République Française

ASSEMBLÉE NATIONALE

SÉNAT

OFFICE PARLEMENTAIRE D'ÉVALUATION DES CHOIX SCIENTIFIQUES ET TECHNOLOGIQUES

La Biométrie

Audition publique du jeudi 4 mai 2006

organisée par M. Christian Cabal, Député de la Loire

L'Office parlementaire d'évaluation des choix scientifiques et technologiques a décidé d'assurer le suivi du rapport de M. Christian Cabal, député, sur les méthodes scientifiques d'identification des personnes à partir des données biométriques, publié en juin 2003 (rapport Assemblée nationale n° 938 et Sénat n° 355), afin de dresser un état des lieux des évolutions en cours et de mieux cerner les enjeux des applications des systèmes d'identification.

Synthèse

I - Les évolutions scientifiques et technologiques

En trois ans, des évolutions technologiques notables se sont produites. Cependant les normes ont peu évolué, et les propositions de mise en place d'instances de concertation et de nouvelles modalités de régulation faites par l'OPECST n'ont pas été suivies d'effet.

1. Les recherches en cours

Dans le domaine médical, des travaux sont envisagés : dictionnaire rassemblant les données biométriques essentielles, définitions et mesures, recherches sur les normes, les moyennes, la variabilité du corps (changement de taille, de couleur de l'iris, etc.) et sur le thème génétique et biométrie.

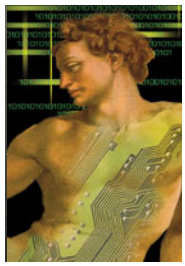
Dans le domaine industriel, les industries dédiées à la biométrie cherchent à accroître la fiabilité et les performances des différentes modalités. Par ailleurs, l'Institut français du textile et de l'habillement est à l'origine d'une campagne nationale de mensuration des Français.

Les recherches dans le domaine des sciences humaines montrent que l'identité change de nature et de signification, entraînant une requalification de la notion d'identité désormais accessible à la mesure. On observe le passage d'une reconnaissance sociale par l'environnement -village, quartier- à la validation automatique par l'informatisation, à l'aide de documents numériques d'identité. Il ne sera plus aussi nécessaire de lier un individu à un nom ou à un prénom, à une date et lieu de naissance etc…, il suffira de le relier à l'une de ses caractéristiques physiques. Les études en cours sur la façon dont la biométrie affecte le rapport entre l'État et les individus révèlent une bonne acceptabilité des techniques biométriques, sans rejet *a priori*. Toutefois, la plupart des personnes interrogées lors d'une consultation publique lancée en mars 2006 dans le cadre du projet européen « éthique des technologies d'identification biométrique » (ETIB) estime que le public n'est pas correctement informé.

2. Les évolutions technologiques

Les modalités

- ***Le visage*** est une modalité dynamisée par les passeports biométriques qui intègrent désormais dans la puce la photographie numérisée du visage. Sur les grandes bases de données, le taux d'erreur a été divisé par deux depuis 2002. Des systèmes permettant d'identifier des visages « à la volée » ou encore d'identifier des personnes recherchées dans des contextes opérationnels particuliers sont désormais envisageables.



- La technologie de ***la forme de la main,*** utilisée pour les contrôles d'accès, a peu évolué.
- ***Les empreintes digitales*** sont toujours la technologie phare, en termes de performance et de déploiement.
- ***L'iris*** donnant de bons résultats est utilisé dans les systèmes d'identification et de contrôle d'accès. Si on arrive à le capter à distance (il existe déjà plusieurs expériences), cette modalité pourra être utilisée pour la surveillance. La technologie actuelle permet de reconnaître des iris « à la volée », à plusieurs mètres de distance. Entre 2003 et 2005, le taux d'erreur a été réduit à 1 % à l'enregistrement et les faux rejets varient désormais entre 1 et 2 %. Le temps de vérification est dorénavant descendu à environ 4 secondes.
- ***Les veines*** sont une modalité sans contact qui se développe en Asie où, sous réserve de validation, elle pourrait se substituer à terme à la reconnaissance par la longueur des doigts.
- ***La reconnaissance vocale*** demeure difficile à utiliser pour l'instant, mais de nombreux travaux sont menés sur les performances en ambiance bruitée. Si cette modalité s'améliore, elle pourra être utilisée dans le domaine de la surveillance.
- ***L'ADN*** nécessitant un laboratoire, il faudra effectuer des progrès en matière d'automatisation pour obtenir un résultat rapide, afin que cette modalité soit performante à grande échelle.

