VÉRITÉS À BIOMÉTRIE VARIABLE

LE 5 MARS 2012 ***JEAN MARC MANACH***

La biométrie, ça ne fonctionne pas. Ou en tout cas pas à coup sûr. À l'occasion du vote de demain à l'Assemblée nationale permettant de créer le plus gros fichier biométrique de la population française, *OWNI* a listé les faiblesses des systèmes biométriques. Et la liste est longue...

> ***"A l'exception de l'analyse de l'ADN, aucune des méthodes utilisées en matière de police scientifique et technique n'a démontré de façon rigoureuse qu'elle avait la capacité de démontrer un lien entre une trace et un individu ou une source spécifique."***

En 2009, aux États-Unis, un **rapport accablant** de l'Académie nationale des sciences jetait un pavé dans la mare de ceux qui accordent une confiance aveugle aux "*experts*" de la police technique et scientifique. Les "*experts*" savent très bien que leurs méthodes ne permettent aucunement de recueillir une "*preuve scientifique*", mais uniquement une "*présomption*".

Erreurs humaines, de calcul, de prélèvement, de conservation ou de comparaison des échantillons, biais méthodologiques ou scientifiques, les "*experts*" ont de très nombreuses raisons de se tromper… sans parler de ceux qui condamnent ainsi des innocents à **plusieurs années de prison**.

50% des victimes d'erreurs judiciaires sorties de prison par l'Innocence Project, une ONG américaine qui utilise l'empreinte génétique pour innocenter des condamnés inculpés à tort, avaient ainsi été condamnées sur la foi de témoignages et de "*preuves*" apportés par des experts de la police scientifique et technique.

Brandon Mayfield, un avocat américain de 37 ans, fut ainsi accusé d'être l'un des auteurs des attentats à la bombe qui frappèrent Madrid en 2006. Pour le FBI, son empreinte digitale correspondait "*à 100%*" à celle trouvé par la police espagnole sur un sac d'explosifs. La police espagnole répondit au FBI que, d'après ses propres analyses, l'empreinte de Mayfiled ne correspondait pas à celle du suspect, il n'en fut pas moins incarcéré, au secret,

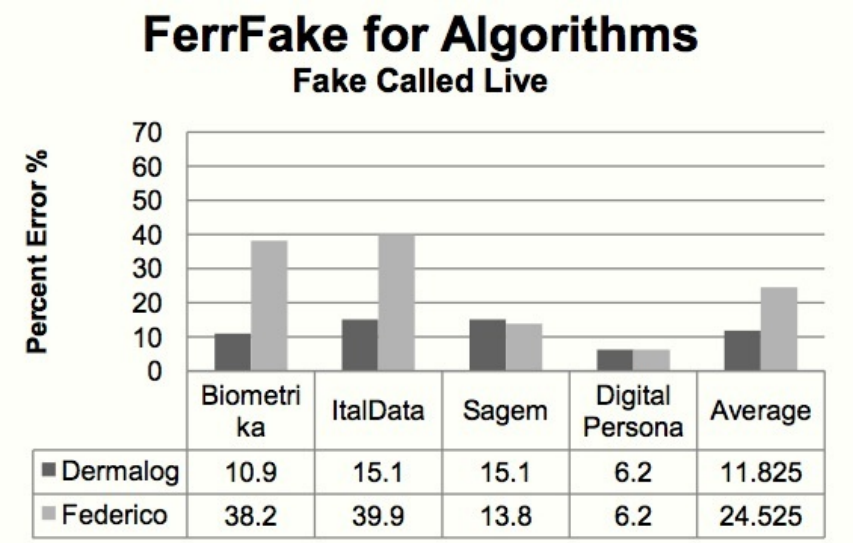
pendant deux semaines. Son empreinte faisait partie d'un groupe de 20 empreintes "*similaires*"… et Mayfield, qui s'était converti à l'islam après s'être marié à une Égyptienne, avait déjà fait l'objet de mesures de surveillance de la part du FBI. Il était donc un suspect tout désigné.

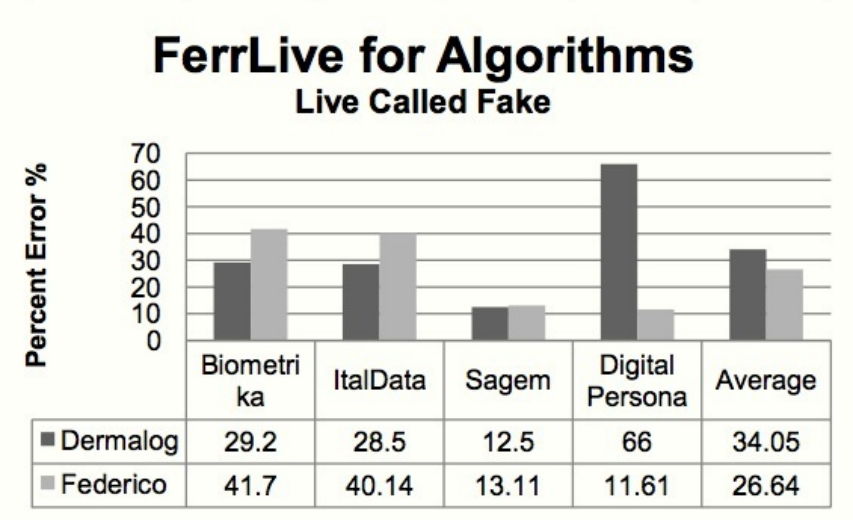
Shirley McKie, une détective de la police écossaise, fut quant à elle accusée de meurtre. Quatre experts de la police technique et scientifique avaient identifié son empreinte digitale sur la porte de la salle de bain d'une femme qui avait été poignardée à mort. Deux "*experts*" américains expliquèrent à son procès que son empreinte ne correspondait pas à celle laissée sur la scène de crime, lui évitant 8 ans de prison. Mais ses confrères britanniques maintinrent leurs versions, déclarant que c'était une "***question d'opinion***". L'autre meurtrier présumé, identifié lui aussi par ses empreintes digitales, fut libéré de prison, d'autres experts ayant eux aussi conclu à une identification erronée.

