

Dispositifs biométriques, dispositifs éthiques ?

Sandra Franrenet
Doctorante en éthique de la Recherche

Introduction

A partir du 28 juin 2009, quelques 2000 mairies françaises seront en capacité de délivrer des passeports biométriques. Ces nouveaux titres d'identité – qui remplaceront progressivement les passeports électroniques – stockeront dans une puce RFID¹ la photo de leur titulaire ainsi que les empreintes digitales² de huit doigts (soit le pouce, l'index, le majeur et l'annulaire de chaque main). Issu d'un règlement européen (1), le passeport biométrique est censé permettre une identification rapide et sûre de son possesseur afin d'éviter tout risque d'usurpation d'identité et de lutter contre le terrorisme international. Fort de cet objectif, le décret du 30 avril 2008 (2) autorise le ministre de l'intérieur à créer « *un système de traitement automatisé de données à caractère personnel dénommé TES* » pour prévenir et détecter la falsification et la contrefaçon de ces documents. Cette actualité offre l'opportunité de revenir sur la multiplicité des dispositifs biométriques, de s'interroger sur leur occurrence éthique et d'entrevoir les principaux risques liés à sa généralisation.

Une multiplicité des dispositifs biométriques pour une multiplicité d'enjeux

Le lexique du site Internet de la cité des sciences³ définit la biométrie comme « *l'ensemble des techniques de mesure des êtres vivants et des méthodes statistiques de traitement de ces mensurations. Dans le domaine de l'identification des personnes, la biométrie utilise l'informatique pour identifier ou authentifier quelqu'un grâce à la mesure d'une ou plusieurs caractéristiques physiques spécifiques à chacun : empreinte digitale, image rétinienne, ADN, etc.* ». Les « *données biométriques* » constituent plus précisément « *les informations à caractère morphologique, biologique ou comportemental propres à une personne* » (3). En quelques années seulement, la « *biométrisation de l'homme* » pour reprendre un terme employé par le Comité consultatif national d'éthique (CCNE) s'est considérablement accéléré tout en se faisant de plus en plus précise : numérisation des photographies du visage et des empreintes digitales, géométrie de la main, réseaux des doigts et du bras, reconnaissance de l'iris, etc. Le recours à ces dispositifs multiples a été justifié dès 2003 par le député Christian Cabal pour lutter contre la fraude, assurer la sécurité des échanges financiers et commerciaux ainsi que l'accès légitime aux services gouvernementaux et enfin contrer le vol d'identité sous toutes ses formes (4). Ils sont aujourd'hui plus particulièrement utilisés dans quatre domaines

¹ Radio Frequency Identification : méthode utilisée pour stocker et récupérer des données à distance en utilisant des balises métalliques, les « Tag RFID ». Ces balises, qui peuvent être collées ou incorporées dans des produits, et qui sont composées d'une antenne et d'une puce électronique, réagissent aux ondes radio et transmettent des informations à distance. Cette technologie est censée, à terme, remplacer les codes barres (http://www.futura-sciences.com/fr/definition/t/high-tech-1/d/rfid_4187/).

² A l'exception des enfants de moins de six ans.

³ http://www.cite-sciences.fr/lexique/pop_definition.php?iddef=737&id_habillage=48&id_expo=33&lang=fr
Sandra Franrenet, avril 2009 ©

Cet article est protégé et ne peut être reproduit ou copié sans l'autorisation de l'auteur.

En cas de citation celle-ci doit mentionner : l'auteur (Nom et prénom), le titre, la rubrique du Site Internet, l'année, et l'adresse www.ethique.inserm.fr

: l'identification judiciaire, la gestion des titres délivrés, la gestion des accès physiques et virtuels et enfin le contrôle des responsables de la sécurité. Leur champ d'application va certainement se propager très rapidement à d'autres secteurs compte tenu de l'image attrayante qui est véhiculée. Et la Commission d'accès à l'information du Québec d'expliquer que la biométrie est présentée au grand public comme un « *remède universel propre à terrasser plusieurs maux : terrorisme, fraude, vol d'identité et atteinte à la vie privée* » ; elle est montrée aux employeurs comme « *une solution au vol de temps par les travailleurs* » ou encore « *un moyen facile de produire les données de base servant au calcul de la paye.* » Aux utilisateurs enfin, elle est représentée « *comme un moyen confortable de s'identifier; plus de cartes qu'on égare et de mots de passe qu'on oublie* » (5). Le sociologue Gérard Dubey considère pour sa part que c'est sans doute moins son utilité pratique qui justifie son utilisation que le fait qu'elle est vue « *comme une avancée technique dans la continuité des évolutions antérieures* » : « *Même si l'on ne perçoit pas toujours à court terme les avantages de la biométrie* » remarque-t-il, « *cette dernière semble s'imposer du fait de la complexité même des dispositifs d'information et de leur nécessaire sécurisation* » (6). Or c'est sans doute ici que le danger est le plus grand : adhérer à une technique parce qu'elle simplifie une situation ou encore parce qu'elle semble inéluctable au nom du sacro-saint progrès.

