N° 3302

ASSEMBLÉE NATIONALE

CONSTITUTION DU 4 OCTOBRE 1958

DOUZIÈME LEGISLATURE

Enregistré à la Présidence de l'Assemblée nationale
Le 8 septembre 2006

N° 480

SÉNAT

SESSION EXTRAORDINAIRE DE 2005 – 2006

Annexe au procès-verbal
de la séance du 11 septembre 2006

**OFFICE PARLEMENTAIRE D'ÉVALUATION
DES CHOIX SCIENTIFIQUES ET TECHNOLOGIQUES**

COMPTE RENDU DE L'AUDITION PUBLIQUE
DU 4 MAI 2006

sur

LA BIOMETRIE

Déposé sur le Bureau
de l'Assemblée nationale
par M. Claude BIRRAUX,

Premier Vice-Président de l'Office

Déposé sur le Bureau du Sénat
par M. Henri REVOL,

Président de l'Office

Composition de l'Office parlementaire d'évaluation des choix scientifiques et technologiques

Président
M. Henri REVOL

Premier Vice-Président
M. Claude BIRRAUX

Vice-Présidents

M. Claude GATIGNOL, Député
M. Pierre LASBORDES, Député
M. Jean-Yves LE DÉAUT, Député
M. Jean-Claude ÉTIENNE, Sénateur
M. Pierre LAFFITTE, Sénateur
M. Claude SAUNIER, Sénateur

Députés

M. Jean BARDET
M. Christian BATAILLE
M. Claude BIRRAUX
M. Jean-Pierre BRARD
M. Christian CABAL
M. Alain CLAEYS
M. Pierre COHEN
M. Francis DELATTRE
M. Jean-Marie DEMANGE
M. Jean DIONIS DU SÉJOUR
M. Jean-Pierre DOOR
M. Pierre-Louis FAGNIEZ
M. Claude GATIGNOL
M. Louis GUÉDON
M. Christian KERT
M. Pierre LASBORDES
M. Jean-Yves LE DÉAUT
M. Pierre-André PÉRISSOL

Sénateurs

M. Philippe ARNAUD
M. Paul BLANC
Mme Marie-Christine BLANDIN
Mme Brigitte BOUT
M. Marcel-Pierre CLÉACH
M. Roland COURTEAU
M. Jean-Claude ÉTIENNE
M. Christian GAUDIN
M. Pierre LAFFITTE
M. Serge LAGAUCHE
M. Jean-François LE GRAND
Mme Catherine PROCACCIA
M. Daniel RAOUL
M. Ivan RENAR
M. Henri REVOL
M. Claude SAUNIER
M. Bruno SIDO
M. Alain VASSELLE

Office parlementaire d'évaluation des choix scientifiques et technologiques

(OPECST)

_____

« La biométrie »

_____

Compte rendu de l'audition publique du Jeudi 4 mai 2006

Assemblée nationale – salle Lamartine

Table des matières

ASSEMBLÉE NATIONALE

RÉPUBLIQUE FRANÇAISE

SÉNAT

OFFICE PARLEMENTAIRE D'ÉVALUATION DES CHOIX SCIENTIFIQUES ET TECHNOLOGIQUES

Mesdames, Messieurs,

L'Office parlementaire d'évaluation des choix scientifiques et technologiques a décidé, lors de sa réunion du 10 mai 2005, de confier à M. Christian Cabal, député, l'organisation d'une audition publique sur la biométrie pour assurer le suivi du rapport sur « les méthodes scientifiques d'identification des personnes à partir des données biométriques et techniques de mise en œuvre » qu'il avait présenté en juin 2003.

Cette audition publique s'est tenue le 4 mai 2006 à l'Assemblée nationale.

L'Office étant un outil d'aide à la décision, il se devait de dresser un état des lieux des nombreuses évolutions, voire des bouleversements, qu'ont connus les applications de la biométrie, trois ans après la publication d'un rapport qui déjà avait contribué largement au débat par ses propositions visant à réguler l'usage de ces applications, dans la perspective d'un développement et d'une diversification de ces technologies.

Cette démarche s'est également inscrite dans le cadre des modalités d'évaluation de l'Office qui a pris l'habitude d'organiser des auditions publiques, ouvertes à la presse, réunissant une pluralité d'acteurs, pour préparer les rapports qui lui sont confiés, en assurer le suivi et répondre à un besoin de débat public sur des problèmes scientifiques et technologiques d'une actualité majeure.

En organisant cette audition et en publiant son compte-rendu, l'Office parlementaire prend ainsi directement part au renforcement du rôle du Parlement sur des problématiques de régulation du développement des sciences et des techniques.

Office A.N. : 233 boulevard Saint Germain 75355 Paris Cedex 07 SP – tél : 01 40 63 88 10 – 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

L'après-midi d'audition, centrée sur l'évolution de la biométrie depuis trois ans, a permis de dresser un état des lieux précis des recherches, des avancées scientifiques et technologiques, et d'apprécier l'impact et l'efficacité des applications industrielles, tant en France qu'à l'étranger.

Elle a, en outre, conduit à une réflexion approfondie sur les grands enjeux des applications des systèmes d'identifications biométriques aux titres de séjour, passeports, et cartes d'identité. Les débats ont souligné l'intérêt de ces technologies pour lutter contre la fraude documentaire et améliorer les systèmes de contrôle aux frontières, même si les analyses étaient parfois divergentes. Des thématiques, comme l'utilisation de puces lisibles à distance dans les documents d'identité ou la gestion des bases de données, ont été abordées. Elles ont fait apparaître les risques potentiels d'atteinte aux libertés que soulèvent certaines applications de la biométrie et la nécessité de concilier les évolutions technologiques avec la protection des libertés publiques.

Diverses opinions se sont exprimées sur l'impact sociologique, psychologique et juridique des technologies de l'identification, révélant la volonté du public d'être informé sur la façon dont elles sont et seront utilisées et son intérêt pour ces innovations.

Henri REVOL
Président

Claude BIRRAUX
Premier Vice-Président

Office A.N. : 233 boulevard Saint Germain 75355 Paris Cedex 07 SP – tél : 01 40 63 88 10 – 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

LA BIOMETRIE

Présidence de

M. Christian CABAL, Député de la Loire

Ouverture par
M. Christian CABAL, Député

Ouverture par M. Christian CABAL, Député de la Loire

J'ai le plaisir de vous accueillir dans cette salle Lamartine où nous allons commencer l'audition prévue dans le cadre des travaux de l'Office parlementaire d'évaluation des choix scientifiques et techniques (OPECST). L'OPECST est une structure commune à l'Assemblée nationale et au Sénat dont le but est d'enrichir et de faire progresser la réflexion au plan scientifique et technologique, d'effectuer des analyses et des évaluations sur des domaines précis, et de formuler des propositions ayant notamment des incidences sur le plan législatif et/ou réglementaire.

Cette audition constitue donc un point d'étape de la réflexion de l'Assemblée nationale et du Sénat concernant la problématique de la biométrie. Celle-ci s'inscrit dans le suivi du rapport que j'avais eu l'honneur et le plaisir de présenter, il y a près de trois ans, après une série d'auditions et de visites auprès des différentes instances en charge de ces questions, ou utilisant ce système ou ces procédures. Ce rapport a pris en compte des observations datant parfois de quatre à cinq ans. Depuis, on constate des évolutions de niveau moyen au plan technique, mais de niveau plus élevé au plan des incidences sociologiques et réglementaires, en raison des préoccupations singulièrement aiguës des pouvoirs publics concernant la prévention du terrorisme et de différentes formes de délinquance. On observe donc une évolution plus ou moins rapide de plusieurs dispositions, même si l'Europe de l'Ouest reste singulièrement en retard dans ce domaine par rapport aux États-Unis et à d'autres pays du continent américain.

Cette audition publique constitue un état des lieux, qui permettra d'éclairer les pouvoirs publics qui sont sur le point de proposer des évolutions législatives, notamment sur la carte nationale d'identité dont les perspectives de modification approchent à grands pas. II était nécessaire, trois ans après, de procéder à une mise à jour des différents domaines ayant trait à la biométrie, d'autant que depuis 2003, la fraude documentaire s'est développée dans de multiples circonstances et situations.

On pourra ainsi éclairer la représentation parlementaire qui a récemment présenté deux rapports s'inscrivant de façon conjointe et connexe sur la problématique de la biométrie : celui de M. Pierre Lasbordes, Député, vice-président de l'OPECST, remis au Premier ministre sur la sécurité des systèmes d'informations et celui de M. Jean-René Lecerf, Sénateur, rapporteur de la mission d'information du Sénat sur l'identité intelligente et le respect des libertés. Le législateur a la volonté d'améliorer les textes déjà existants pour renforcer les moyens de lutter contre les différentes formes de délinquance liées à l'identité et à

l'expression de cette identité. Des initiatives concernant l'utilisation de techniques biométriques ont émergé dans presque tous les pays développés et dans des pays moins développés. Il était indispensable de faire le point, sur un plan scientifique, des différentes techniques, et des observations auxquelles elles ont donnés lieu.

Les recommandations du rapport

Le rapport que j'ai rendu préconisait plusieurs recommandations. Les premières notamment tendaient à définir un cadre législatif plus précis et les conditions dans lesquelles les autorités publiques pouvaient être habilitées à utiliser et à accéder à des traitements comportant des données biométriques.

Une deuxième série de préconisations visait à garantir l'information du Parlement sur les différentes techniques et sur les différents systèmes de données biométriques, afin de disposer d'un mécanisme qui assure des éléments de contrôle des dispositifs au niveau parlementaire.

Le troisième point consistait à créer un observatoire associant les différents acteurs et utilisateurs concernés afin d'assurer d'une part, une veille juridique et technique et, d'autre part, l'information du public.

Il s'agissait enfin de mettre en place un organisme de concertation entre les structures publiques et privées avec des moyens techniques et financiers de fonctionnement, en faisant réaliser par des laboratoires indépendants les évaluations nécessaires.

Trois ans plus tard, où en sommes-nous ?

Concernant les principes que je viens d'énoncer, on n'a pas constaté d'évolution particulièrement notable : les choses sont demeurées pour une bonne part plus ou moins en l'état, presque anarchiques, sans mise en œuvre de l'organisation que nous avions imaginée. On est resté en attente de données comparatives notamment, car il eut été très improductif que chaque pays, aussi grand soit-il - à part les États-Unis qui font ce qu'ils ont envie de faire et se préoccupent peu de ce qui se passe dans le reste du monde - développe ses propres systèmes sans un minimum de compatibilité entre eux et d'harmonisation dans les critères d'appréciation et de mesure de leur fiabilité.

