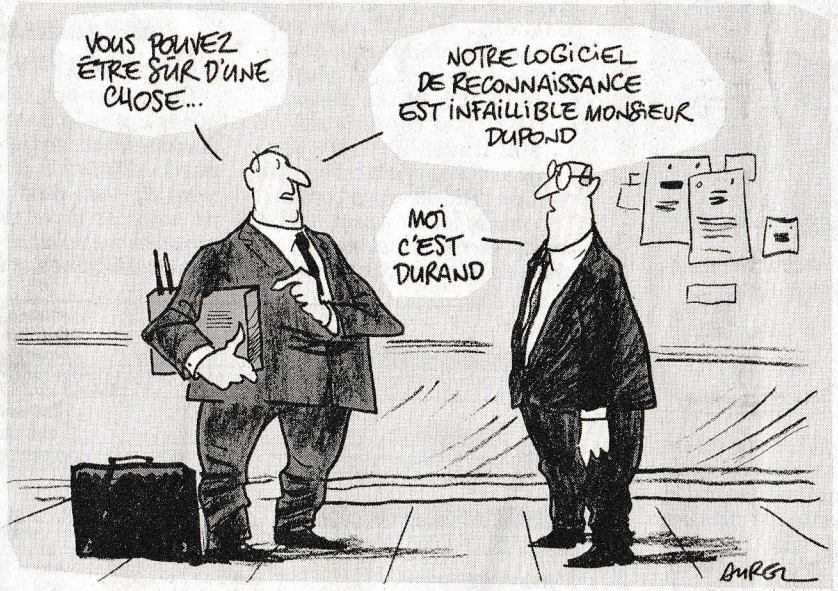
Mieux que les grandes oreilles, ces gros yeux qui nous espionnent...

Reconnaissance faciale, ciblage des ennemis, mesure des mouvements de hanche, le flicage biométrique envahit l'espace. De quoi s'inquiéter. Et parfois, heureusement, rigoler...

LA SURVEILLANCE et le flicage des citoyens ? Le débat sur StopCovid et le traçage des malades l'ont montré : dans ce domaine, les entreprises débordent d'imagination ! Exemple en or, la biométrie, qui permet l'identification – et le fichage – des quidams à partir de caractéristiques physiques.

Parmi les usages les plus sympas de cette technologie : l'espionnage des populations grâce aux caméras à reconnaissance faciale (la Chine en utilise 600 millions) et... le meurtre ciblé. Selon le GAO, l'équivalent américain de la Cour des comptes, 1 700 personnes ont ainsi été arrêtées ou tuées par l'armée US entre 2008 et 2017.

Fiables à 100 %, ces charmantes méthodes ? Pas vraiment. Comme le montrent les exemples ci-dessous, les grosses bavures ne sont pas rares.

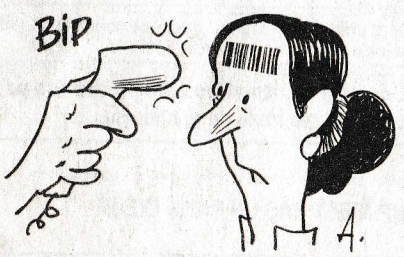


Pas loin du cœur, pas loin des yeux...

Selon la revue du Massachusetts Institute of Technology (MIT), la reconnaissance du rythme cardiaque développée par le Pentagone permet, grâce à un laser mesurant les battements du cœur à la surface de la peau, d'identifier une personne à 200 mètres !

Génial, à condition que le sujet y mette du sien : qu'il reste immobile au moins trente secondes, ne porte pas de vêtements trop épais et reste calme. « *Son état émotionnel peut influer sur le résultat,* souligne l'informaticien Jean-Luc Dugelay. *Ce procédé reste confidentiel, comme la reconnaissance de l'odeur du corps.* »

Dommage...



Y a pas à tortiller !

L'entreprise chinoise Watrix, championne de la « reconnaissance de la démarche », vend ses services à la police de Pékin et de Shanghai. Contrairement à la prise d'empreintes, cette technique ne réclame aucune coopération du sujet, se moque des déguisements, de la pénombre et de la distance (50 mètres, contre 30 cm pour l'analyse de l'iris).

Seul hic : si la cible change de démarche, tortille des hanches ou titube, ça ne (dé)marche plus !

Veines et déveine

Elaborée par la société israélienne BioCatch, la reconnaissance à « multiples facteurs cognitifs et physiologiques » (prise en main du téléphone, façon de taper ou de faire défiler son écran) permettrait de savoir si une personne agit sous l'influence d'une autre. Sceptique, Jean-Luc Dugelay la considère plutôt comme « *une démarche de communication* ».

La reconnaissance gestuelle, qui permet de commander une pizza depuis sa voiture grâce à un signe des doigts, n'intéresse guère les espions : elle aide surtout les sourds-muets. La reconnaissance de la dynamique de frappe sur un clavier (notamment lorsque l'on tape son mot de passe) ou celle des veines de la main, qui commence à équiper des smartphones, ne sont ni très répandues ni réellement infaillibles...

L'algorithme dans la peau

Toutes ces techniques sont perfectibles. Lors des premiers tests de reconnaissance faciale de la police galloise à Cardiff, en juin 2017, le criminologue Alain Bauer rappelle que 93 % se sont révélés bidon ! Mounia Hocine, la présidente de la Société française de biométrie, cite une étude menée en décembre 2019 par le National Institute of Standards and Technology (une agence d'Etat américaine) qui comparait 189 algorithmes liés à ce procédé. Tous généraient de fausses identifications, et en quantité plus grande lorsque les sujets étaient noirs ou asiatiques !

Si cette technologie de reconnaissance faciale est censée fonctionner uniquement quand on a les yeux ouverts, des internautes ont découvert que certains smartphones (comme le Google Pixel 4) pouvaient être déverrouillés par leur propriétaire... les yeux fermés. Idéal pour qui souhaite fouiller dans le téléphone de son conjoint pendant son sommeil.

L'œil était dans l'ordi...

Encore une précision rassurante ? Lorsque ces technos comparent une identité avec celles d'une base de données, les infos sont piratables ! « *C'est extrêmement difficile techniquement de comparer des versions cryptées* », analyse l'informaticien Jean-Luc Dugelay.

Une fois « hackées », ces données peuvent être modifiées, ce qui permet toutes les manipulations. Finis les vols de portefeuille à l'arraché, et bienvenue aux détournements d'identité ou de personnalité à distance, sans traces de violence...

Jérôme Canard