

Biométrie : sécurité ou menace ? - 1/2

La biométrie, sécurité ou menace ? Un peu des deux sans doute...

Depuis le 11 septembre 2001, la biométrie, cet ensemble de techniques de contrôle de l'identité comme la reconnaissance de l'iris, des empreintes digitales ou des caractéristiques du visage, est en pleine expansion. D'ici quelques années, il est vraisemblable que chaque citoyen américain possédera une carte d'identité biométrique et que le gouvernement en exigera une de tous les visiteurs étrangers. Est-ce une bonne ou une mauvaise nouvelle ? Les opposants à la biométrie parlent de Big Brother. Les responsables de la sécurité se réjouissent. Et les deux camps ont probablement raison.

Nous sommes à l'aéroport d'Amsterdam. Comme partout dans le monde, les fouilles sont fréquentes, l'attente est longue, les règles sont strictes. Pour accélérer le flot des passagers, les autorités ont installé un nouvel appareil aux douanes. Plus besoin de présenter un passeport. Notre œil suffit. Après un contrôle par un officier de police, le voyageur s'installe devant un scanner et introduit sa carte d'identité. La caméra balaie l'iris et relève plus de 250 points de références. L'appareil les transforme ensuite en une formule mathématique qui est stockée sur une carte à puce. C'est rapide, mais aussi très sûr parce que chaque iris est différent. En plus, le contrôle de l'iris est un moyen moins vulnérable que celui des empreintes digitales. Vous pouvez vous couper le doigt ou la paume de la main, alors qu'avec l'iris, c'est tout de même moins fréquent. C'est donc un système très sûr.

La reconnaissance de l'iris fait partie d'un ensemble de techniques qu'on appelle la biométrie. Chaque individu possède des caractéristiques physiques qui sont uniques et permanentes : son visage, ses yeux, ses mains et, bien sûr, ses empreintes digitales. Les appareils de biométrie servent à capter ces informations. Elles deviennent alors une référence biométrique. La preuve que vous êtes bien la personne que vous prétendez être.

A l'aéroport de San Francisco, les employés utilisent la biométrie depuis une dizaine d'années pour avoir accès aux zones réservées. L'appareil mesure les différences entre la main de l'employé et une main standard. Ces données sont ensuite cryptées et enregistrées dans un fichier qui servira ensuite de référence. Qui empêcherait alors un terroriste de couper la main d'un employé et de l'utiliser pour ouvrir une porte ? "Quand une main est coupée, le sang coule forcément. Or, le sang contribue à donner la forme et la taille à la main. Dès qu'elle est coupée, elle change directement. Donc ce n'est pas la solution pour tromper le système", rassure un employé de l'aéroport. Le terroriste devra donc contraindre l'employé vivant à mettre sa main dans le scanner s'il veut franchir la barrière de sécurité.

Pour les services de sécurité, c'est un outil de travail extraordinaire. Mais pour les simples citoyens... En effet, la biométrie doit être accompagnée d'une banque de données sur les personnes. C'est au sujet de ces banques de données qu'il faut alors se questionner. Est-ce que les libertés fondamentales et la protection des renseignements personnels seront respectées ?

La biométrie réduit le marge d'autonomie du citoyen. Et ces libertés sont très précieuses. Il ne faut donc pas renoncer à ces libertés sans se poser de questions. Il est à mon avis essentiel de comprendre le potentiel et les limites de cette technologie.

À Québec, une compagnie a remis à jour une ancienne technique : celle des empreintes digitales. Elle a conçu un appareil portatif qui reproduit les empreintes digitales en trois dimensions : le "smartprint". Il suffit

Biométrie : sécurité ou menace ? - 2/2

d'inscrire un nom, de choisir un doigt et de le placer sur le lecteur. L'appareil prend une quarantaine de mesures, qui sont ensuite inscrites sur une carte à puce. L'avantage de ce système, c'est qu'il ne retient rien en mémoire. Vous êtes le seul propriétaire de votre identité biométrique.

Le marché des empreintes digitales est en pleine expansion. D'ici deux ans, tous les Américains qui travaillent dans le secteur de la défense et du transport posséderont leur carte d'identité biométrique.

Mais comme c'est le cas avec tous les systèmes biométriques, une erreur est toujours possible. On peut tromper la biométrie parce que la biométrie est digitalisée, donc on peut l'altérer, la changer. Là, on parle de vol de votre identité biométrique. Ce serait vraiment un scénario surréaliste... Mais si on vole mon identité biométrique, j'aurai de la difficulté à rétablir mon identité comme citoyenne.

Les autorités dans les aéroports, principales intéressées par la biométrie, assurent que tout ce qu'ils désirent est d'utiliser cette technologie pour confirmer votre identité, par mesure de sécurité. Le problème est que l'utilisation d'une nouvelle technologie dépend rarement des seules intentions de ceux qui l'ont mise au point. Parfois, sur le terrain, tout devient possible...