Comme la biométrie existe et existera, il serait dommage qu'on évacue l'enjeu industriel qui est particulièrement important ; il n'est pas toujours agréable d'évoquer le marché, mais nous sommes dans une société marchande. Il existe donc un marché, même si celui-ci obéit à des dispositions réglementaires dans beaucoup de cas. En France, le secteur de la biométrie est l'un des rares à occuper une position très respectable au plan économique, au travers de plusieurs entreprises qui ont pu développer des systèmes biométriques dont l'efficacité est reconnue dans les différents et nombreux marchés du monde. Cela fera l'objet d'une présentation sur le plan de l'économie et de l'emploi, qui en est la conséquence directe.

Pour ces multiples raisons et afin de garder une position en pointe dans le domaine international, induisant une activité économique qu'il convient de soutenir, une nouvelle évaluation « à distance » du rapport sur la biométrie a été proposée. En outre, des décisions formelles devront être prises à une échéance proche dans le domaine de la carte nationale d'identité, décisions qui seront éclairées par l'expérience acquise dans la mise en œuvre de nouveaux dispositifs, comme le passeport électronique. Celui-ci a connu ces derniers mois une actualité assez complexe liée à des contestations du dispositif d'impression de ces documents. De nombreux citoyens qui devaient et voulaient aller dans un pays exigeant ce type de passeport ont rencontré des difficultés.

Telles sont les raisons pour lesquelles nous avons organisé cette audition d'actualisation. Nous allons entamer la première table ronde où interviendront le Professeur Cabanis, Madame Dorrizzi, Madame Deloison, Monsieur Didier, Monsieur Robin, Monsieur Mordini, Madame Lahalle et Monsieur de Mengin. Cette première table ronde est centrée sur les questions scientifiques et technologiques, les nouveautés et les évolutions significatives depuis le rapport précédent.

Je vais donc donner la parole à mon collègue, le Professeur Cabanis, de l'Université Paris VI « Pitié-Salpêtrière » et du centre hospitalier des Quinze-Vingts. Président de la Société de Biométrie Humaine et membre de l'Académie nationale de médecine, il est également l'auteur de plusieurs ouvrages sur l'ophtalmologie et la neuroradiologie et vient de créer un groupe de travail « Génétique et biométrie », à l'Académie nationale de médecine.

Les évolutions scientifiques et technologiques

Professeur Emmanuel-Alain CABANIS, Président de la Société de biométrie humaine (SBH)

Monsieur le Président, Monsieur le Député, cher collègue en médecine universitaire et ami, Professeur Christian Cabal, prendre la parole en premier est un honneur. Je vous en remercie. A moi revient donc l'agréable et premier devoir de vous rendre l'hommage que vous méritez, à la hauteur de votre rapport de 226 pages, publié en juin 2003. Vous nous avez impressionnés, mes collègues et moi, par la qualité de l'efficacité et de la vitesse adaptatives déployées par votre équipe et vous même, dans la réalisation de ce travail. Cette somme, scientifiquement vérifiée et remarquablement multi disciplinaire, associe des spécialistes venus de multiples horizons.

La confiance que vous avez témoignée, dès votre première invitation (2002), puis renouvelée dans cette belle salle (2003), au petit groupe que nous sommes (section Hommes et milieux du Centre national de la recherche scientifique) nous touche et nous encourage. Nous sommes quelques centaines en France, beaucoup plus en Europe et sur les autres continents à vivre le quotidien de cette discipline, née vers 1860, avec le très illustre Professeur Paul Broca (1824-1880), membre de l'Académie nationale de médecine et chirurgien des Hôpitaux de Paris, sous le nom d'« anthropologie ». Je me plais à saluer, ici, le Professeur Raymond Ardaillou, membre du bureau et Secrétaire Adjoint de l'Académie nationale de médecine (ANM), qui, acceptant votre invitation, représente cette institution auprès de l'OPECST. Académicien également, au XIX^{ème} siècle, le Professeur Paul Broca a apporté au monde sa découverte d'une première localisation reconnue sur le cortex cérébral, celle du langage articulé dont la perte est appelée « aphasie ». Issus de son premier laboratoire d'anthropologie, quelques uns de ses élèves créeront, plus tard, la Société de Biotypologie (1932, Professeur Henri Laugier) devenue Biométrie humaine. Vos collaborateurs et vous-même avez reconnu notre Société de biométrie humaine grâce à notre site Internet et au moteur de recherche « *Google* », au moment même où votre Mission « biométrie » prenait corps. Nous vous en remercions.

Le terme « biométrie » associe le vivant (bios) à sa mesure (metron) chez l'humain. Le XIX^{ème} siècle et Paul Broca utilisent le décimètre, le compas, des instruments en bois, la balance, puis le crayon, la gomme et des équations qu'ils

imaginent. Le Professeur Philippe Monod-Broca[1], chirurgien des Hôpitaux de Paris et membre de l'Académie nationale de médecine comme son arrière-grand-père, l'un de nos proches maîtres, est le récent auteur d'un ouvrage où il décrit, d'une plume alerte et captivante, ce siècle prolifique dont les lumières construiront notre modernité, dans tous les champs du savoir. L'auteur de ces lignes, collaborateur de ce livre, par sa culture anatomique initiale et sa présence à l'émergence du scanner à rayons X (1972) puis pionnier de l'Imagerie par Résonance Magnétique (IRM) française (1983), se trouve, plus que d'autres, en situation de deviner combien la numérisation et l'informatique changent radicalement la mesure du corps humain. Les fichiers et les technologies de l'information et de la communication augmentent encore la puissance de cette « mise en chiffres » du corps de l'homme. Elles sont « la potion magique » d'une nouvelle connaissance qui vient compléter la connaissance alpha numérique de la biologie. La médecine y mérite une place de conducteur (de l'homme malade à l'homme sain) et de vigile, au nom de la morale pour certains, de l' « éthique » pour d'autres.

Ainsi la SBH souhaite-t-elle encore contribuer à l'efficience de ce rapport de l'OPECST, indicateur et porteur d'un avenir sûr. Avec intérêt et ardeur nous nous présentons aujourd'hui à ce premier suivi du travail initial. Au cours des trois années écoulées, la SBH a organisé son X^{ème} colloque intitulé : «Biométrie Humaine et Reconnaissance Individuelle, Aspects anthropologiques, méthodologiques, et législatifs » (Paris, 17-19.10.03). Le numéro 2004-22-3-4 du journal Biométrie Humaine et Anthropologie en rapporte quelques extraits[2]. En 2005, la participation active au débat « Carte d'identité électronique et biométrie », guidée par le Forum des Droits sur l'Internet[3] pour le programme INES, a permis de faire valoir le point de vue, peut être neuf, de « l'électronique, premier rempart de la liberté individuelle, aujourd'hui »[4]. Ainsi, notre groupe a-t-il avancé dans trois directions, grâce à l'aide précieuse de l'Académie nationale de médecine, en particulier. Comme médecins, donc, et comme biométriciens, nous avons imaginé d'avancer dans trois domaines, ceux des mathématiques, de l'anatomie et de la médecine.

Les mathématiques et les statistiques, un premier champ d'action.

L'occasion nous fut donnée d'avancer dans le domaine des statistiques, à propos des grands nombres. Même si nombreux sont ceux qui sont plus compétents que nous ne sommes dans ce domaine difficile, nous osons affirmer notre admiration pour cet ensemble de démarches dites « Six Sigma », normes

[1] Monod-Broca Philippe – Paul Broca un géant du XIXème siècle, Vuibert, Paris, 2005
[2] Cabanis Emmanuel Alain – La biométrie humaine en 2005 : du millimètre au nanomètre. Editorial. Biométrie Humaine et Anthropologie, 2004, 3-4, 125-126
[3] Cabanis Emmanuel Alain – Identité électronique : le paradoxe de la liberté, aujourd'hui. Participation au 5ème débat national, Rennes, 11.05.05, www.foruminternet.org
[4] Cabanis Emmanuel Alain – Identité électronique : le paradoxe de la liberté, aujourd'hui. Participation au 5ème débat national, Rennes, 11.05.05, www.foruminternet.org

qualitatives industrielles nées il y a 80 ans aux États-Unis[5]. Elles y ont prospéré et se sont étendues au monde, comme à tous les secteurs de l'activité humaine moderne. De cette notion de critères de qualité industrielle, hier, on extrait, aujourd'hui, des leçons de quantification de la qualité du travail accompli, jusque dans l'exercice de la médecine et de la chirurgie. Mon équipe va commencer à travailler avec un nouveau système d'imagerie par résonance magnétique, deux fois plus puissant que celui utilisé jusqu'à présent. L'outil statistique de contrôle de qualité dit «Six Sigma » doit nous faire gagner en performances, pour le patient, pour la recherche et pour la gestion. Nous avons travaillé et avancé à travers beaucoup de leçons. Or, cette normativité de l'écart type appliqué à une réduction de la variabilité trouve un vaste champ d'application en biométrie humaine. Plusieurs mathématiciens le conviennent. « Six Sigma » doit s'appliquer aux normes à venir, obligatoires, et qui ne peuvent que s'annoncer à travers les utilisations modernes de la biométrie humaine. Cette contribution des outils statistiques qui nous environnent est une pierre à l'édifice de sécurité et de liberté que construit ce rapport.

L'anatomie du corps humain, aujourd'hui référence quotidienne : un dictionnaire.

Le deuxième domaine où nous souhaitons contribuer à l'exhaustivité de ce rapport est l'anatomie du corps humain. Cette biométrie humaine concerne le corps de l'homme et sa mesure. C'est ce qu'on apprend dans les facultés de médecine depuis les années cinquante et soixante, et que depuis les années quatre-vingts on n'apprend plus du tout, pour des raisons variées. Il se trouve que, alors étudiant en «biométrie et anatomie quantitative» à la faculté, il y a 30 ou 35 ans, quand je préparais l'agrégation d'anatomie, je fus marqué car passionné. Cela laisse des traces. Dans le contexte de ce succès contemporain de la biométrie, une partie du grand public s'intéresse davantage au corps de l'homme, avec de multiples conséquences heureuses, au plan de la santé publique. Mais des bases manquent, et l'absence de références élémentaires en anatomie humaine pèse son poids d'errements inutiles et coûteux. Quelle est la différence entre les mots « crâne » et « tête » ? Je consacre du temps à expliquer à des médecins généralistes, spécialistes ou d'autres que la « tête » est la « région anatomique supérieure du corps humain, avec une limite inférieure passant etc. » et que le « crâne » est le « squelette de la tête », tout simplement, et, non pas, une quelconque « boîte » etc... Bref, on ne fait pas des radiographies du crâne mais de la tête. Il est évident que la rigueur statistique du chiffre affiché doit prolonger la précision sémantique.