Office parlementaire - Assemblée nationale 233 bd Saint Germain 75355 Paris 07 SP - tél : 01 40 63 88 15 - fax : 01 40 63 88 08
Sénat 6 rue Garancière 75291 Paris Cedex 06 - tél : 01 42 34 25 58 - fax : 01 42 34 38 55 - www.assemblee-nationale.fr - www.senat.fr

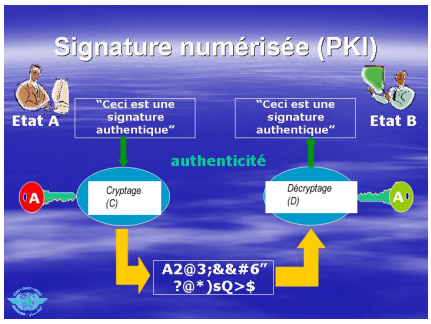
La validation des algorithmes

Les variations du corps humain sont une donnée extrêmement importante, les recherches menées dans ce domaine ont pour objectif d'appliquer la norme de qualité « Six Sigma » pour limiter les erreurs et augmenter la fiabilité des techniques.

La multi-modalité

La combinaison de plusieurs modalités biométriques permet d'augmenter les performances globales, de diminuer les taux d'erreur et d'impossibilité de captage. Elle associe distinctement le visage et les empreintes digitales de différents doigts dans un passeport. Mais ce système plus coûteux nécessite plusieurs capteurs et implique des conditions d'acquisition plus difficiles. Utilisera-t-on alors ces deux biométries de manière alternative ? Y gagnera-t-on en performance?

L'amélioration de la sécurisation des données personnelles est essentielle et fait l'objet de recherches. Lorsque les données sont stockées sur le document du porteur, le mécanisme de sécurisation est similaire à celui d'un code PIN. Quand elles sont stockées dans une base, la base n'étant pas nominative, on détecte simplement que la personne était déjà dans la base sans identification possible. Pour empêcher les accès malveillants à la base, la sécurisation physique fonctionne



si la base n'est pas reliée au réseau ; les échanges s'effectuent alors par transit des données sur des supports physiques, sans possibilités d'accès à distance. Une sécurisation totale est à l'étude pour que les données ne sortent jamais du document du porteur qui disposerait éventuellement de son capteur. Par ailleurs, des liaisons unidirectionnelles à partir de diodes optiques permettent d'envoyer des informations dans une base en étant sûr qu'elles ne repartent pas dans l'autre sens. On gère ainsi le sens des transmissions. Des recherches sont menées pour extraire un code identifiant unique, stable, d'une donnée biométrique.

Les standards

En 2003, un groupe de référence au Centre Européen de Normalisation (CEN) consacré à la biométrie a été crée ainsi qu'un Comité Biométrique à l'AFNOR en 2004. Dès 2004, le Bureau International du Travail (BIT) a conduit des certifications d'interopérabilité dans le cadre du projet de la carte d'identité des marins. En 2005, le standard de gabarit biométrique « Minutiae » des empreintes digitales est sorti. En 2006, le *National Institute of Standards and Technology* (NIST) a confirmé l'interopérabilité de gabarits d'empreintes digitales « Minutiae » avec des performances opérationnelles acceptables.