Principales questions éthiques soulevées par les dispositifs biométriques

Malgré les avantages offerts par la biométrie, le CCNE s'est récemment interrogé sur les principales questions éthiques qu'elle soulève (7). Et de se demander si les données qu'elle nécessite de collecter ne contribuent pas finalement à « *une instrumentalisation du corps et en quelque sorte à une déshumanisation* » qui risque à terme de « *déséquilibrer le regard sur la personne enfermée dans sa « biométrie » au profit de la seule apparence scientifiquement déterminée* » ? Or comme l'a démontré Paul Ricoeur dans son ouvrage « *Soi-même comme un autre* » (8), l'identité humaine ne se réduit pas au seul corps dans son objectivité (concept qu'il intitule « *mémeté* »), mais englobe également le vécu d'existence subjective qu'il appelle « *ipséité* » et qu'il définit comme « *le maintien de soi de l'individu à travers les aléas événementiels qui construisent son histoire.* » L'individu ne se résume donc pas à sa seule identité biologique mais intègre des éléments non palpables qui façonnent l'être humain tout au long de son existence. A côté de cet argument identitaire, le comité d'éthique pose une autre question qui peut d'ailleurs concerner n'importe quel autre procédé morphologique : la biométrie ne risque-t-elle pas aussi de stigmatiser les personnes vivant avec un handicap et d'exclure celles qui ne sont pas « *aisément paramétrables* » ?

Principaux risques engendrés par les dispositifs biométriques

Outre les questions éthiques qu'il soulève dans son avis n° 98 (7), le CCNE alerte également sur les principaux risques qu'un dispositif biométrique peut entraîner.

Risques relatifs au recueil des données

La collecte de données personnelles, qu'il s'agisse d'une empreinte digitale, du contour de la main ou d'une photographie de l'iris, exige que l'autorité ou l'organisme qui y procède sollicite en amont le consentement éclairé de la personne concernée. Or, selon le comité d'éthique, cette exigence « *est bafouée lorsque la donnée identifiante est recueillie à l'insu de l'intéressé (photographie de l'iris à distance, enregistrement électrique à distance) ou lorsque*

Sandra Franrenet, avril 2009 ©

Cet article est protégé et ne peut être reproduit ou copié sans l'autorisation de l'auteur.

En cas de citation celle-ci doit mentionner : l'auteur (Nom et prénom), le titre, la rubrique du Site Internet, l'année, et l'adresse www.ethique.inserm.fr

le consentement n'est pas demandé comme en Angleterre, lors d'un prélèvement de cheveu, d'ongle ou de salive. » Dans les deux cas, la personne n'est pas en mesure de faire jouer son droit d'opposition et s'expose à ce que ses données soient utilisées à d'autres fins que celles pour lesquelles elles ont été collectées.

Risques relatifs à la finalité de l'utilisation des données

Coordinateur du projet ETIB⁴ (9) qui a pour objectif d'aider l'industrie et les universités à faire face aux questions éthiques soulevées par la biométrie et de lancer un débat public sur ses implications, le Professeur Emilio Mordini, considère que l'aspect le plus controversé de la biométrie réside dans le risque de divulgation des données recueillies. Compte tenu de leur nature intime et personnelle, ces données risquent en effet de fournir des informations confidentielles sur l'état de santé d'une personne (maladie, grossesse) et plus globalement sur son mode de vie (alcool, drogue, médicaments, etc.). Fort de ce danger, le comité d'éthique français estime qu'un « *strict respect de la finalité recherchée est essentiel* » afin d'éviter notamment toute collusion entre données publiques et privées qui risquerait d'entraîner « *de graves discriminations dans le domaine des assurances ou de l'emploi en particulier au moment de l'embauche* » (7).

Cette situation menace pourtant de devenir réelle à l'occasion du remplacement des passeports électroniques par les passeports biométriques. Le décret du 30 avril 2008 (2) autorise en effet le ministre de l'intérieur à créer en parallèle un système de traitement automatisé de données à caractère personnel dénommé *TES* pour prévenir et détecter la falsification et la contrefaçon de ces titres d'identité. Cette disposition va cependant à l'encontre de la délibération de la Commission Nationale Informatique et Libertés (CNIL) du 11 décembre 2007 (11) qui considère que « *les finalités de simplification administrative et de lutte contre la fraude documentaire ne sauraient à elles seules justifier la création d'un tel fichier, dès lors qu'aucune mesure particulière n'est prévue pour s'assurer de l'authenticité des pièces d'état civil fournies.* » Et d'en conclure que « *la conservation dans un fichier central des photographies et des empreintes digitales était disproportionnée au regard des finalités du fichier*⁵. » Trois ans plus tôt, le groupe des autorités européennes de protection des données (G29) avait déjà exprimé « *les plus grandes réserves sur la conservation de données biométriques dans des bases de données au-delà de la période nécessaire aux contrôles légaux pour la délivrance, la production et la remise aux demandeurs des (visas ou titres de séjour), dans la mesure où les éléments biométriques concernés sont des éléments dont la personne laisse des traces dans la vie quotidienne* » (12). Le président du G29 avait d'ailleurs adressé une lettre datée du 18 août 2004 aux présidents des différentes institutions européennes (Commission, Conseil, Parlement) manifestant son opposition à la constitution d'une base de données européenne des passeports et documents de voyage des Européens incluant les données biométriques au motif que celle-ci n'est pas nécessaire pour assurer le lien entre un document et son titulaire légitime. Force est de constater que ce courrier n'a trouvé aucun écho au niveau français.