En effet, une fois précisée sa nomenclature, cette anatomie devient préoccupation quotidienne de nos concitoyens. Au-delà de la maladie, la femme et l'homme en bonne santé se préoccupent plus que jamais de l'équilibre de leur corps. Il leur faut des références pour leur alimentation, le suivi de leurs mesures,

[5] Cabanis Emmanuel Alain, Couturier Nadir, Pivet Nicolas, Pineau Jean-Claude – La méthode statistique « Six Sigma » (6 s), du contrôle de qualité industrielle à l'optimisation des performance en médecine. Biométrie humaine et anthropologie, 2006, 24, 1-2 (à paraître)

comme le montre la préoccupation de « l'indice de masse corporelle » dans le grand public, leurs vêtements etc... Ainsi, l'Institut français du textile et de l'habillement (IFTH) est-il à l'origine d'une campagne nationale de mensuration des français qui a débuté en 2002[6]. Cet important et sérieux travail français de biométrie, à grande échelle, offre la solution industrielle moderne d'adaptation aux variantes individuelles des formes et dimensions pour les vêtements. Cet exemple illustre la part croissante de cette mesure du corps humain, comme la presse s'en est fait l'écho, avec l'aide notamment, de la belle exposition à la Cité des sciences et de l'industrie « Biométrie, le corps identité », représentée parmi nous aujourd'hui.

Telles sont les raisons qui nous ont fait commencer, il y a déjà près de 11 mois, un « travail de dictionnaire », dans lequel pourraient (si Dieu nous prête vie) être rassemblées les données essentielles en matière de définitions des mots en biométrie et mesures du corps de l'homme. Nous savons faire, car nous avons hérité d'une tradition, amplifiée et renouvelée depuis le XIX^{ème} siècle. Croyant dans l'efficacité de ce deuxième travail, nous y progressons. Nous avons commencé à croiser les fichiers que nous connaissons, comme scientifiques, chercheurs, médecins et comme anatomistes. Nous espérons déposer auprès de cette commission des documents qui apporteront à chacun un outil de certitude dans les techniques biométriques utilisées.

Le groupe de travail « Identification des personnes par les techniques de la biométrie et de la génétique » à l'Académie nationale de médecine

Cette troisième et ultime convergence, nous la devons au Professeur Raymond Ardaillou, membre du bureau de l'Académie nationale de médecine, mon illustre aîné qui nous fait l'honneur et l'amitié de sa présence aujourd'hui. Il a imaginé de constituer un groupe de travail à l'Académie nationale de médecine, destiné à faire progresser ce dossier. Nous lui devons d'avoir lié le domaine de la réflexion biométrique à celui de la médecine en général, à commencer par la génétique, source d'avancées considérables dans la connaissance statistique du corps humain (ADN). Ce groupe de travail doit se mettre en place avant l'été. A partir de la rentrée, sont prévues des auditions qui se dérouleront à l'Académie, pendant l'année universitaire. Si nous savons tous qu'un iris change de couleur en fonction de certaines pathologies, que la stature se modifie aux heures de la journée comme avec l'âge, que les cheveux et phanères changent de couleur, il est indispensable que le contrôle de la connaissance médicale pathologique puisse s'exercer sur cette référence croissante au corps humaine.

Cette troisième opportunité est la plus importante des trois présentées ici. Notre Président a accepté de garder un oeil attentif sur l'activité de ce groupe de travail. L'an prochain, une fois achevées les auditions, sous la houlette du Professeur Ardaillou et de votre serviteur, la rédaction du rapport final débutera. Il sera soumis à l'assemblée générale des membres de l'Académie nationale de

[6] IFTH campagne nationale de mensuration 2006, www.ifth.org/mensuration

médecine, pour un avis favorable que nous espérons le plus large possible. Nous y travaillons. La fin de ce rapport comportera, probablement, différentes recommandations destinées aux Pouvoirs Publics, puisque telle est la vocation de l'Académie.

M. Christian CABAL, Député de la Loire

Je vous remercie pour cette présentation complète. Je donne maintenant la parole à Madame Bernadette Dorizzi, Responsable de l'équipe de recherche « interactions pour le multimédia » de l'Institut national des télécommunications.

Mme Bernadette DORIZZI, Responsable de l'équipe de recherche « interactions pour le multimédia » de l'Institut national des télécommunications (INT)

Je me réjouis également de présenter les enjeux et les nouveautés de la biométrie.

Nous travaillons dans le cadre d'une équipe de recherche au sein du GET, Groupe des écoles de télécommunication. Ce groupe est une fédération d'écoles d'ingénieurs et de management, au sein de laquelle s'est constituée une équipe multi sites de recherche en biométrie, travaillant dans le projet « Bio Identité ». Une de nos particularités est de travailler à la fois sur les différentes techniques de la biométrie (modalités de la biométrie : voix, visage, forme de la main, empreintes digitales, algorithmes biométriques, problèmes d'évaluation, et multi modalité) et sur les aspects sociologiques et juridiques, qui sont fondamentaux dans ce domaine dans lequel on ne peut pas dissocier les avancées techniques, des avancées en termes d'acceptabilité et d'usage.

Nous sommes soutenus par le GET, qui dépend du Ministère de l'industrie, et divers projets européens et nationaux. L'un d'eux est le projet BioSecure, réseau d'excellence européen qui fédère le travail de 30 institutions académiques universitaires européennes et essaye de conférer une certaine visibilité à la recherche en biométrie, en particulier face aux collègues américains ou chinois qui possèdent une certaine force actuellement dans ce domaine. J'essayerai d'aborder plusieurs thèmes, sachant qu'il ne me sera certainement pas possible d'être exhaustive dans cet exposé.

J'évoquerai d'abord la validation des algorithmes et des systèmes biométriques. C'est, il me semble, un point assez important aujourd'hui, sur lequel on manque encore de cadre de travail, de transparence et surtout d'outils d'évaluation. Ensuite, j'aimerais aborder le thème de la multi modalité, c'est-à-dire

l'utilisation conjointe de plusieurs modalités biométriques. Dans les données apparaissant sur les passeports, on préconise d'avoir à la fois l'enregistrement de la photo numérisée et des empreintes digitales. La question est donc de savoir, en quoi il est intéressant d'avoir ces deux modalités et comment on peut les utiliser. C'est à mon avis, une question qui reste encore ouverte. Puis j'évoquerai le futur, les perspectives de la biométrie : quels seront les systèmes biométriques dans 10 ou 20 ans et je tenterai, ensuite, d'illustrer les travaux conduits actuellement à l'INT autour des approches sociologiques. Je terminerai en abordant l'expérience du comité d'industriels et d'utilisateurs du réseau BioSecure. C'est à mon sens une expérience intéressante de travail collaboratif d'industriels, d'universitaires et d'utilisateurs.

L'évaluation

J'ai beaucoup aimé la présentation du Professeur Cabanis à propos des statistiques car la variabilité est une des caractéristiques de l'humain et donc toute évaluation biométrique sera nécessairement statistique. Chacun sait qu'un système biométrique va faire des erreurs. Je crois qu'il est fondamental de pouvoir évaluer les performances des systèmes biométriques, et pas uniquement en termes d'erreurs, mais surtout de pouvoir comparer plusieurs systèmes biométriques entre eux.

Pour les industriels et les chercheurs académiques, il est fondamental de pouvoir disposer de jeux d'essais biométriques significatifs pour apprécier la performance de leurs travaux. Pour les prescripteurs, il est fondamental de disposer de jeux d'essais non publics, et d'une méthodologie d'évaluation, pour apprécier en toute neutralité les solutions proposées. Pour les utilisateurs, à part certaines organisations étatiques, il est particulièrement lourd et difficile d'évaluer les performances réelles des solutions proposées. Dès qu'il est question de statistique, on évoque le problème des bases de données, et d'accès à des données pour pouvoir produire des résultats. On sait aussi que plus on a de données, mieux c'est, et plus fiables seront les résultats. Il est difficile d'avoir suffisamment de données et nous avons aussi besoin de données pour mettre au point des algorithmes, pour tester de nouvelles biométries. S'il est question demain de biométrie de l'oreille ou d'autres biométries, il faudra bien évaluer les performances des systèmes que l'on fabriquera.

Une des voies dans lesquelles nous travaillons dans le réseau BioSecure est de produire des évaluations biométriques multimodales de l'identité. Un premier travail a été conduit l'été dernier. Pendant un mois, des chercheurs du réseau et des chercheurs étrangers ont collaboré pour tenter de mettre à disposition et de définir une plate-forme d'évaluation qui comprenne à la fois des bases de données, des protocoles d'évaluation et des algorithmes de référence, afin d'être en mesure de comparer les algorithmes entre eux. C'est un travail actuellement en cours de finalisation et qui devrait permettre de donner au marché de la biométrie des outils d'évaluation *a priori* des algorithmes, c'est-à-dire des outils de base contenus dans le système biométrique.

Un de nos objectifs importants est de préparer pour 2007 des évaluations internationales de grande taille, un peu à la manière du *National institute of standards and technology* (NIST) aux États-Unis qui propose des évaluations régulières sur la vérification par le visage ou par l'iris. L'objectif est d'essayer de mettre en place de telles évaluations dès 2007, en particulier dans le cadre de la multi modalité. L'intérêt est aussi d'améliorer le niveau de la recherche : aujourd'hui de nombreux laboratoires testent leurs algorithmes sur leurs données propres, ce qui n'est pas très approprié, en termes de validité des résultats de recherche. De plus, il s'agit de pouvoir évaluer des scénarios, sans forcément se heurter dès le départ à la lourdeur de la mise en œuvre. L'aspect comparatif et l'aspect indépendance sont également importants : en tant qu'organisme de recherche, nous pouvons nous prévaloir de n'avoir pas d'intérêts commerciaux et de jouir d'une certaine indépendance. Pour l'instant, il n'y a pas de test de système opérationnel prévu dans BioSecure, mais c'est un point très important. Mes collègues industriels vont pouvoir développer cet aspect par la suite.

La multi modalité : avantage ou handicap ?

La multi modalité est l'utilisation conjointe de plusieurs biométries différentes. Elle correspond, par exemple, à l'enregistrement des données visage et empreintes digitales dans un passeport. Elle permet d'améliorer les performances de chaque système pris indépendamment. Les performances de la modalité visage seule ne sont pas acceptables. L'usage de deux modalités permet aussi de réduire les taux d'impossibilité d'acquisition : pour les empreintes ou le visage, on ne peut pas acquérir la modalité pour certaines personnes. De plus, ceci permet également de rendre plus difficile la falsification, ce qui est important, l'objectif étant d'évaluer réellement les taux de fausses acceptations, ce qui est quasi impossible à effectuer en opérationnel si on ne dispose pas d'une deuxième biométrie de contrôle.

Cependant la multi modalité pose quelques problèmes. Dans une mise en œuvre à grande échelle, elle est plus coûteuse puisqu'il faut plusieurs capteurs ; elle implique des conditions d'acquisition plus difficiles. Il convient de savoir quel prix on veut payer. Encore aujourd'hui, un problème de stratégie d'utilisation se pose : comment va-t-on utiliser ces deux biométries ? Est-ce toujours intéressant en termes de gains de performance ? Les utilisera-t-on de manière alternative ? Cela reste encore des questions ouvertes sur lesquelles des recherches sont nécessaires.