L'évaluation

Le 30 mars 2005, la Commission européenne a rendu public le rapport *« Biometrics at the frontiers : assessing the impact on society »* qui montre que les États ont un rôle à jouer dans l'émergence d'une industrie biométrique européenne dynamique. Mais ce rapport déplore l'absence de données indépendantes et souligne l'urgence d'organiser des essais à grande échelle sur le terrain. S'inscrivant dans cette logique, le projet européen BIODEV *(Biometric Data Experimented in Visas)* vise à tester l'introduction de la biométrie dans les visas pour entrer dans l'espace Schengen et à évaluer la faisabilité de cette opération. Le premier volet de cette expérimentation pilotée par la France s'est terminé fin mai 2006. Plusieurs logiciels et matériels ont été testés par des postes consulaires répartis sur chaque continent. Les temps d'enregistrement des données biométriques et ceux passés au contrôle à la frontière ont été progressivement réduits. Sur le plan technique, le système basé sur la prise d'empreintes des dix doigts posés à plat a été validé pour éviter les faux rejets ou les fausses acceptations, et donc réduire les marges d'erreurs ; le support sur une base de données centralisée a été également validé. Le projet BIODEV, qui implique que tous les requérants se présentent en personne pour la prise d'empreintes digitales, est coûteux, car il entraîne une augmentation de la fréquentation des locaux consulaires et des effectifs à la frontière. Néanmoins la Commission Européenne a jugé les résultats intéressants et a autorisé le lancement du deuxième volet de l'expérimentation afin de tester l'interopérabilité de systèmes informatiques avec des appareils et des équipements provenant de pays différents.

II - Les applications de la biométrie : actualité et perspectives

1. L'avenir des grands domaines d'application

Le domaine identitaire exigera des performances accrues pour combattre les usurpations ou les changements d'identité. Il faudra traiter des bases de 60 millions à 100 millions de personnes et des flux de personnes interrogées de l'ordre de 10 000 à 20 000 par jour tout en obtenant des taux de précision extrêmement élevés pour identifier correctement les personnes et contrôler leur identité.

Le contrôle d'accès dont on recherche la plus grande fluidité se décline de deux manières : l'accès physique aux sites sensibles (entreprises, aéroports, banques) ou l'accès logique à un ordinateur de bureau ou de poche, à un téléphone, à un distributeur de billets.

La surveillance tend à faire évoluer les technologies vers l'identification à distance, en mouvement, à la

volée de personnes recherchées grâce à la photo, la vidéo, bientôt l'iris.

2. Le marché de la biométrie

Les marchés biométriques gouvernementaux et ceux des équipements personnels se sont davantage accrus que ceux à usages industriels et commerciaux. Les marchés gouvernementaux restent toujours les moteurs du développement d'une industrie de la biométrie. Le marché grand public de la biométrie par empreintes digitales se développe plus rapidement que les autres. En 2004, plus de 2,4 millions de capteurs d'empreintes digitales ont été vendus au travers d'ordinateurs portables, d'assistants personnels et de téléphones mobiles. Ce nombre devrait doubler en 2005. L'usage de la biométrie, comme technologie permettant de gérer des grands flux de personnes aux frontières sans failles de sécurité, devient le ferment d'une biométrie mondiale inter opérable. Les programmes de cartes d'identité devraient faire l'objet d'une modernisation. Dans les trois prochaines années, des bases de plus de 100 millions de personnes, voire de plusieurs centaines de millions, feront l'objet de projets concrets.

3. Les applications et perspectives à l'étranger

Aux Etats-Unis, la biométrie est devenue, au cours de ces trois dernières années, une technologie de souveraineté et de sécurité nationale. Le NIST a constitué des bases de tests de millions de données biométriques. L'administration fédérale met en œuvre la biométrie dans le cadre de programmes de gestion d'identité des personnes pour les travailleurs du secteur des transports et pour les employés fédéraux et leurs contractants, ou encore des systèmes de contrôle d'identité biométrique en préalable à toute autorisation de travail sur une activité sensible. En 2006, le FBI doit lancer un programme développant une nouvelle génération de systèmes de traitement automatique d'empreintes digitales permettant de gérer plusieurs centaines de millions de personnes.

En Australie, un système de contrôle aux frontières par reconnaissance du visage est mis en oeuvre.

Au Mexique, le système électoral gérera à terme les empreintes digitales et les visages de 72 millions de personnes.

