Enjeux des techniques de biométrie - Une première approche

Meryem Marzouki
Association IRIS (Imaginons un réseau Internet solidaire).
294 rue de Charenton, 75012 Paris.
http://www.iris.sgdg.org

24 Septembre 2001

1. Introduction

Je voudrais tout d'abord remercier les organisateurs de cette conférence pour m'avoir permis de participer à ces travaux. Je voudrais surtout les remercier pour avoir organisé ce débat sur un sujet important, notamment en France, où les dangers de l'utilisation des techniques de biométrie sont encore peu perçus, contrairement à ceux de la vidéosurveillance, malgré l'existence de travaux au sein de plusieurs laboratoires de recherche publique ou de sociétés commerciales.

Dans le monde, les utilisations de techniques biométriques à grande échelle qui ont fait le plus de bruit sont celle de Newham, dans la banlieue de Londres, dès 1998, et celle du *Super Bowl* organisé à Tampa en Floride (USA) début 2001. Dans les deux cas, il s'agit de reconnaissance automatique des visages, qui n'est que l'une des techniques de biométrie.

Mais qu'est-ce que la biométrie ? En Français, la biométrie est *l'étude mathématique des variations biologiques à l'intérieur d'un groupe déterminé*. En Anglais, on désigne par *biometrics* la *mesure des éléments morphologiques des humains*, ce qui correspond en fait au terme français *anthropométrie*. Il est intéressant de noter que l'on utilise le terme *biométrie* en lieu et place du terme *anthropométrie* : simple anglicisme, sans doute, mais qui permet de dégager l'ensemble de ces techniques d'une longue histoire policière, ce qui favorise certainement leur acceptation par la population.

Un système biométrique est donc un système automatique de mesure, basé sur la reconnaissance de caractéristiques physiques ou comportementales d'un individu. Ces caractéristiques doivent être **universelles** , **uniques** , **permanentes** , **collectables et mesurables** . La finalité d'un système biométrique est **la vérification et l'authentification** (pour l'éligibilité à un accès ou des services), **l'identification** ou encore **le chiffrement de données** à l'aide d'une clé biométrique.

On peut classer les techniques biométriques en trois catégories :

- Celles basées sur l'analyse de traces biologiques (odeur, salive, urine, sang, ADN, ...)

- Celles basées sur l'analyse comportementale (dynamique du tracé de signature, frappe sur un clavier d'ordinateur, ...)

- Celles basées sur l'analyse morphologique (empreintes digitales, forme de la main, traits du visage, réseau veineux de la rétine, iris de l'oeil, ...)

Les techniques biométriques permettent donc la mesure et la reconnaissance de **ce que l'on est**, à la différence d'autres techniques de mêmes finalités, mais permettant de mesurer ou vérifier **ce que l'on possède** (carte, badge, document, ...) ou **ce que l'on sait** (mot de passe, code pin, ...).

Les techniques biométriques étant basées sur **ce que nous sommes**, de façon unique, permanente au cours de notre vie, collectable et mesurable donc identifiable, il devient clair que leur utilisation pour le contrôle constitue à la fois l'objet de toutes les convoitises du point de vue du **contrôleur** (et de son **fournisseur**, car le contrôle est un marché lucratif) et de toutes les craintes du point de vue du **contrôlé.** Elles sont, en quelque sorte, en ces temps de manichéisme aigu, le *bien absolu* ou le *mal absolu*, selon le point de vue.

En tant que représentante d'une association de protection des libertés individuelles et des libertés publiques, je consacrerai le reste de mon intervention aux enjeux de protection de la vie privée et des données personnelles soulevés par l'utilisation des techniques biométriques.

2. Enjeux

Pour pouvoir appréhender correctement les enjeux de l'utilisation de techniques biométriques, il convient de les classer suivant un certain nombre de critères :

- **Finalité** : la distinction entre l'objectif d'identification et celui de vérification/authentification est importante. Selon le cas, l'information est nominative ou non et permet l'anonymat (qu'il soit absolu ou relatif) ou non. Une finalité de vérification peut se contenter d'accepter ou de refuser un accès, ou donner droit à une classe de services, sans pour autant qu'il y ait nécessité d'identification de l'individu. On citera à cet égard les exemples du contrôle d'accès à des zones dangereuses et sécurisées, ou encore une application basée sur la reconnaissance de la géométrie de la main pour la reconnaissance de l'accès des abonnés au parc d'attraction de DisneyWorld en Floride.

- **Mode d'activation** : on distinguera les techniques selon que l'activation de la reconnaissance est réalisée par la personne à reconnaître - ou à tout le moins en sa présence - ou non, dans le cas où l'activation peut être effectuée par un tiers sans nécessité d'information de la personne. On citera à titre d'exemple un système de reconnaissance à base d'empreintes digitales pour remplacer le mot de passe comme identifiant d'accès à un service de courrier électronique, ou comme clé de déchiffrement d'un courrier crypté, ou encore comme validation d'un mode de paiement à distance. Il y a dans ce cas identification, mais l'individu maîtrise l'utilisation, qui reste personnelle.