Quelles biométries dans le futur ?

La biométrie n'est pas du tout un domaine fermé, elle est en constante évolution ; ce qui est stimulant pour les chercheurs. Certes, il existe des systèmes dont on parle plus que d'autres, mais on constate qu'apparaissent toujours de nouvelles modalités et des perspectives intéressantes pour des voies nouvelles. Ce domaine nécessite donc une veille technologique permanente. Pour la mise en place de normes, cela peut constituer un handicap. Cette normalisation doit être

progressive car on est toujours obligé d'envisager le futur alors qu'on est en train de poser plusieurs principes. Il s'agit pourtant d'une nécessité dans ce domaine en constante évolution.

Il est possible que la multi modalité ne soit pas la solution universelle. En revanche, il apparaît très clairement que, même si on n'utilise pas forcément plusieurs modalités, on cherchera à utiliser différentes sources d'informations au sein d'une même modalité. Aujourd'hui, on n'envisagerait plus de système d'empreintes avec un seul doigt. Partout, on s'est tourné vers l'utilisation de plusieurs doigts, de 2 à 10. C'est l'utilisation redondante ou complémentaire d'informations qui rendra plus fiable la biométrie. Ceci n'est pas étonnant, comme l'a rappelé le Professeur Cabanis ; au niveau du corps humain, une information redondante est nécessaire.

Ainsi, on trouve pour le visage, de nombreux travaux sur l'intérêt ou pas d'utiliser une prise de vue de type 3D, en complément ou en remplacement de celle en 2D. De nouveaux capteurs d'image et d'empreintes digitales, apparaissent. A l'avenir toutes ces évolutions risqueront encore une fois de modifier aussi bien les performances que le paysage biométrique en général.

La recherche de l'Institut national des télécommunications sur les usages de la biométrie

L'approche suivie est sociologique et essaye d'étudier la façon dont la biométrie affecte le rapport entre l'État et les individus, comme la confiance qui fonde ce rapport. Quelques bribes de résultats commencent à apparaître et montrent qu'il y a apparemment, une bonne acceptabilité des techniques biométriques ; les gens ne manifestent pas de rejet *a priori* envers ces techniques.

En revanche, de profonds bouleversements apparaissent qui entraînent une requalification de la notion d'identité ; en particulier l'idée que la notion d'identité est désormais accessible à la mesure. C'est important. On observe le passage d'une reconnaissance sociale par l'environnement uniquement (comme dans un village où on est reconnu sans avoir besoin de présenter de papiers), à la validation automatique, à l'aide de documents numériques d'identité. L'individu est quelque part un peu dépossédé, ou en tout cas son identité change un peu de nature et de signification.

Un autre point mis à jour par nos sociologues concerne le lien entre les systèmes biométriques et les notions de gestion de flux, et d'automatisation que l'on retrouve aussi dans l'entreprise, et qui touche forcément la relation de l'employé à son travail et à sa légitimité. Plusieurs terrains d'enquête ont été explorés : cantines scolaires (contours de la main), Air France et Aéroports de Paris (accès aux zones réservées), usages de l'ordinateur personnel. Le dernier en date est celui de l'expérimentation sur les visas biométriques (BIODEV) pour lequel nos chercheurs ont pu aller sur le terrain et ont produit un rapport assez intéressant.

L'expérience du comité d'industriels et utilisateurs du réseau BioSecure

L'expérience menée actuellement au sein de ce réseau européen BioSecure est celle d'un travail coopératif entre des industriels du domaine comme Motorola, Sagem, Philips, Softpro, Agnitio, Atmel, A4vision, Viisage, des utilisateurs comme le groupement des cartes bancaires ou les aéroports de Paris, le Forum Biométrique Européen (EBF), Telecom Italia et plusieurs universités comme le GET, University of Kent, University of Magdeburg, CWI.

Ces acteurs travaillent ensemble au sein d'un comité d'industriels et d'utilisateurs et se réunissent environ tous les trois mois pour des présentations techniques et surtout pour des débats et des présentations conjointes autour de la biométrie. L'idée étant de s'influencer mutuellement afin que la recherche menée par les universitaires ne soit pas découplée des besoins des utilisateurs ou des industriels et inversement, que les industriels et les utilisateurs puissent donner leur avis sur le programme de travail des réseaux académiques, et aussi relayer les résultats de BioSecure vers les industriels et les utilisateurs.

En guise de conclusion, je soulignerai l'importance d'avoir une recherche interdisciplinaire, internationale et une coopération entre chercheurs, industriels et utilisateurs.

M. Christian CABAL, Député de la Loire : Je vous remercie beaucoup pour cette présentation très claire, tout à fait analytique et synthétique à la fois. Je vais maintenant donner la parole à Madame Yvette Deloison, Chargée de recherche au CNRS, membre de l'équipe « Dynamique de l'évolution humaine » dans le cadre des études sur « Individus, population et espèce », associée à la chaire du Collège de France « paléoanthropologie et préhistoire », dirigée par le Professeur Yves Coppens et intervenante dans différentes universités au plan international.

Mme Yvette DELOISON, Chargée de recherche au CNRS, unité de dynamique de l'évolution humaine

Je vous remercie et serai très brève, le Professeur Cabanis ayant exposé tous les projets qui concernent la biométrie. En tant qu'anthropologue, nous collaborons depuis une dizaine d'années, et il me fait l'honneur et la confiance de m'associer à ses projets. Je n'aurai rien à ajouter dans ce domaine.

Je donnerai seulement une information concernant l'intérêt de la biométrie et notamment des nouvelles méthodes (scanners, IRM…) dans l'étude de la paléontologie humaine, dans l'étude de l'origine de l'homme. Ces méthodes

permettent actuellement de progresser de plus en plus pour arriver à des consensus qui n'existent absolument pas pour le moment.

M. Christian CABAL, Député de la Loire : Je vais donner la parole à Monsieur Bernard Didier, Directeur scientifique et du développement des affaires (division sécurité de Sagem Défense Sécurité, (désormais groupe SAFRAN), l'un des fondateurs des technologies et des recherches liées à la biométrie et une des personnalités les plus actives dans le domaine des applications biométriques dans la vie courante notamment des entreprises.

M. Bernard DIDIER, Directeur scientifique et du développement des affaires (division Sécurité de Sagem Défense Sécurité, groupe SAFRAN)

Monsieur le Président, Mesdames, Messieurs, je pense que je vous laisserais insatisfaits si je réduisais mon intervention aux seules évolutions scientifiques et techniques de la biométrie. Aussi articulerai-je mon propos en cinq parties : les marchés, la technologie, la mise en œuvre de la biométrie, le respect des données personnelles et enfin les standards.

Les marchés

Les marchés biométriques gouvernementaux et ceux des équipements personnels ont connu un développement plus important que ceux à usages industriels et commerciaux. A cet égard, avant de revenir sur des points plus spécifiques, je souhaiterais faire trois commentaires généraux :

1. En 2004, pour la première fois, des cabinets d'analyses marketing américains ont annoncé un marché mondial des systèmes biométriques à usage civil plus important que les marchés à usage policier, tendance que nous avions déjà signalée en 2003.

2. S'agissant du marché grand public, contrairement à la tendance que je voyais lors de la précédente audition, la biométrie par empreintes digitales est en train de se développer plus rapidement que les autres biométries. C'est ainsi qu'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.

3. S'agissant des applications strictement industrielles et commerciales, la difficulté à apprécier des retours d'investissement, l'absence de textes réglementaires, ne laissent possibles des usages que dans des applications sous

prescription gouvernementale. Cela a été le cas avec les systèmes de contrôle d'accès par empreintes digitales à l'aéroport de Paris.

Les marchés gouvernementaux doivent être analysés en tenant compte de quatre remarques :

1. Pris sous diverses contraintes internes ou externes, des gouvernements ont retardé des projets de cartes d'identité biométriques au profit de passeports électroniques ou de visas biométriques.

2. L'usage de la biométrie, comme technologie permettant de gérer des grands flux aux frontières sans failles de sécurité, devient le ferment d'une biométrie mondiale inter opérable.

3. Les programmes de cartes d'identité devraient faire l'objet d'une deuxième vague de modernisation, y compris dans des pays tels que l'Angleterre qui ne possèdent pas aujourd'hui de cartes d'identité.

4. D'une manière générale, les États sont plus rapides à inclure la biométrie sur des visas ou des cartes de résidents de citoyens étrangers que sur les passeports de leurs propres ressortissants. C'est ainsi que les États-Unis ont imposé l'acquisition de deux empreintes digitales et du visage pour tous les visiteurs étrangers à partir de janvier 2005.

En conclusion, les marchés gouvernementaux restent toujours les moteurs du développement d'une industrie de la biométrie. Les marchés industriels et commerciaux, pris en tenaille entre des utilisations personnelles et des utilisations gouvernementales, se mettront probablement à la biométrie dans une dernière phase.

De manière plus précise, sur le plan géographique, on constate :

1. Aux États-Unis

La biométrie est devenue sur ces trois dernières années une technologie de souveraineté et de sécurité nationale : l'attitude du gouvernement en la matière est plus proche des pratiques de la défense que des activités commerciales classiques. C'est ainsi que l'on observe des procédures de classification des sociétés, des délivrances d'habilitations pour le personnel, la définition notamment par *la National security agency* (NSA) de profils de protection qualifiant les produits de vérifications biométriques, des subventions ciblées envers certaines sociétés sur des systèmes de recherche ou des donations permettant à des pays étrangers de s'équiper de solutions biométriques qualifiées. Enfin, l'ensemble de ces opérations est sous-tendu et structuré par une montée en puissance remarquable de l'office de normalisation, le NIST *(National institute of standards and technology)* qui, en plus de son travail de normalisation, a constitué des bases de tests de millions de données biométriques en provenance du Département d'État, du Département du Homeland Security, du FBI et de différentes autres organisations. Ces bases de

données ont permis au NIST de conduire plus de sept campagnes lourdes d'évaluation comparative d'algorithmes de reconnaissance du visage, d'iris et d'empreintes digitales.

Au-delà de l'emblématique programme *« US VISIT »* (*Visitor and immigrant status indicator technology*), l'administration fédérale est en train de mettre en œuvre, plus vite qu'en Europe, la biométrie dans le cadre de programmes de gestion d'identité des personnes tels que TWIC *(Transportation worker identification credential)* pour les travailleurs d'activités de transport, l'ancien programme CAC *(Common access card programm)* ou le nouveau programme PIV *(Personal identity verification)*, pour les employés fédéraux et leurs contractants, ou encore des opérations dites de « *background check* », c'est-à-dire de contrôle d'identité biométrique en préalable à toute autorisation de travail sur une activité sensible. Ces programmes serviront probablement de modèles dans une seconde phase aux entreprises qui travaillent avec le gouvernement, puis seront utilisés par l'ensemble des acteurs économiques et industriels.

