américains : Clearview aurait fiché également des millions de citoyens de l'Union européenne. « *Après mes demandes réitérées, Clearview a reconnu posséder trois photos de moi, sans aucune base légale* », raconte Zoé Vilain, avocate en protection des données. Elle a saisi la Cnil, qui a ouvert une enquête, emboîtant le pas à l'Australie et au Royaume-Uni. L'affaire résume toute l'ambivalence de la reconnaissance faciale : un outil séduisant mais à manier avec d'extrêmes précautions.

« *Pour bien comprendre les enjeux, il faut commencer par distinguer entre ses deux grands types d'usages : l'authentification et l'identification* », rappelle Benoît Jouffrey, directeur technique des activités identité et sécurité numériques de Thales. La première consiste à scanner un visage pour s'assurer qu'une personne est bien celle qu'elle prétend être. L'outil fonctionne alors comme une clé d'accès. Ainsi, quand un voyageur passe par le portique Parafe d'un aéroport, un logiciel compare la photo stockée dans la puce de son passeport biométrique avec son visage. Un usage bien différent de l'identification, qui vise à reconnaître une personne dans une foule, en rapprochant son visage d'une base de données d'images.

L'authentification est rentrée dans les mœurs : ouvrir son smartphone avec son visage est devenu banal. Pour autant, cette clé n'a rien d'inviolable. « *Une course technologique oppose les fabricants aux hackers*, explique Marc Norlain, fondateur d'Ariadnext, société spécialisée dans l'identification à distance de documents. *Comme il ne suffit plus de présenter une photo statique volée pour déjouer une reconnaissance faciale, les faussaires fabriquent des* deep fakes, *des vidéos fictives, pour commettre ces attaques dites par présentation.* »

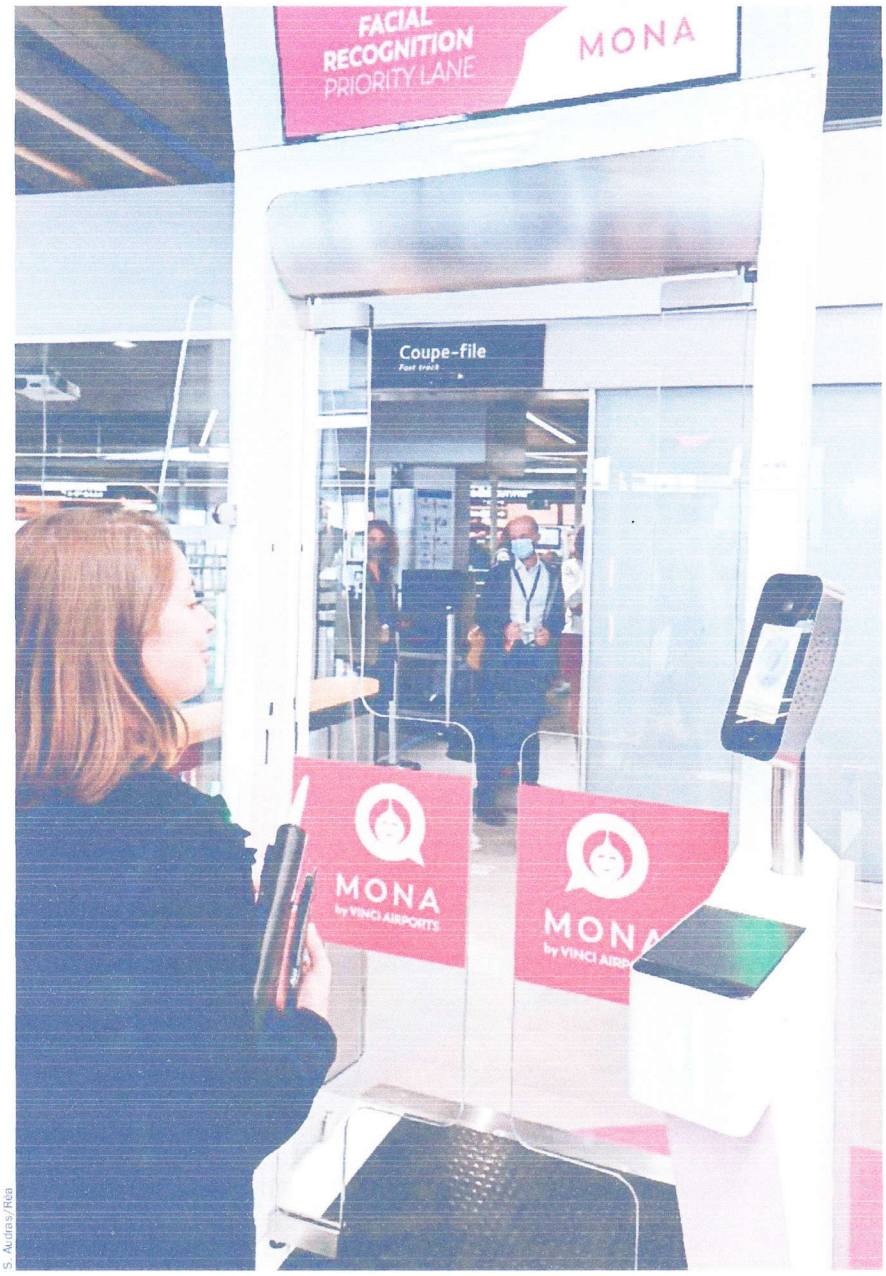
Erreurs judiciaires

Pierre Pozzi, cofondateur d'Aerendir renchérit : « *Si un hacker réussit à s'emparer des 35 000 points composant votre visage et le revend sur le darkweb, il vous sera quasi impossible de récupérer votre identité numérique.* » L'entrepreneur s'est associé au physicien Martin Zizi pour lancer la technologie NeuroPrint, qui capte l'empreinte neurophysiologique – la « signature » du cerveau – propre à chacun. Une clé infalsifiable, qui ne contient aucune donnée sensible et reste associée localement à un smartphone. Pas comme la reconnaissance faciale, qui fait transiter les images vers des clouds. Avec le risque d'un vol massif de profils biométriques.