Conclusion

Depuis le décret du 30 avril 2008, le remplacement des passeports électroniques légitime la constitution d'un système de traitement automatisé de données à caractère personnel justifié

4 Le projet ETIB (Ethique des Technologies d'Identification Biométrique) également appelé BITE (Biometric Identification Technology Ethics) est financé au titre de la section Science et Société du 6^{ème} programme-cadre. Sandra Franrenet, avril 2009 ©

⁵ <http://www.cnil.fr/index.php?Id=2428> reproduit ou copié sans l'autorisation de l'auteur.

En cas de citation celle-ci doit mentionner : l'auteur (Nom et prénom), le titre, la rubrique du Site Internet, l'année, et l'adresse www.ethique.inserm.fr

par un argument sécuritaire. Cette vaste base sera composée de deux types de données identifiantes : les empreintes digitales et les photographies de tous les titulaires de passeport biométriques. Comment dès lors garantir que les informations collectées pour éviter la falsification et la contrefaçon de leur propre titre d'identité ne feront pas, à terme, l'objet de collisions avec d'autres bases de données ? Comment également leur assurer que ces mêmes données conserveront leur caractère confidentiel après leur éventuelle transmission, alors que des expertises convergentes réalisées par des sociétés informatiques et par la groupe Fidis⁶ pour le compte de l'Union Européenne ont montré que la confidentialité des données transmises à partir des puces électroniques intégrées au passeport biométrique était illusoire ? Comment empêcher également que ces informations biométriques ne réduisent pas, à terme, l'identité des citoyens à « *une somme de marqueurs instrumentalisés*⁷ » ? Face à l'importance de ces questions et l'ampleur des risques qui y sont associés, le Comité d'éthique a formulé plusieurs recommandations et préconisé la mise en œuvre d'un « *réel contre-pouvoir* » indépendant offrant des garanties contre « *d'éventuelles dérives technocratiques, économiques, policières ou politiques liées à l'exploitation des données biométriques* » (8). Gageons qu'il soit entendu au nom de l'histoire récente de ces cinquante dernières années...

BIBLIOGRAPHIE

- (1) Règlement (CE) n° 2252/2004 du Conseil du 13 décembre 2004 établissant des normes pour les éléments de sécurité et les éléments biométriques intégrés dans les passeports et les documents de voyage délivrés par les États membres
- (2) Décret 2008-426 du 30 avril 2008 modifiant le décret n° 2005-1726 du 30 décembre 2005 relatif aux passeports électroniques
- (3) Commission de l'éthique, de la science et de la technologie (Québec), Document de réflexion, L'utilisation des données biométriques à des fins de sécurité : questionnement sur les enjeux éthiques, 7 décembre 2004, <http://www.ethique.gouv.qc.ca/L-utilisation-des-donnees.62.html>
- (4) Les méthodes scientifiques d'identification des personnes à partir de données biométriques et les techniques de mise en œuvre, Office Parlementaire d'Evaluation des Choix Scientifiques et Technologiques (OPCEST), Christian CABAL, député, Sénat, Assemblée nationale (France), juin 2003, p. 7.
- (5) Commission d'accès à l'information du Québec, « La biométrie au Québec : Les enjeux », juillet 2002, p. 23
- (6) Dubey G., Nouvelles techniques d'identification, nouveaux pouvoirs. Le cas de la biométrie, Cahiers internationaux de sociologie 2008/2, n° 125, p. 263-279.
- (7) CCNE, avis n°98 « Biométrie, données identifiantes et droits de l'homme », 26 avril 2007, <http://www.ccne-ethique.fr/avis.php>
- (8) Ricoeur P., Soi-même comme un autre, Ed. du Seuil 1990
- (9) <http://www.biteproject.org/>
- (10) Le projet ETIB, point de départ d'un débat européen sur l'éthique de la biométrie, 14 mai 2005, www.biteproject.org/press_book/etib.pdf
- (11) CNIL, délibération n°2007-368 du 11 décembre 2007 portant avis sur un projet de décret en Conseil d'Etat modifiant le décret n°2005-1726 du 30 décembre 2005 relatif aux passeports électroniques, <http://www.cnil.fr/index.php?id=2427>
- (12) G29, avis du 11 août 2004, <http://www.cnil.fr/index.php?id=1666&print=1>

⁶ Sandra Fronrenat, avril 2009: ©

⁷ Cet avis du CCNE n° 98, p. 19, ne peut être reproduit ou copié sans l'autorisation de l'auteur.

En cas de citation celle-ci doit mentionner : l'auteur (Nom et prénom), le titre, la rubrique du Site Internet, l'année, et l'adresse www.ethique.inserm.fr