Par ailleurs des systèmes d'identification biométrique existent ***au Kenya, au Cameroun, en Namibie et en Ethiopie.***

Dans l'Union Européenne, sous l'impulsion de la Direction Générale Justice Liberté et Sécurité (JLS), de grands programmes voient le jour et portent sur une gestion plus efficace des frontières de l'Union avec des projets comme BMS (*Biometric Matching System)*, BIODEV ou l'annonce pour 2008 de passeports biométriques à empreintes digitales. L'Union Européenne, contrairement aux États-Unis, traitera de la même façon ses citoyens et ses visiteurs. Par ailleurs, la plupart des pays membres de l'Union projettent de mettre en place ou disposent déjà de documents d'identité contenant de la biométrie.

4. Les applications et perspectives en France

Des projets pilotes significatifs ont été lancés : c'est le cas du Programme d'Expérimentation et de Gestion Automatisée et Sécurisée (PEGASE) ou encore de l'expérimentation BIODEV. Ces deux programmes ont permis à la France d'acquérir en moins de trois ans une notoriété internationale en matière de grands programmes biométriques. Le projet d'identité nationale électronique sécurisée (INES) est en cours de réexamen.

III - Les principaux enjeux de l'application des systèmes d'identification biométrique

Il existe une tension fondamentale entre ceux qui soutiennent que les données engendrées par le corps sont elles-mêmes un corps bénéficiant des mêmes droits et protections que le corps humain et ceux qui pensent que les données engendrées par le corps doivent être considérées comme des produits qui ne bénéficient pas du même statut et des mêmes protections que celui-ci.

1. Les organisations internationales

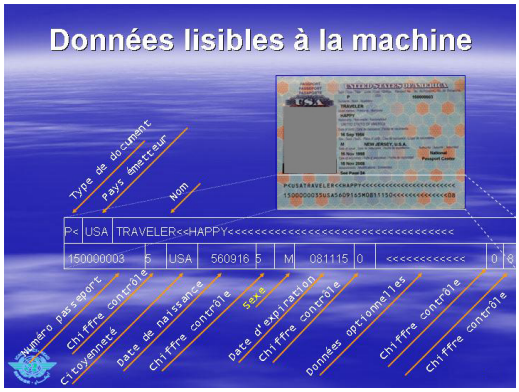
L'OCDE a rendu public, en novembre 2005, un rapport élaboré en 2003, sur l'usage transfrontalier de l'authentification dans les pays de l'OCDE. Il présente les principales technologies biométriques et traite des faiblesses des systèmes biométriques qui doivent être protégés.

Le Conseil de l'Europe a élaboré un rapport d'étape en février 2005 sur l'application des principes de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (n°108). Il souligne la spécificité des données biométriques, préconise une évaluation des avantages et inconvénients possibles pour la vie privée, la biométrie ne devant pas être choisie parce qu'elle est pratique à utiliser. Les données biométriques, et toutes données associées générées par le système, doivent être adéquates, pertinentes et non excessives par rapport à la finalité du traitement, être utilisées à des fins déterminées, explicites et légitimes, et ne pas être ultérieurement traitées d'une manière incompatible avec ces finalités. Le rapport du Conseil de l'Europe insiste sur l'importance du système de traitement des données qui doit être protégé, évalué et utilisé par un personnel compétent, être configuré de façon à exclure la collecte et le traitement de plus de données biométriques ou associées que sa finalité ne l'exige.

L'Organisation internationale de l'aviation civile (OACI)

Le Conseil de l'OACI a, en mars 2005, adopté une recommandation visant l'intégration de données biométriques dans les documents de voyage lisibles à la machine (MRTD). Elle prévoit l'utilisation de puces sans

contact pour stocker ces données, l'élaboration d'une structure logique des données qui doivent être protégées par une signature numérisée sur la base du système de gestion des clefs publiques (PKI) pour en garantir l'inviolabilité. Les spécifications techniques pour l'intégration



des données biométriques dans les passeports seront publiées à l'automne 2006. L'OACI a décidé d'évaluer les technologies disponibles en fonction des exigences précises qu'impliquent la délivrance et l'inspection des documents de voyage.

La Conférence internationale des Commissaires à la protection des données et à la vie privée s'est tenue en Suisse du 14 au 16 septembre 2005 et s'est conclue par l'adoption d'une déclaration finale visant au renforcement du caractère universel des principes de la protection des données.