Enfin, pour terminer ce bref tour d'horizon américain, l'année 2006 devrait être celle du lancement par le FBI d'un programme de rupture technologique : le développement d'une nouvelle génération de systèmes de traitement automatique d'empreintes digitales permettant de gérer plusieurs centaines de millions de personnes.

2. En Europe

Sous l'impulsion de la Direction générale JLS (Justice Liberté et Sécurité), de grands programmes voient le jour et se dessinent. Ces programmes portent essentiellement aujourd'hui sur une gestion plus efficace des frontières de l'Union avec des projets comme BMS (*Biometric matching system)*, BIODEV *(Biometric data experimented in visas)* par exemple ou encore l'annonce pour 2008 de passeports biométriques à empreintes digitales. Sur ce dernier point l'Europe, contrairement aux États-Unis, traitera de la même façon ses citoyens et ses visiteurs. En revanche, pour des raisons structurelles évidentes, l'Europe mettra probablement plus de temps à articuler les projets biométriques de gestion d'identité comparables aux programmes américains TWIC ou PIV. Enfin, sujet préoccupant, l'expérience passée de BIOTEST a démontré la difficulté de mettre en place une autorité d'évaluation réellement indépendante, si l'Europe n'accepte pas de soutenir l'indépendance financière d'une telle structure.

3. En France

Sous l'impulsion remarquable du Ministère de l'Intérieur, accompagné par le Ministère des Affaires Etrangères, des projets pilotes significatifs ont été lancés : c'est le cas du programme PEGASE (Programme d'expérimentation et de gestion automatisée et sécurisée) ou encore du programme BIODEV. Il est important de souligner que ces deux programmes ont permis à la France

d'acquérir en moins de trois ans une notoriété internationale en matière de grands programmes biométriques.

En revanche, deux points négatifs sont à relever : le manque de lisibilité des différents programmes de cartes nationales d'identité et l'absence toujours remarquée de procédures qualifiantes, c'est-à-dire de critères communs aux produits biométriques.

En effet, contrairement au gouvernement allemand, qui a publié en août 2005 des critères communs de profils de protection, de mécanismes de vérification des équipements biométriques, rejoignant ainsi l'Angleterre et les États-Unis, la France, malgré le constat qui avait été fait en 2003, n'a toujours pas progresser en la matière.

Les technologies

Comme il fallait s'y attendre, les technologies moins matures que les empreintes digitales ont entamé une courbe de progrès rapide significatif. Pour illustrer mon propos, je prendrai comme exemple ce que notre société fait en la matière.

S'agissant de la reconnaissance du visage, sur les grandes bases de données depuis 2002, nos équipes ont divisé par deux le taux d'erreur. Les programmes d'évaluation comparative conduits aux États-Unis ou encore les programmes européens « 3D Face », dont nous assurons la coordination, ont clairement pour objectif de mettre le visage à un niveau de performance comparable à celui des empreintes digitales. Le niveau de performance auquel nous sommes arrivés permet d'envisager dès aujourd'hui des systèmes permettant d'identifier des visages « à la volée » ou encore d'identifier des personnes recherchées dans des contextes opérationnels particuliers. Ces travaux ont déjà des retombées opérationnelles, ils nous permettent notamment, comme nous le verrons un peu plus tard, de gérer l'accès biométrique aux frontières de l'Australie.

En ce qui concerne la reconnaissance de l'iris, entre 2003 et 2005, les progrès ont été encore plus remarquables :

- le taux d'erreur a été ramené à 1 % à l'enregistrement,

- les faux rejets ont été divisés par un facteur deux et parfois quatre, pour être ramenés entre 1 et 2 %,

- le temps de vérification a été réduit de 12 à 4 secondes.

La technologie actuelle permet de reconnaître aussi des iris « à la volée », à plusieurs mètres de distance, et résout le problème ergonomique auquel était confrontée cette technologie. Après quelques programmes significativement opérationnels, le dernier challenge pour les années à venir sera celui du prix des capteurs.

L'empreinte digitale est maintenant arrivée à un stade de maturité qui ne suscite pas de remarques particulières dans ce tour d'horizon rapide.

Enfin, il faut noter le développement en Asie de la technologie de reconnaissance des veines qui, sous réserve de validation, pourrait se substituer à terme à la technologie de reconnaissance par la longueur des doigts.

La mise en œuvre de la biométrie

Notre société a le privilège d'avoir gagné trois programmes de contrôle aux frontières particulièrement visibles, à savoir : la Grande-Bretagne, l'Australie et la France.

En Grande-Bretagne, il s'agit du contrôle aux frontières des cinq plus grands aéroports par analyse automatique de l'iris. Dans cette approche, le voyageur passe sans présenter de titre de transport et pratiquement « les mains dans les poches », si vous me permettez l'expression. Techniquement, l'opération biométrique consiste à acquérir l'iris, en extraire le gabarit et à le comparer à une base de données dont la capacité est de deux millions de personnes. L'ensemble de l'opération se fait en un temps moyen de 4 secondes, pour un temps total moyen de passage aux frontières de 20 secondes.

En Australie, il s'agit du contrôle aux frontières par reconnaissance du visage, le temps de passage total, incluant la lecture du passeport biométrique, la reconnaissance du visage et l'ouverture de la porte, est en moyenne de 6 secondes. En matière de stricte performance biométrique, le taux de reconnaissance constaté en vérification est de 96 à 98 %.

En France, il s'agit du contrôle aux frontières par reconnaissance des empreintes digitales dont le détail sera certainement abordé dans la deuxième partie de l'audition.

De ces trois programmes, nous tirons un enseignement commun intéressant. La maturité des technologies biométriques est confirmée. En revanche, les difficultés rencontrées se situent davantage dans l'adaptation de ces technologies à l'environnement, c'est-à-dire plus précisément dans l'ergonomie, l'optimisation en temps d'un processus global pouvant nécessiter l'adaptation de l'organisation existante -comme nous l'étudions en Australie par exemple-, les aspects juridiques, l'information et l'éducation des utilisateurs sur le plan technique etc… A notre surprise, l'effort n'est pas à faire sur la biométrie mais sur l'état de l'art de la détection qu'une personne est seule quand elle passe une frontière. Sur tous ces sujets, le fait que nous soyons nos propres développeurs de technologies biométriques a particulièrement servi pour faire progresser les solutions ; si je pouvais résumer, on « ne plaque pas » la biométrie sur une organisation existante, on l'intègre.

En matière de reconnaissance de visage, nous constatons maintenant depuis un an, une tendance de plus en plus marquée de différentes polices dans le

monde à mettre en place des projets pilotes de reconnaissance des visages. Cette tendance, dans un contexte international où les passeports posséderont de plus en plus souvent des visages numérisés, devrait soutenir le développement de la reconnaissance faciale.

Sur un plan plus général, les opérations mettant en jeu plusieurs biométries sont encore rares. Le seul exemple significatif est celui du système électoral du Mexique, que nous mettons en place, et qui gérera à terme les empreintes digitales et les visages de 72 millions de personnes, ce qui en fait le plus grand système biométrique multimodal civil au monde.

Enfin, sur les tendances à plus long terme, les systèmes biométriques deviendront de plus en plus importants en taille. 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. En complément à ces grands systèmes, on observe une montée en puissance des terminaux biométriques mobiles.

La protection des données personnelles

Je me bornerai volontairement aux aspects techniques du sujet. L'apparition de concepts de bases centrales de données biométriques pouvant respecter la protection de données personnelles- bases de données dites à liens faibles et qui ont fait l'objet d'une présentation plus détaillée dans le rapport de l'an dernier de Monsieur le Sénateur Lecerf, ici présent, sur l'identité intelligente- modifie profondément l'analyse *a priori* que l'on peut avoir sur la mise en œuvre de systèmes biométriques.

Je suis tout aussi convaincu que la mise en place d'une démarche de qualification sur des critères communs pourrait enfin créer un lieu de dialogue original entre sécurité et respect des données personnelles.

Enfin, pour terminer ce volet, j'évoquerai la notion de code unique qui fait l'objet de nombreux travaux de recherche dans le monde, dont l'objectif est d'être capable d'extraire un code identifiant unique, stable, d'une donnée biométrique. Sur ce sujet comme d'autres, nous avons fait beaucoup de progrès au sein de Sagem. Cette notion, à mon point de vue, pourrait déboucher vers une véritable révolution systémique du concept de biométrie.

Les standards

J'évoquerai le timide réveil en Europe sur les standards avec la création, en 2003, d'un *focus group* au Centre européen de normalisation (CEN) consacré à la biométrie, suivie de la création d'un Comité Biométrique à l'AFNOR en 2004. Comme annoncé lors de ma précédente audition, 2005 a vu la sortie du standard de gabarit biométrique « *Minutiae* » des empreintes digitales. Dès 2004, le Bureau international du travail (BIT) a conduit des certifications d'interopérabilité de ce format dans le cadre du projet de la carte d'identité des marins. Cette année enfin, le NIST a confirmé, au travers de l'évaluation *Minutiae interoperability exchange*

(MINEX), l'interopérabilité de gabarits d'empreintes digitales « Minutiae » avec des performances opérationnelles acceptables. Il est à noter que cette évaluation place Sagem comme ayant la seule technologie qui offre la meilleure garantie d'interopérabilité, tant pour la construction des gabarits que pour les comparaisons.

Tel est ce qui nous semble intéressant de rapporter sur les évolutions de la biométrie sur ces trois dernières années

M. Christian CABAL, Député de la Loire : Je pense qu'il n'y aura pas énormément de questions techniques, puisque vous avez survolé les divers domaines sur lesquels on peut avoir des appréciations ou des expériences différentes. Je vous remercie pour cette présentation.

Nous allons passer tout de suite « à la maison d'en face », si j'ose dire, avec l'intervention de Monsieur Philippe Robin, Directeur technique de Thales Security System, qui va nous donner sa vision et son approche complémentaire à celle de Sagem.

M. Philippe ROBIN, Directeur technique, Thales Security System

Monsieur le Président, Mesdames et Messieurs, mon exposé s'articulera en plusieurs paragraphes : les évolutions des technologies, les applications et la sécurisation. Nous retrouvons donc les problématiques que chacun évoquait ici. Auparavant, je présenterai rapidement l'activité de Thales en matière de protection des personnes, des sites et des biens.