- **Consentement** : le consentement de la personne peut être nécessaire ou non à l'usage d'une technique, soit lors de la phase d'enrôlement (capture de l'échantillon), soit lors de la phase de reconnaissance. À ce titre, la reconnaissance faciale à l'aide de caméras installées dans les lieux publics peut être réalisée sans consentement ni même conscience du processus. En revanche, la reconnaissance de la géométrie de la main, par exemple, suppose ce consentement dans les deux phases. Une technique basée sur les empreintes digitales implique, elle, la conscience de la capture de l'échantillon, mais pas forcément de sa reconnaissance, puisque nous laissons partout des empreintes.

- **Stockage** : le stockage des profils d'identification (nominatifs) dans une base de données, la possibilité de coupler cette base de données à d'autres informations, de la transmettre à d'autres systèmes pour d'autres utilisations, sont également des critères déterminants, de même que l'aspect massif ou non de ce stockage.

- **Fiabilité** : la fiabilité d'un système biométrique est mesurée par son taux d'erreurs. On distingue deux taux d'erreurs : celui des acceptations erronées (reconnaissance d'une personne qui n'est pas la bonne) et celui des rejets erronés (non reconnaissance de la bonne personne). Ce taux d'erreur peut être très important dans certains cas.

Au regard de ces critères, on examinera plus particulièrement les enjeux des techniques de reconnaissance faciale et de reconnaissance d'empreintes digitales, toutes deux ayant des finalités

d'identification. Dans les deux cas, plusieurs produits commerciaux existent, et on connaît des exemples d'utilisation.

2.1. Empreintes digitales

Cette technique est bien connue et utilisée depuis longtemps par la police, à laquelle son utilisation reste liée dans l'esprit des gens.

L'empreinte digitale est omniprésente, puisque nous en laissons partout. La constitution de la base est systématique dans plusieurs pays, puisque l'obtention de papiers d'identité y est soumise à la collecte de l'empreinte. Cette situation peut autoriser des recherches indues, notamment dans des pays non démocratiques, et pose donc un problème, tout particulièrement pour les militants politiques. Le problème est encore plus accru lorsqu'il existe un fichier national centralisé.

Mais le plus préoccupant dans le futur réside dans l'utilisation de l'empreinte digitale hors de la sphère policière et, par conséquent, la possibilité de croisement avec les fichiers de police.

On note par exemple l'utilisation de l'empreinte digitale dans l'État de New-York (USA), ou encore en Afrique du Sud, pour le contrôle de l'attribution de prestations sociales. Aux Philippines, la sécurité sociale a établi une base complète des empreintes de ses affiliés.

On note également dans certains pays l'utilisation de l'empreinte digitale pour des contrôles d'accès opérés sur des mineurs, voire de jeunes enfants, par exemple pour l'accès aux cantines scolaires. Signalons qu'en France, une telle demande émanant d'un collège de Nice n'a pas été autorisée par la CNIL qui a considéré, dans une délibération rendue au cours de l'année 2000, la demande excessive au regard de la finalité poursuivie.

On peut craindre la création de méga bases de données, auxquelles les individus ne pourraient pas se soustraire, sauf à renoncer à des prestations essentielles. Ces bases de données pourraient être interconnectées, y compris avec des fichiers de police.

Par ailleurs, plusieurs prestations de service public devenant déléguées à des opérateurs privés, notamment dans un contexte de privatisation et de désengagement de l'État, on peut également craindre la transmission, la revente ou le croisement de bases de données d'empreintes, associées à d'autres informations sur les comportements de consommation.

2.2. Reconnaissance faciale

L'utilisation de techniques de reconnaissance faciale connaît un développement à grande échelle depuis le milieu des années 90, avec des avancées décisives dans les algorithmes de traitement d'images et de fouille d'entrepôts de données *(datamining)*, donnant lieu à la disponibilité de produits commerciaux.

Ces produits permettent :

- l'identification, par comparaison d'un visage à ceux mémorisés dans une base ;

- la vérification, par comparaison des identités déclarées avec les identités associées aux visages mémorisés ;

- la supervision, qui permet de suivre l'image d'une personne dans une séquence vidéo ;

- la surveillance, qui permet de retrouver, en temps réel, une personne dans une séquence vidéo à

partir d'une liste de visages.

L'exemple le plus connu d'utilisation à grande échelle de la reconnaissance faciale est celui de la ville de Newham, dans la banlieue de Londres. Il s'est vu décerner le trophée *Big Brother Award* en 1998 par l'organisation non gouvernementale *Privacy International.*

Outre les questions de fiabilité du système de reconnaissance, de risques de transmission de la base de données à d'autres organismes, y compris du secteur marchand, l'expérience de Newham renvoie exactement aux questions soulevées en France par le STIC (Système de traitement des infractions constatées) : comment est alimentée la base de suspects ? Suivant quelle procédure ? Comment est-elle mise à jour ? Quand un suspect quitte-t-il la base de données ? Et surtout qu'est-ce qu'un suspect ? N'y a-t-il pas risque de confusion entre la suspicion de crimes et de délits mineurs ? Ne risque-t-on pas de trouver dans la base des suspects, mais aussi des victimes ou des témoins, c'est-à-dire toute personne pouvant faire l'objet d'un enregistrement à un moment donné ?