Les craintes se focalisent sur l'authentification. D'abord, parce qu'on peut tromper un système de reconnaissance faciale. Mis au point par des chercheurs de l'université de Chicago, le logiciel Fawkes, sorte de brouilleur, rend par exemple les photos illisibles par une IA. Plus grave, elle est faillible et sujette à des biais. Entraînés sur des visages blancs, les algorithmes sont moins performants pour reconnaître les visages noirs. Jeté en prison pen-

En Chine, un outil ciblant les Ouïgours

Dans un pays où les caméras sont omniprésentes, les Ouïgours font l'objet d'une surveillance particulière, avec la complicité des industriels. Le 17 décembre, un rapport du cabinet de recherche IPVM a révélé que le géant Alibaba disposait d'un logiciel de reconnaissance faciale permettant de repérer spécifiquement les Ouïgours. Les archives du logiciel montrent qu'il peut détecter le caractère ethnique du sujet, et plus précisément s'il est issu de cette minorité musulmane. Une semaine plus tôt, c'est Huawei qui avait été mis en cause. Toujours selon IPVM, l'industriel aurait testé un logiciel capable d'alerter automatiquement la police quand ses caméras repèrent des visages ouïgours. Alibaba et Huawei assurent qu'il ne s'agit que d'expérimentations. Alors que la Chine mène une politique « d'assimilation culturelle », notamment en incitant à des mariages interethniques, voilà de quoi enrichir le dossier noir de la reconnaissance faciale.



S. Audras/Réa

dant dix jours, Nijeers Parks est le troisième Américain à avoir été accusé de crimes qu'il n'a pas commis, parce que sa photo a été associée à tort à une autre. D'où le recul spectaculaire de plusieurs géants du numérique. En juin, IBM a annoncé qu'il cessait de vendre des outils de reconnaissance faciale. Il a été suivi par Amazon et Microsoft.

Ces faiblesses techniques masquent un problème bien plus vertigineux : le risque d'un glissement vers une surveillance en continu de l'espace public. Les expérimentations se multiplient partout dans le monde, la Chine ayant poussé à l'extrême la surveillance de ses populations. En France, il a été question d'installer des caméras pour contrôler l'accès à deux écoles, à Nice. Un projet retoqué par la Cnil. « *La finalité du projet, donner simplement accès à une école, ne justifiait pas l'usage d'une technologie aussi intrusive* », explique Thomas Dautieu, responsable de la conformité au sein de l'autorité. En revanche, le Code de procédure pénale autorise la police à utiliser la reconnaissance faciale pour le fichier TAJ (traitement des antécédents judiciaires), qui contient 19 millions de fiches et 9 millions de photos. Une décision attaquée devant le Conseil d'Etat par La Quadrature du Net.

Système de reconnaissance faciale Mona, à l'aéroport de Lyon. Ce type d'authentification est entré dans les mœurs, mais les données biométriques peuvent être volées.

Face à la menace terroriste et à l'approche des jeux Olympiques, la tentation est grande pour les pouvoirs publics d'aller plus loin. « *Quand le secrétaire d'Etat au Numérique Cédric O entend accélérer les expérimentations, il déplace le sujet vers la compétition technologique* », s'inquiète Emmanuel Netter, professeur à l'université d'Avignon, qui pointe un effet cliquet : « *Les dispositifs de surveillance de la voie publique risquent de suivre le même chemin que le fichier génomique, qui s'est considérablement élargi au fil des années.* » Dans son rôle de vigie, la Cnil a bien conscience des dérives et du risque d'accoutumance. « *Nous soulignons le caractère très particulier de la reconnaissance faciale et appelons à une prise de conscience politique, éthique, juridique et sociétale* », martèle Thomas Dautieu.

Mobilisation européenne

La Commission européenne doit préciser, en mars, le cadre légal, encore flou. « *L'approche ne sera pas basée sur les seuls intérêts des Etats membres ou sur des considérations économiques, mais aussi sur les droits humains* », assure un porte-parole. Les ONG comptent mobiliser les citoyens. Fédérant plusieurs défenseurs des libertés civiles, dont La Quadrature du Net en France, l'association EDRi (European Digital Rights) a lancé en novembre la campagne *Reclaim Your Face*. L'ONG bruxelloise espère récolter 1 million de signatures nécessaires à son initiative citoyenne européenne (ICE), explique Ella Jakubowska, responsable de la campagne. Objectif ? Obtenir une loi qui « *interdise un usage arbitraire ou sans discernement des données biométriques, conduisant à de la surveillance de masse* ». De quoi empêcher un scénario à la *Black Mirror*.

Delphine Déchaux