Thales Security Systems possède plusieurs activités dans ce domaine :

- la sécurité des sites, des événements : systèmes de sûreté et supervision intégrés, contrôle d'accès, vidéosurveillance, détection d'intrusion,

- les centres opérationnels de sécurité, et systèmes de détection de produits nucléaires, radiologiques, biologiques (NRBC)

- les centres de contrôle et commande : PC police, pompier, urgence, plate-forme de gestion de crise, détection des risques et menaces NRBC,

- identification : solutions identitaires sécurisées,

- sécurité des systèmes d'information : conseil, gestion du risque sécuritaire, solutions intégrées de sécurité, gestion de services de sécurité (MSS),

- conseil en gestion du risque sécuritaire,

- certification et l'évaluation de composants de sécurité.

Dans ces différents domaines d'activité, la biométrie est une composante essentielle. Au niveau identitaire, un système identitaire sécurisé, tel qu'il est conçu par Thales concerne la gestion et la personnalisation de documents (graphiques ou électriques), les signatures électroniques (PKI), de l'acquisition à la gestion d'état civil, en passant par l'identification biométrique jusqu'à la délivrance, et le contrôle du document. Ceci s'accompagnant évidemment d'une logistique de services de maintenance et formation.

Les principales références

Il s'agit à la fois des références purement identitaires, où il n'y a que des documents, comme la France, le Maroc, la Serbie, le Liban, la Pologne et d'autres pays dans lesquels nous avons également développé un système d'identification biométrique comme le Kenya, le Cameroun, la Namibie et l'Ethiopie.

Qu'est-ce qu'un système d'émission de documents biométriques ? Cela suppose :

- des matériaux (papier, plastique, puces, éléments de sécurité, hologramme, impression offset),

- un centre de personnalisation graphique et électrique pour la mise en forme des fichiers, la personnalisation et la sécurisation,

- un fichier de production pour l'état-civil, la biométrie, la signature et évidemment de l'acquisition.

Lors de l'acquisition, on prend les empreintes, la photo, on pourrait prendre l'iris. C'est le premier endroit où l'on voit apparaître la biométrie. Ces fichiers d'acquisition remontent à l'état civil, suivant l'organisation du pays. L'organisation du pays peut mettre en place une identification biométrique, grâce au fameux AFIS *(Automatic fingerprint recognition system)*, avec base de données qui permettent d'identifier une personne parmi des millions d'autres pour être sûr qu'on ne donne pas deux documents à une même personne, avec des identités différentes.

Une fois que l'État a pu identifier correctement les personnes à qui il veut donner le document, les fichiers de production contenant de la biométrie avec la signature de l'État interviennent, car il faut sécuriser et valider cette démarche. Ces fichiers sont mis en forme dans le centre de personnalisation graphique et électrique. Il faut personnaliser, sécuriser, et cela s'effectue dans ce centre approvisionné par les papiers, plastiques, puces et éléments de sécurité visuels. Il faut continuer à pouvoir contrôler ces documents d'identité à l'œil nu. Ce centre fabrique les documents biométriques (cartes ou passeports). Le contrôle de l'intégrité du document et de sa biométrie intervient ensuite pour vérifier que le porteur est bien le bon. L'exemple d'actualité est le passeport biométrique français

fabriqué à l'Imprimerie nationale dont le procédé est calqué sur ce schéma. Thalès a fourni le système de personnalisation.

L'évolution des technologies

L'empreinte digitale est toujours la technologie phare, en termes de performance et de déploiement. Monsieur Didier l'a indiqué, l'interopérabilité des formats de codification est en train d'arriver. Si on se projette un peu plus loin, on pourrait envisager une sécurisation totale pour faire en sorte qu'ils ne sortent jamais du document du porteur : le document aurait éventuellement son capteur.

Le visage est l'objet d'une technologie dynamisée par les passeports biométriques puisque, maintenant que la photographie numérisée du visage est intégrée dans la puce, ce sera de plus en plus utilisé. Ceci conduira à une amélioration des performances par la prise en compte des éléments tridimensionnels pour introduire de plus en plus la biométrie dans le domaine vidéo.

Pour l'iris les vitesses de contrôle étaient relativement longues il y a quelques années, mais les portiques permettent d'aller maintenant beaucoup plus vite.

S'agissant des veines, modalité sans contact, l'intérêt de cette acquisition reste à démontrer.

En ce qui concerne la forme de la main, l'évolution est réduite pour l'instant ; elle est utilisée pour les contrôles d'accès.

L'utilisation de la voix demeure très difficile pour l'instant mais de nombreux travaux sont menés sur les performances en ambiance bruitée.

L'ADN reste aussi une modalité biométrique qui doit effectuer beaucoup de progrès en matière d'automatisation pour obtenir un résultat rapide.

La multi modalité

Comme l'a indiqué Madame Bernadette Dorrizi, la combinaison de plusieurs types de biométrie permet d'augmenter les performances globales d'une part, et de diminuer les taux d'impossibilité d'enrôlement d'autre part, ce qui conduira à développer notamment les algorithmes de fusion de données et de prises de décision : ce sont des perspectives de recherche universitaire importantes et riches. Au niveau des capteurs : certains capteurs existent déjà puisque le téléphone portable est déjà une caméra et un microphone. Des possibilités sont donc offertes.

L'évolution des applications

On peut classer les applications en trois grands domaines.

- Le domaine identitaire : il nécessitera des performances, puisque l'on devra traiter des bases de 60 millions et 100 millions de personnes. Si, de surcroît, on estime qu'il y aura un flux de personnes interrogées de l'ordre de 10 000 à 20 000 par jour, on doit obtenir des taux de précision extrêmement élevés. Il s'agit bien d'identifier des personnes afin d'éviter le changement ou l'usurpation d'identité et de contrôler leur identité.

- Le contrôle d'accès : cette deuxième application, se décline de deux manières : l'accès physique aux sites sensibles (entreprises, aéroports, banques) ou l'accès logique à un ordinateur, à un PDA, à un téléphone, à un distributeur de billets. Le contrôle d'accès ira probablement dans le futur vers la fluidité : on voudra faire passer les personnes de plus en plus vite. Telle est la piste d'évolution.

- La surveillance : on cherche de plus en plus à être en mesure d'identifier des personnes recherchées. Il est probable que les événements terroristes ne soient pas anodins quant au développement de cette application. On tendra à faire évoluer les technologies vers l'identification à distance et en mouvement, ce qui est complètement différent d'un dispositif où une personne vient poser son doigt sur un capteur.

Quelles sont les évolutions des technologies par rapport aux applications ?

On connaît bien l'identification, le contrôle d'accès au niveau de l'authentification pour les empreintes digitales. L'utilisation du visage, qui était plus dans notre jargon « un contre un », va passer vers l'identification soit seule, soit en multimodal et sera utilisée lors de la surveillance à partir de caméras vidéo.

L'iris donnant de bons résultats est plutôt utilisée dans les systèmes d'identification, voire de contrôle d'accès. Si on le capte à distance (et on est en train d'y arriver, il existe déjà plusieurs expériences), cette technique sera également peut-être utilisée pour la surveillance.

La forme de la main restera probablement utilisée pour le contrôle d'accès.

Pour l'usage de la configuration des veines, il faut peut-être attendre un peu.

Si la reconnaissance vocale s'améliore nettement, elle pourra être utilisée dans le domaine de la surveillance.

L'ADN, qui nécessite un laboratoire peut s'améliorer au niveau rapidité de l'usage, mais les échéances devraient être beaucoup plus lointaines.

On constate que lors de l'identification et du contrôle d'accès, les personnes sont coopératives : vous leur avez demandé leur identité et vous la vérifiez face à des personnes de bonne foi. Vous leur avez demandé leurs

identifiants biométriques, il faut donc les sécuriser. Pour la surveillance, il s'agit de trouver des personnes recherchées, c'est donc un environnement non coopératif. Il faudra résoudre un problème de gestion de la preuve pour ne pas accuser à tort une personne qu'on aurait repérée.

La sécurisation des données biométriques

Il y a deux possibilités pour sécuriser les données biométriques.

- les données sont stockées sur le document du porteur : plusieurs applications se suffisent avec cette manière de stocker. Le contrôle d'accès peut être fait de cette façon. Les mécanismes de sécurisation sont très similaires à ceux qui existent déjà avec un code PIN. Des mécanismes dans les puces sont déjà utilisés pour sécuriser sérieusement les fichiers.

- les données sont stockées dans la base : il s'agit là d'un sujet extrêmement important, comme l'ont rappelé les orateurs précédents. Il existe déjà des solutions technologiques pour résoudre ces questions. D'abord les bases anonymes : la base n'étant pas nominative, on détecte simplement que la personne était déjà dans la base, mais il n'y a pas d'identification. Afin d'empêcher les accès malveillants à la base, la sécurisation physique est une solution qui fonctionne très bien : la base n'est pas reliée au réseau, donc les échanges s'effectuent par transit des données sur des supports physiques, sans accès au réseau et donc sans inquiétude sur les possibilités d'accès à distance. Ce système est peut-être un peu rudimentaire mais il fonctionne très bien. La sécurisation logique : des liaisons unidirectionnelles à partir de diodes optiques permettent d'envoyer des informations dans une base tout en étant sûr qu'elles ne repartent pas dans l'autre sens. L'on gère ainsi le sens des transmissions dans un système.

La sécurisation des données ne s'effectue pas au hasard. Il convient de définir des politiques de sécurité. Des organismes de certifications évalueront la sécurité de ces bases, de ces capteurs ou de ces données, les testeront et proposeront aux personnes responsables de la sécurité des systèmes d'information de donner l'accréditation. Il s'agit d'organismes bien connus, comme la direction centrale de la sécurité des systèmes d'information (DCSSI) et l'ensemble des centres d'évaluation de la sécurité des technologies de l'information (CESTI) en France.

M. Christian CABAL, Député de la Loire : Je vous remercie pour cette présentation très claire et synthétique. Je donne la parole au Professeur Emilio Mordini, qui nous fait l'honneur de nous rejoindre depuis Rome. Il est médecin et psychanalyste, professeur de bioéthique à l'Ecole de Médecine de l'Université de Rome « la Sapienza ». Directeur du Centre pour la science, la société et la citoyenneté, il coordonne les programmes européens *Bioethical implication of globalization* (BIG) et Éthique des technologies d'identification biométriques (ÉTIB) ou *Biometric identification technology ethic* (BITE). Je vous donne la parole.

Professeur Emilio MORDINI, Coordinateur du projet européen sur l'Éthique des technologies d'identification biométrique (ÉTIB)

Je remercie les organisateurs de m'avoir invité. Je suis ici à double titre : en tant qu'expert qui s'occupe depuis plusieurs années de problèmes de l'identité , et en tant que coordinateur d'un projet de recherche, financé par la Commission européenne, sur l'Éthique des technologies d'identification biométrique, le projet ÉTIB.