2. Les débats en France

La lutte contre la fraude documentaire et les exigences des organisations internationales tendent à justifier l'introduction de la biométrie dans les passeports et les cartes d'identité. Selon les associations regroupées dans le collectif Droits et Libertés face à l'Informatisation de la Société (DELIS), la France et l'Union Européenne ont été contraintes, sous la pression des Etats-Unis, de donner certaines informations concernant les passagers se rendant aux Etats-Unis, les *Personal Name Records* (PNR), ainsi que de fabriquer des passeports biométriques sans obtenir de garanties suffisantes quant à l'utilisation et au stockage des données y figurant. Ces associations s'inquiètent également du risque de captage de ces données à distance avec des puces d'identification par fréquence radio (RFID). Selon elles, la biométrie associée aux supports RFID, dont personne ne connaît la limite, crée un outil qui recèle une vocation totalitaire.

La lutte contre la fraude documentaire

En France, 90 000 titres vierges ont été volés entre 1999 et 2004, 90 000 passeports déclarés perdus ou volés par leur titulaire sur la même période. Les pertes ou vols de cartes nationales d'identité sont passées de 37 000 en 1997 à 527 000 en 2003. La source d'information relative à l'état-civil est extrêmement poreuse à la fraude car il n'existe ni registre d'état-civil national, ni système de recueil automatisé des données personnelles des citoyens.

Le projet d'identité nationale électronique sécurisée (INES) fait l'objet d'un réexamen portant notamment sur les usages électroniques de la carte d'identité qui n'est pas obligatoire en France et sur la nécessité d'une base de données biométriques pour fiabiliser les données d'identité. Améliorer significativement la fiabilité des titres implique l'aménagement des procédures, pour que l'état-civil ne soit plus demandé par un citoyen à sa mairie de naissance, mais échangé directement entre la mairie de naissance et celle de demande du titre. Selon le ministère de l'Intérieur, il n'existe pas d'autre moyen que la base de données pour délivrer des titres non falsifiables dans le système français où il n'y a ni registre de population, ni numéro universel.

La position de la Commission nationale informatique et libertés (CNIL)

La loi du 6 août 2004 soumet à autorisation de la CNIL la biométrie lorsqu'elle est mise en œuvre par des organismes privés. Par ailleurs, la CNIL est saisie pour avis des projets de l'État en matière de biométrie, ce qui l'a amenée à se prononcer sur le passeport électronique, sur l'expérimentation BIODEV et sur l'expérimentation du programme d'expérimentation et de gestion automatisée et sécurisée (PÉGASE). En principe, la CNIL autorise la biométrie quand elle ne laisse pas de trace quel que soit le mode de stockage. Si elle en laisse, comme dans le cas de l'empreinte digitale, le support individuel permet d'obtenir cette autorisation. Le recours à une base centrale pose la question de l'existence d'un impératif fort de sécurité ou de la légitimité du motif. Il n'y a pas jusqu'à présent de cas où la CNIL donne une autorisation en l'absence d'impératif de sécurité. La CNIL a adopté, au cours de sa séance du 27 avril 2006, des autorisations uniques pour les systèmes de contrôle de la main, d'empreintes digitales avec cartes à puce, lorsqu'un tel système sert à l'accès aux locaux.

Conclusion

La biométrie est en constante évolution. On constate qu'apparaissent toujours de nouvelles modalités, ce qui exige une veille technologique permanente, des études comparatives effectuées par des organismes indépendants et des instances de régulation fiables car on ne plaque pas la biométrie sur une organisation existante, on l'intègre. La mise en place de normes d'utilisation doit être progressive. La finalité des utilisations de la biométrie dans le domaine de l'identification des personnes doit être définie avec précision afin d'éviter la collecte et le traitement de plus de données biométriques qu'il n'en faut. Il y a des règles à respecter, des méthodes à définir, des contrôles à effectuer régulièrement. Il est d'ailleurs important que la France et l'Union européenne continuent d'occuper une position influente dans le domaine de la biométrie pour peser sur l'évolution des diverses techniques et sur la définition des normes.

Septembre 2006