Le processus étant basé sur l'image du visage, la crainte du *délit de faciès* est très vive. Rappelons que Newham est un quartier populaire, où vivent un nombre important de personnes de nationalité étrangère, réelle ou supposée. Le risque de discrimination est loin d'être exclu.

Un autre exemple d'utilisation ayant eu un certain retentissement est celui de la surveillance et l'identification de personnes recherchées, par reconnaissance des visages dans une foule lors de la finale de foot-ball *(Super Bowl)* des USA, qui a eu lieu à Tampa en Floride, en janvier 2001. Cette utilisation a été fortement critiquée par l'ACLU (American Civil Liberty Union), qui a qualifié l'événement de *Snooper Bowl*, autrement dit de *championnat d'espionnage.*

Il est à craindre que la surveillance de grands événements publics par cette méthode augmente. D'autant que l'objet n'est pas uniquement la surveillance pour des questions de sécurité du public, mais surtout la recherche de suspects, y compris de délits mineurs, dans des lieux publics très fréquentés.

Au-delà même de cette utilisation, on peut craindre, encore une fois, des dérives graves liées au *délit de faciès* ou encore au *délit de pauvreté* ou au *délit de comportement déviant.* Qui empêchera de suspecter une personne se trouvant à un moment donné en un lieu, d'être associée à un délit commis en ce lieu ou non loin de là, simplement parce que cette personne ne correspond pas, par son allure extérieure, à l'idée que se ferait un policier d'une personne *légitimement autorisée* à se trouver en un tel lieu ?

3. Premières recommandations

On ne manquera pourtant pas de justifier l'utilisation de techniques biométriques par des questions de rentabilité, voire de productivité du contrôle, et par une politique sécuritaire comme celle dite de *tolérance zéro,* qu'il s'agisse du secteur marchand ou du secteur non marchand, notamment de la police.

Des études comme celles du sociologue Loïc Wacquant sur la ville de New-York (étude non liée à l'utilisation de techniques biométriques) montrent que cette politique de la *tolérance zéro* ne donne pas de meilleurs résultats que celles basées sur la présence d'une police de proximité, privilégiant la prévention sur la répression. Pour une baisse de la criminalité du même ordre observée dans les villes de New-York et de San Diego entre 1993 et 1996, l'accroissement des effectifs de police est moindre à San Diego, de même que le nombre d'arrestations pour infractions mineures, ainsi que le volume des plaintes [Loïc Wacquant. *Les prisons de la misère*. Éditions Liber-Raisons d'agir. Novembre 1999].

Plus généralement, on peut se poser des questions sur une telle société sécuritaire, voire totalitaire : est-ce bien vers cela que nous souhaitons aller ? Le problème de la finalité des traitements basés sur la

biométrie est crucial : est-il vraiment si grave qu'un enfant bénéficie indûment d'un repas dans une cantine ? Est-il si capital de contrôler les horaires des employés à la minute près par de tels moyens ? Certainement pas, au regard des risques encourus et des dangers d'utilisations détournées.

Il importe que la législation encadre très sévèrement les conditions d'utilisation autorisée des techniques biométriques, étant donnée l'importance accrue des risques associés à ces techniques, car il y a un net changement d'échelle par rapport à l'utilisation actuelle des données nominatives, ou de la vidéosurveillance sans traitement des images.

L'autorisation de ces techniques ne devrait se justifier que dans la mesure où leur utilisation est proportionnée au niveau de risque (pour des raisons de sécurité des personnes) et où cette utilisation ne crée ni un sentiment erroné de sécurité par rapport à son efficacité réelle, ni une accoutumance et une perte de la conscience de l'intrusion de ces techniques dans notre vie privée.

À cet égard, l'utilisation de la reconnaissance faciale dans les lieux publics devrait être proscrite, de même que son utilisation dans des lieux privés ou semi-privés, lorsque les personnes concernées sont des mineurs ou n'ont ni la conscience effective de l'existence du système, ni la possibilité de refuser son utilisation, sauf dans des cas très précis impliquant un danger pour les personnes.

Remerciements

L'auteur tient à remercier les personnes suivantes, dont les travaux et écrits ont permis une meilleure compréhension des techniques de biométrie : Philip E. Agre (University of California, Los Angeles ; dlis.gseis.ucla.edu/pagre), Didier Guillerm (Biometrie online ; biometrie.online.fr), Barry Steinhardt (American Civil Liberty Union ; www.aclu.org), sans oublier les membres de la Commission Nationale de l'Informatique et des Libertés (www.cnil.fr) pour la documentation très détaillée qu'ils ont réunie.