Etant psychanalyste, je travaille depuis plusieurs années sur les problèmes de l'identité – et par le biais de ceux-ci, je suis parvenu à la biométrie. Il est vrai que nous vivons dans une période où la question de l'identité est cruciale. Il est intéressant de noter que le développement de la biométrie correspond à une période d'identité multiple, changeante.

Le projet ÉTIB

Ce projet réunit neuf partenaires : leur objectif est d'aider l'industrie comme les décideurs publics et surtout de préparer une future initiative au niveau européen. Ce projet, coordonné par le Centre pour la Science, la Société et la Citoyenneté de Rome que je dirige, regroupe trois universités (La Sapienza de Rome, l'Université de Lancaster, l'Université Erasmus de Rotterdam), deux entreprises européennes (la société Humanscan, allemande et la société Optel, polonaise), une organisation internationale qui est directement impliquée dans le débat politique sur l'utilisation des passeports biométriques (l'Organisation Internationale des Migrations), l'Institut Européen de Bioéthique de Bruxelles et un des plus grands groupes mondiaux de certification des technologies biométriques, *l'International Biometric Group*.

Le projet se développe à travers divers rencontres en Grande-Bretagne, en Italie, en Allemagne, en Suisse et en Pologne. Nous avons eu quatre rencontres en 2005 : « Génétique et biométrie », « Vie privée et biométrie », « Questions liées aux migrants », « Le contexte industriel européen » et, dernièrement, en mars 2006, « Les futures technologies ».

L'impact du projet

Le projet ÉTIB a eu jusqu'à présent un fort impact sur le débat européen et mondial. Il a déjà engendré deux conférences s'y rapportant. La première s'est tenue les 13 et 15 décembre à Bruxelles, organisée par la Commission Européenne pour lancer une plate-forme de confrontation entre les États-Unis et l'Europe sur les questions d'éthique sociale et de politique de la biométrie. En septembre prochain un atelier de travail organisé dans le cadre du programme de l'OTAN se

tiendra en Israël sur le thème *« Security, identity and democracy »*. Jusqu'à présent nous avons eu plus de 72 articles dans les journaux et les magazines au cours de cette première année et demie de travail, en six langues et pratiquement dans tous les pays européens. Le projet a été présenté au cours du forum des Comités éthiques nationaux européens le 25 novembre 2005 à Londres, et déjà trois Comités éthiques nationaux ont déjà placé la biométrie parmi leurs priorités d'étude : il s'agit de l'Italie, du Danemark et de Malte.

La consultation publique

La consultation publique lancée au mois de mars par le projet – et qui restera ouverte jusqu'à la mi-juin de cette année – a déjà collecté environ 4000 réponses, toutes très qualifiées au plus haut niveau de compétences politiques et techniques. Il s'agit d'un résultat extraordinaire, surprenant même pour nous, membres du consortium. La France, avec les États-Unis, la Belgique (probablement des personnes qui travaillent dans les structures européennes) et l'Italie, est le pays qui a envoyé le plus de réponses. La plupart des personnes estime que le public n'est pas correctement informé. Les experts sont favorables à la promotion d'initiatives telles que celle d'aujourd'hui, c'est-à-dire des conférences publiques, des auditions, des conférences de consensus pour tenter d'impliquer le public dans ces débats. Le projet s'achèvera par une conférence à Bruxelles en février 2007.

L'identification

Souvent ceux qui s'occupent de questions identitaires, soupçonnent, voire méprisent, ceux qui s'occupent d'identification. On dit que l'identification est une activité de policiers et les philosophes ne s'occupent pas d'identification, ils s'occupent d'identité. Pour celui qui vient de la psychanalyse et de la philosophie, l'identification n'est pas *a priori* une activité aussi noble que celle consistant à se préoccuper de problèmes d'identité. C'est la première réaction, mais je considère que c'est une erreur car dans notre culture le problème d'identité et le problème d'identification sont posés en même temps. Ceux qui encore de temps en temps fréquentent l'un des livres qui ont fondé notre culture, l'Odyssée, le savent bien – la distance entre identité et identification n'est pas si grande. Quand Ulysse arrive à Ithaque, lorsqu'il débarque et se présente sous l'aspect d'un mendiant, c'est un étranger, sans identité ; mais il porte une marque sur son corps, une cicatrice qui permettra à sa nourrice Euryclée de le reconnaître.

Les marques du corps

C'est justement des marques du corps que s'occupe la biométrie. La reconnaissance de l'autre est tout d'abord intérieure. L'étranger n'est pas seulement toujours parmi nous, mais, comme nous l'apprennent Albert Camus et Julia Kristeva, il est toujours en nous, dans nos corps. Le corps est le chiffre qui permet d'affronter le sujet de la biométrie, les enthousiasmes qu'elle engendre, les craintes qu'elle peut révéler.

La section aurea

A cet égard, la manière dont la biométrie a été présentée à la Cité des sciences de Paris est remarquable. Parmi les antécédents de la biométrie, on retrouve la section aurea, le canon de Polyclète, la progression harmonique et toutes les tentatives de Platon à Leibniz faites par la culture occidentale pour trouver l'harmonie cachée, le chiffre, l'algorithme sous les apparences.

Auschwitz

Le couple corps / biométrie, toutefois, doit également nous rappeler la marque de l'infamie, la seule fois où, au cours du siècle dernier, des êtres humains ont été connus seulement par un numéro imprimé dans leur chair : Auschwitz.

Il y a ceux qui, comme le philosophe Giorgio Agamben, soutiennent que la biométrie nous conduit tous vers une spoliation des identités, vers une nudité face au pouvoir, que l'on pourrait comparer à celle des prisonniers des camps de concentration.

C'est entre ces deux extrêmes - Platon et Agamben,- entre la biométrie en tant qu'entreprise de civilisation ou en tant qu'outil de contrôle, que s'inscrit le débat d'aujourd'hui.

Corps et Biométrie

Le corps est la clé pour comprendre les questions politiques et éthiques de la biométrie. Ceci est vrai au moins selon trois points de vue : tout d'abord il faut comprendre le rapport entre le corps et les données biométriques ; puis il s'agit de savoir si la biométrie peut dévoiler les secrets du corps ; enfin il faut déterminer si le corps peut être la source d'une nouvelle forme de droit.

Le corps informatisé

L'un des sujets les plus débattus de ces dernières années a été celui du corps informatisé. Tous les jours, des milliards d'informations qui nous concernent et qui concernent notre corps voyagent le long des réseaux électroniques. Notre corps virtuel est démembré et reconnu d'innombrables fois dans les ruisseaux des mille banques de données auxquelles nous appartenons. Mais quel est le statut du corps informatisé ? Quel est le statut des renseignements collectés par un système biométrique et stockés dans une banque de données ? La question est beaucoup plus politique qu'elle ne le semble à première vue. Il suffit de penser à la controverse entre les États-Unis et l'Europe sur la détention des données biométriques des passagers d'avions.

Il existe une tension fondamentale entre ceux qui soutiennent que les données engendrées par le corps sont elles-mêmes un corps (autrement dit, que le corps virtuel, le corps qui s'étend tout au long du réseau télématique, bénéficie des mêmes droits et protections que le corps physique, localisé dans l'espace et dans le

temps), et ceux qui pensent que les données engendrées par le corps doivent être considérées comme des produits, sur lesquels on peut continuer à exercer un droit de propriété, mais qui ne bénéficient pas du même statut et des mêmes protections que le corps humain. Il y a également ceux qui, sur une position intermédiaire, proposent de traiter les données biométriques de la même manière que les images photographiques ou télévisées. On comprend bien que l'un ou l'autre choix entraîne une série considérable de conséquences juridiques et pratiques. En outre, il ne faut pas oublier que des cultures différentes traitent le corps de façon différente, et que le corps féminin est traité différemment que le corps masculin.

Le corps médicalisé

Une autre question concerne ce que les systèmes biométriques sont en mesure de révéler par rapport au corps. Il s'agit d'un sujet qui, généralement, fait enrager les techniciens qui se donnent du mal à expliquer que non seulement aucun système biométrique n'a jamais été conçu pour produire des informations médicales confidentielles, mais que, entre autres, il y aurait des moyens beaucoup plus efficaces pour obtenir les mêmes informations. Ces objections sont ingénues, elles ne prennent pas en compte le fait que ces systèmes se développent de manière exponentielle.

A ses débuts, la biométrie est née comme technique médicale : en effet, toutes les techniques d'étude instrumentale médicale ne sont que des formes de biométrie. Même en faisant simplement une comparaison entre les données biométriques stockées d'un individu et les données obtenues au moment de l'authentification ou de l'identification, on peut en tirer de nombreuses informations.

Tous les systèmes biométriques, en outre, tendent également à vérifier que la source des données est « vivante ». La vérification que la source des données est vivante implique souvent qu'il faut tester sa réactivité. À partir du moment où l'on teste la réactivité, on fait un profil fonctionnel de ce système vivant donné, autrement dit, on produit des données ayant une importance biomédicale.

Il est facile de prévoir, malgré toutes les assurances contraires, qu'à moyen ou long terme certaines biométries seront utilisées également à des fins médicales et que l'on sera tenté d'exploiter cette possibilité à des fins illicites ou, du moins, non éthiques.

Ce n'est pas davantage une raison pour s'opposer à la biométrie pas plus que de s'opposer à l'industrie automobile prétextant qu'une voiture peut renverser une personne ; mais c'est un bon motif pour se rappeler que, dans la biométrie, aussi bien que dans la circulation urbaine, nous avons besoin d'un code de la route.

Le corps et la citoyenneté

Le noyau central de la "question biométrique" consiste toutefois à placer le corps au centre d'une nouvelle forme de droit et de citoyenneté. Le concept actuel de citoyenneté et d'identité civile est relativement récent. Des siècles durant, la communauté locale avait été le garant principal de l'identification personnelle. Au début du XVI^{ème} siècle, la transmission du nom avait trouvé une première stabilisation dans les registres paroissiaux des naissances. Ce système naissant avait subi une grave crise due à la rupture provoquée par la Réforme. Les protestants ne comparaissaient pas sur les registres paroissiaux catholiques et dans de nombreux pays de l'Europe continentale le réseau d'inscription civile basée sur les structures ecclésiastiques s'était interrompu. Entre-temps, les processus de migrations internes aux pays européens s'accentuent et la capacité d'identification liée à l'appartenance à une communauté préexistante s'affaiblit.

En France le système des registres des naissances devient progressivement étatique et, dès la moitié du XVII^{ème} siècle, il remplace totalement le système de constatation de l'identité par le biais de témoins. D'autres pays européens suivent un double régime – religieux et civil – tandis qu'en Grande Bretagne le système d'identification de l'état civil reste flou jusqu'à la Première Guerre mondiale**.** Cependant, c'est en France, en août 1794, qu'est promulguée la première loi en Occident obligeant chaque individu de se conformer au nom qui lui avait été assigné lors de la naissance et inscrit sur le registre des naissances. Durant ces années-là, la France affirmait également un nouveau concept de citoyenneté basé sur les droits universels de l'homme. La continuité entre naissance et citoyenneté, telle que la postule la Déclaration des droits de l'Homme et du citoyen, est le fondement de l'État-nation. La souveraineté des États fondés sur la nation confirme donc notre statut de citoyen porteur de la dignité humaine. Tout se tient.

