Édito

La surenchère biométrique

Jacques Vétois*

L'amendement du député Mariani du projet de loi portant sur la "maîtrise de l'immigration", adopté le 23 octobre 2007, veut imposer aux étrangers déposant une demande de regroupement familial une analyse et un enregistrement d'une partie des séquences de leur ADN qui prouvent leurs liens familiaux. Une fois de plus, les techniques biométriques sont utilisées pour justifier, auprès de l'électorat, la fermeté du gouvernement sur les problèmes liés à l'immigration[1].

La biométrie est au centre des nouvelles technologies d'identification et de surveillance qui, depuis les attentats du World Trade Center, encadrent les activités des États dans toutes leurs fonctions régaliennes, des entreprises et même des particuliers.

Bien que présentées comme des technologies émergentes par les nombreuses entreprises qui se sont engouffrées sur ce marché en pleine expansion, la biométrie désigne une discipline scientifique consacrée à la mesure du vivant et s'inscrit dans la suite du travail d'anthropométrie de la police scientifique initié par Bertillon au début du siècle précédent. Aujourd'hui, l'usage médiatique consacre un sens plus restreint recouvrant les techniques d'identification basées sur la biométrie, voire parfois le contrôle lui-même et non plus seulement la technique de contrôle. Le changement décisif, c'est la numérisation, l'automatisation et la simplification des procédures de saisie et d'enregistrement des données. Ce glissement du sens caractérise assez bien le discours des apôtres d'un contrôle social strict, tant l'instrumentalisation de plus en plus poussée de la science et de la technologie s'avère nécessaire au type de contrat social qu'ils souhaitent établir.

Au problème posé depuis le début du XX^{e} siècle de trouver des procédures d'identification des personnes, s'est ajouté celui de l'authentification

* Jacques Vétois : Directeur de la rédaction de *Terminal*.

1. *Demandeurs de visas : après les empreintes digitales, les tests ADN*, communiqué de presse d'IRIS, 17 septembre 2007.

dans le cadre de la lutte contre la fraude. Après les attentats du 11-Septembre 2001, les États-Unis ont institué d'une manière unilatérale un passeport contenant à la fois la photographie et les empreintes digitales numérisées pour les entrants sur leurs territoire. L'Organisation de l'Aviation civile internationale a pesé de tout son poids pour faire adopter des mesures de sécurité et de contrôle sur tous les vols internationaux. L'Union européenne, malgré les réticences du Parlement européen, s'est ralliée à ces mesures et collabore à leur mise en place. La France n'est pas la dernière à suivre l'exemple des États-Unis. Le gouvernement Villepin sous la présidence de Jacques Chirac s'est dépêché de mettre en chantier un nouveau projet de carte d'identité infalsifiable, INES[2], qui se poursuit à l'heure actuelle.

Le recours aux moyens biométriques, par exemple l'analyse des empreintes digitales, serait justifié selon nos gouvernants par l'insuffisance des techniques classiques de protection des accès aux ordinateurs (*login* et mot de passe) et la multiplication des fraudes par usurpation d'identité. Encore que les renseignements d'ordre statistique que nous avons en la matière, ne proviennent que de sources liées aux entreprises directement intéressées au développement de ce domaine d'activités ou aux instances étatiques travaillant dans la sécurité. Ces chiffres existent, même si on peut les contester. Et les failles de sécurité découvertes dans les systèmes d'exploitation et les logiciels de grande diffusion (libres ou propriétaires) sont en général rapidement connues et corrigées.

La fiabilité des techniques biométriques reste à prouver. Or peu d'études indépendantes existent aujourd'hui. Les chaînes de numérisation et de traitement des processus d'analyse et de scanning des empreintes digitales, de la forme de la main ou des dessins de l'iris de l'œil ont un taux d'erreur sans doute faible (quelques pourcents). L'analyse de séquence de l'ADN est réputée plus fiable mais là encore, le taux d'erreur de l'opération complète, en tenant compte des possibles erreurs de manipulation, n'est pas nulle non plus. Pour un nombre de personnes restreint (une entreprise, une administration...), ces procédés peuvent mettre en correspondance un individu et une suite de données numériques d'une manière univoque. Mais à l'échelle d'un pays, voire du monde entier, il y aura forcément des doublons (la technique n'est plus en cause, c'est un pur effet statistique), c'est-à-dire que des individus différents posséderont la même représentation numérique.

Quand ces informations seront stockées dans des bases de données et ainsi validées, comment les corriger ? Et que se passera-t-il si elles sont volées ou empruntées ? On ne peut changer ni les empreintes digitales, ni l'ADN de quelqu'un. A moins de recourir à des méthodes intrusives ou chirurgicales comme dans le film *Minority report* où le héros n'a pas d'autres solutions pour changer l'iris de son œil et ne pas être retrouvé par les robots de la police. La divulgation des données biométriques d'une personne invalidera toute utilisation ultérieure par cette personne de tout dispositif

2. "INES : de la suspicion au traçage généralisé", DELIS, *Terminal*, 93-94, 2005.

d'authentification[3]. La biométrie n'apporte pas de garanties de protection des données et de confidentialité. Les recours à des sociétés privées dans le traitement des données se multiplient. Le marché de l'identification biométrique est en plein essor, en particulier celui basé sur les empreintes digitales.

La plupart des pays (même la Grande-Bretagne) se dotent de papiers d'identité enregistrant des données biométriques. Qu'adviendra-t-il des données ainsi accumulées ?

Les détournements de finalités des systèmes mis en place se font bien souvent avec l'accord des instances gouvernementales : le fichier des empreintes génétiques FNAEG initialement institué pour les délinquants sexuels a été étendu aux militants politiques et syndicaux interpellés lors d'actions illégales comme celle des faucheurs volontaires.

L'opinion publique est anesthésiée et consentante au nom de la sécurité : la lutte contre le terrorisme justifie toutes les mesures prises. Gare à ceux qui par malchance (victime d'un disfonctionnement, d'une usurpation d'identité) se retrouveront pris dans les filets de la machine sécuritaire, ou à ceux qui entendront résister à cette mise en fiche généralisée.

■

3. "De l'authentificatiion biométrique", Philippe Wolf, *Sécurité informaique* n° 46, octobre 2003.