On sait d'autre part qu'il est aussi possible de tromper les systèmes de reconnaissance biométrique en leur soumettant des fausses empreintes digitales réalisées à base de pâte à modeler, de gélatine, de silicone, de latex ou encore de colle à bois.

Le Centre de recherche des technologies d'identification (**CITER**), chargé par la National Science Foundation (NSF) d'aider les industriels à évaluer et améliorer la "*crédibilité*" de leurs technologies, a ainsi initié un concours, LivDet, de reconnaissance des fausses empreintes digitales.

Les **résultats (.pdf)** de l'édition 2011 sont assez édifiants : en fonction des algorithmes, systèmes et logiciels utilisés, de 6 à 40% des fausses empreintes digitales étaient identifiées, à tort, comme véritables, et de 12 à 66% des vraies empreintes digitales étaient, tout aussi à tort, identifiées comme fausses…





Par ailleurs, plus une base de donnée biométrique est importante, plus grande est la probabilité statistique d'identifier quelqu'un par erreur ou, a contrario, de mettre de côté un individu de peur de l'identifier par erreur. Les spécialistes de la biométrie sont ainsi amenés à élaborer de très complexes algorithmes statistiques jonglant entre "*faux positifs*" et "*faux négatifs*", et basés sur un taux d'erreur acceptable.

Tel le projet du gouvernement indien de ficher ses 1,2 milliards de citoyens. Jamais on avait

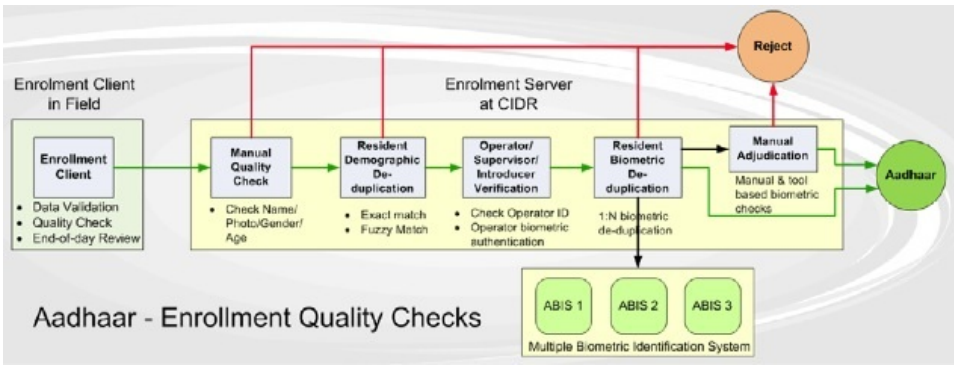
en effet cherché à procéder à une reconnaissance biométrique d'une telle ampleur.

Pour Joachim Murat, responsable pour l'Inde de Morpho, **n°1 mondial de l'empreinte digitale** et filiale de Safran, interrogé par *Les Echos*, "*la confirmation de la décision de relever les données biométriques de tous les Indiens « garantit un très gros marché pour les terminaux qui captent les iris et les empreintes digitales »*", dont son employeur est l'un des principaux fournisseurs mondiaux.

Le marché est d'autant plus juteux que Morpho qu'il faut non seulement recueillir les empreintes digitales et les numériser, mais également leur appliquer nombre de traitements pour en "*dédupliquer*" les identifiants, afin de vérifier que le nouvel inscrit n'avait pas été préalablement fiché.

Sur les 200 millions d'Indiens d'ores et déjà fichés par l'Autorité d'identification unique indienne (UIDAI), la "*déduplication*" a ainsi permis de réduire la base de données à 130 millions. Pour inciter les Indiens à venir se recenser, les autorités leur offre en effet de l'argent, voire une collation, entraînant certains à revenir s'identifier plusieurs fois…

On aurait pu espérer que ces 70 millions de doublons eussent pu être évités d'emblée, lors de la prise des identifiants, mais non : la reconnaissance par empreintes biométriques ne permet pas tant, en effet, d'identifier "*scientifiquement*", et donc à coup sûr, le porteur de telle ou telle empreinte digitale, mais d'estimer la probabilité statistique qu'il s'agisse bien de lui, ou non. Ce qui requiert tout un tas de vérifications :



L'UIDAI vient ainsi de publier **une étude très détaillée (.pdf)** expliquant comment elle est parvenue à identifier, de façon unique, 99,86% de la population, tout en précisant que 99,965% des doublons étaient identifiés comme tels.

Une **précédente étude (.pdf)**, basée sur des recherches effectuées sur 46 millions d'identifiants contenus dans la base de données du FBI, avait démontré que la prise d'empreintes de deux doigts seulement débouchait sur un taux de "*fausses acceptations*"

(False Acceptance Rate, ou FAR : personnes identifiées, à tort) de 10,3%, et de 29,2% de "*faux rejets*" (False Rejection Rate, ou FRR : personnes rejetées, à tort).

Avec 10 empreintes, le taux de faux négatifs tombait à 0, mais les faux positifs se maintenaient à 10,9%. D'où la nécessité de rajouter à ces 10 empreintes digitales celles des deux iris, seule combinaison à même de pouvoir identifier avec certitude, et sans risque de doublon ou de fausse identification, l'intégralité de la population.

Dans un ouvrage d'anthologie consacré à **l'identification biométrique**, **Bernadette Dorizzi**, spécialiste de la question, et notamment des taux d'erreurs, écrit que "*pour les systèmes d'identification (titres identitaires, vote), le FAR (les "faux positifs", NDLR) peut être défini entre 1/1 000 000 et 1/100 000 000. Le FRR (les "faux négatifs"), quant à lui, est de 1/1000 (0,1%)*", ce qui n'est pas sans incidence sur l'utilisation même du système :

> ***Un système identitaire avec une base de données d'un million d'individus recevra, pour des demandes de renouvellement et de création, environ 1 milliard de requêtes par jour (sur une vingtaine d'heures ouvrées), soit environ 14 000 mises en correspondance par seconde pour un gabarit. Si l'on considère un taux d'erreurs de 1/1 000 000, cela veut dire qu'il faudra traiter manuellement 1000 cas par jour dans le pire des cas.***

La question reste donc de savoir comment les industriels français parviendront, d'une part à identifier, de manière unique, de 45 à 60 millions de gens à partir de deux empreintes digitales seulement, mais également de parvenir à un taux d'erreur acceptable limitant autant que faire se peut "*faux positifs*" et "*faux négatifs*", et donc la probabilité statique d'entraîner des erreurs judiciaires…

Photo par **Chris John Beckett (CCbyncnd)**

YR86
le 5 mars 2012 - 17:31 • SIGNALER UN ABUS - PERMALINK

Bon article, même si l'affirmation d'ouverture est fausse, vu que l'analyse ADN est partiel (9 à 16 segments en théorie non codant analysé) elle a les même failles que les empreintes digitales.

VOUS AIMEZ 1 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

5 pings

Big Brother, Little Sister : techno pour suivre et gérer le demo | Pearltrees le 5 mars 2012 - 21:21

[...] Vérités à biométrie variable » OWNI, News, Augmented [...]

Le « vrai » visage des « gens honnêtes » | BUG BROTHER le 6 mars 2012 - 15:08

[...] fait… #oupas Demain on fiche (sur ces questions que les parlementaires ont "oublié" de discuter) Vérités à biométrie variable (sur les failles, et meme les erreurs judiciaires, imputables à la [...]

LIBERTÉ?_SÉCURITÉ!!%surveillance% | Pearltrees le 8 mars 2012 - 12:16

[...] Pour le FBI, son empreinte digitale correspondait "à 100%" à celle trouvé par la police espagnole sur un sac d'explosifs. La police espagnole répondit au FBI que,

d'après ses propres analyses, l'empreinte de Mayfiled ne correspondait pas à celle du suspect, il n'en fut pas moins incarcéré, au secret, pendant deux semaines. Son empreinte faisait partie d'un groupe de 20 empreintes "similaires"… et Mayfield, qui s'était converti à l'islam après s'être marié à une Égyptienne, avait déjà fait l'objet de mesures de surveillance de la part du FBI. Il était donc un suspect tout désigné. Shirley McKie, une détective de la police écossaise, fut quant à elle accusée de meurtre. Quatre experts de la police technique et scientifique avaient identifié son empreinte digitale sur la porte de la salle de bain d'une femme qui avait été poignardée à mort. Vérités à biométrie variable » OWNI, News, Augmented [...]

Biométrie appliquée à des libertés fondamentales oubliées… « Digital Wanderer le 26 mars 2012 - 14:39

[...] les verrous. Fiction bien loin de la réalité comme le démontre ce billet démontrant par a+b que nous sommes loin d'avoir un système fiable empêchant que des innocents soient accusés à tort de faits qu'ils n'ont pas [...]

Lila - Become an influencer le 16 mai 2012 - 14:25

[...] biométrique, qui relève plus de la probabilité statistique que de la preuve scientifique, est loin d'être aussi fiable que cela, et l'on a d'ores et déjà répertorié plusieurs cas de gens, inculpés à tort après que [...]