Ce n'est donc pas par hasard que les processus de mondialisation qui ont investi le monde au cours de la deuxième moitié du XX^{ème} siècle, en mettant en crise l'État nation, ont également mis en crise la prétention que l'identité civile doit être certifiée par les États.

Trois événements importants marquent le passage du système identitaire basé sur les États nationaux à l'actuelle situation de transition.

Tout d'abord le développement de la mobilité humaine ; un seul chiffre : chaque jour l'Autriche tout entière vole au-dessus de nos têtes. Tous les jours environ 8 millions de passagers dans le monde entier envahissent les routes aériennes. Dans l'ensemble, environ 800 millions de personnes sont en mouvement sur notre planète, environ 22 millions de réfugiés, 10 à 15 millions de sans-papiers, 698 millions de voyageurs internationaux, 70 à 80 millions de travailleurs migrants et au moins 700.000 trafiquants.

Mais le mouvement physique n'est pas le seul ni le principal facteur : en 2004 le nombre de connexions Internet a dépassé le milliard. Ce réseau

électronique a besoin d'un système d'identification pour fonctionner et créer du commerce.

Puis il y a un troisième facteur : l'apparition sur la scène mondiale d'économies émergentes, de pays en voie de développement, a entraîné la multiplication des pièces d'identité peu fiables.

Le droit à l'identité

De nos jours encore, dans certains pays, l'enregistrement à l'état civil lors de la naissance n'est pas obligatoire. Chaque année, en Asie ou en Afrique, naissent 50 millions d'enfants non enregistrés. Au Pakistan, par exemple, après le tremblement de terre, on a constaté que des millions d'enfants n'étaient pas enregistrés. Dans notre société opulente, on évoque souvent le droit à l'anonymat, mais on oublie que tout d'abord, le droit à l'identité existe. Sans une identité légale, aucun droit politique, civil ou social ne peut être reconnu et exercé : il n'y a pas d'anonymat, s'il n'y a pas d'abord une identité.

Biométrie et citoyenneté

Jusqu'ici l'État-nation constituait un référent stable: en son sein la dimension du local prenait une extraordinaire importance, conférant aux membres de la société leur point d'ancrage privilégié: le triangle culture territoire identité. Or, les migrations, d'une part, les flux électroniques et médiatiques de l'autre, ont bouleversé l'ordre régnant. La biométrie est la réponse au problème de la vérification de l'identité, tel qu'il est posé de manière originale par la *global network society*. Si la biométrie devient le standard, le concept même d'identification est destiné à changer. Cela n'aura plus d'importance de lier un individu à un prénom ou à un nom, à une ville et à une nation, à une date et à un lieu de naissance, pas plus qu'à un sexe ou à une profession : toutes ces données ne seront plus essentielles. Il suffira de le relier à l'une de ses caractéristiques physiques.

Citoyenneté biologique

En fait, la question générale posée par le recours à la biométrie concerne au premier chef la détermination des identités dans un contexte de plus en plus déterritorialisé. Autrement dit, nous sommes face à un nouveau concept de citoyenneté : la citoyenneté biologique. Le citoyen mondialisé issu du déficit de légitimité des nations découvre son identité en tant qu'entité biologique, que pur individu humain.

Si la biométrie est si cruciale aujourd'hui, c'est parce qu'elle révèle le caractère en définitive illusoire des identités certifiées par l'État-nation. La crise actuelle de la citoyenneté est l'expression de la crise de l'appartenance à une communauté politique et à un État.

Un nouvel étalon

La biométrie peut avoir un rôle structurant dans la constitution de nos sociétés, un rôle social au moins aussi important, sinon plus, que ses rôles techniques apparents. La biométrie peut jouer le rôle tenu par l'or durant le XVII^{ème} siècle, celui qui a vu la naissance des grandes nations européennes. Le XVII^{ème} siècle avait eu besoin de créer un étalon monétaire pour fonder les transactions financières sur une valeur reconnue internationalement. La question de l'étalon se pose à l'aube du XVII^{ème} siècle quand l'or, affluant depuis les mines du Nouveau Monde, provoqua la richesse de l'Espagne et du Portugal, avant de profiter aux autres États européens qui surent mieux le capter, tels la France et la Grande-Bretagne. Puis, l'or a servi d'étalon (*Gold Standard*), après les accords de Bretton Woods, en 1944, entre les différents pays du monde, jusque dans les années soixante-dix. En 1971, les États-Unis d'Amérique suspendirent la convertibilité du dollar or, et les accords de la Jamaïque contractés par les pays du FMI supprimèrent l'étalon de change or.

La mondialisation contemporaine a besoin de trouver un nouvel étalon pour fonder les transactions financières, humaines, culturelles - des personnes, des données, et des marchandises - dans les routes réelles et virtuelles du réseau mondial. La biométrie peut devenir cet étalon.

Un nouveau système de citoyenneté

On trouve là une nouvelle tension entre ceux qui pensent à la biométrie en tant - et seulement - qu'outil pour la sécurité, et ceux qui la conçoivent en tant qu'outil pour promouvoir la participation et l'inclusion. La biométrie peut donc être au service d'une «bonne» mondialisation mais également être un outil pour réaffirmer des localismes, des formes de xénophobie.

Le défi d'aujourd'hui, face à l'érosion de la souveraineté des États fondés sur la nation, consiste à fonder un nouveau système de citoyenneté (et de droits) à l'échelle mondiale. Relever sérieusement ce défi et en faire une raison de progrès collectif est l'un des objectifs stratégiques du projet ÉTIB.

M. Christian CABAL, Député de la Loire : C'était passionnant, je vous remercie. Je crois que tout l'auditoire a été passionné par votre intervention qui se situe évidemment dans un domaine largement différent des autres, mais tout aussi intéressant. Madame Marie-Pierre Lahalle et Monsieur Aymard de Mengin, respectivement Commissaire de l'exposition « Biométrie, le corps identité » et Responsable de l'évaluation à la Cité des sciences et de l'industrie, interviendront ensemble pour présenter cette exposition.

Mme Marie-Pierre LAHALLE, Commissaire de l'exposition « Biométrie, le corps identité » de la Cité des sciences et de l'industrie

N'étant pas spécialistes de la biométrie, contrairement à la plupart des intervenants de cette audition, mais spécialistes de la médiation scientifique pour le grand public, nous présenterons ici les réactions du public à l'exposition sur la biométrie organisée par la Cité des sciences et de l'industrie, en partenariat avec Sagem - groupe Safran, dans le cadre de sa galerie des innovations. Ce lieu de la Cité des sciences est dédié aux expositions sur les innovations technologiques qui, au-delà de leur intérêt scientifique et technique, posent de vraies questions de société, éthiques ou politiques. Il est évident que la biométrie en fait partie et présente un grand intérêt pour le grand public.

Il s'agit d'une exposition dont le concept contient une valeur ajoutée par rapport aux informations données par les médias (presse, TV, radio…) puisqu'elle propose de l'interactivité, du ludique, des possibilités d'expérimentation, mais aussi d'entendre des opinions contrastées. Le média exposition permet en effet au visiteur d'être sujet de la biométrie et de pouvoir directement l'expérimenter : le principe étant qu'il s'enregistre à l'entrée de l'exposition avec deux données biométriques : l'empreinte digitale et la photo du visage. Ces données ont été choisies car elle sont faciles à enregistrer, donc elles permettent un flux d'enregistrement de visiteurs important. Cet enregistrement non obligatoire permet simplement au visiteur d'être reconnu dans certains multimédias de l'exposition et d'avoir un accueil personnalisé « Bonjour Paul, pour jouer à… faites…». Bien évidemment, s'il ne s'est pas enregistré, il accède aussi au contenu du multimédia mais sans accueil personnalisé.

L'exposition s'intitule « La biométrie, le corps identité », puisque la question du corps est au centre de la biométrie : il en est la « clé ». L'exposition est organisée en trois ensembles thématiques :

- les fondements de la biométrie avec les aspects historiques et des informations sur les constantes et les différences corporelles qui fondent la biométrie ;

- un ensemble thématique sur les usages de la biométrie où il est fait état de ses applications dans le monde et des questions éthiques qu'elle pose, que nous avons travaillé avec le concours de la CNIL ; sont également diffusées des interviews de personnalités ayant des opinions contrastées sur la biométrie ;

- un ensemble thématique sur les techniques où le visiteur peut expérimenter la plupart des techniques biométriques comme la reconnaissance par l'empreinte digitale, par le visage, par l'iris, qui ont déjà été évoquées. Il y a

également la signature dynamique, dont on n'a pas parlé pour l'instant, mais qui fait partie des techniques dites comportementales, techniques moins fiables mais présentant néanmoins beaucoup d'intérêt.

Ouverte le 30 novembre 2005, soit depuis cinq mois, l'exposition est très visitée pour une exposition de type « moyen format », soit environ 500 m². Ce n'est pas un *« blockbuster »*, comme l'exposition *« Star Wars »* qui bénéficie d'une promotion et d'une visibilité bien plus importante. Mais Biométrie est l'exposition la plus visitée de la Cité des sciences, après *« Star Wars »*, ce qui est une belle performance !

Nous disposons à la Cité de deux outils d'évaluation de nos expositions :

- Le premier, le moins intéressant, est le livre d'or, où tout visiteur peut s'exprimer librement sur l'exposition. On peut y relever des opinions très contrastées sur la biométrie elle-même (« c'est super » ou « c'est *big brother* » pour simplifier), des expressions sur l'exposition elle-même (« c'est clair ou pas », « il n'y a pas assez de postes informatiques »…). Il est en revanche intéressant de noter qu'il y a peu d'observations, d'une part, sur le choix de la Cité des sciences de traiter ce sujet, et d'autre part, sur la légitimité de nous associer à un industriel pour cette exposition, alors que d'autres expositions faites en partenariat on déjà essuyé de sévères critiques de la part de certains visiteurs. Cette absence de critique pour « Biométrie » tient sans doute au fait que l'exposition est assez équilibrée. Elle propose tout le panel des sujets biométriques, y compris les questions critiques, éthiques et politiques.

- Le deuxième outil d'évaluation, le plus important, est l'enquête *in situ* surtout menée lors des trois premiers mois d'ouverture. M Aymard de Mengin va exposer plus précisément les conclusions qui peuvent être tirées de ces évaluations.

M. Aymard de MENGIN, Responsable de l'évaluation à la Cité des sciences et de l'industrie

Le principal objectif de ces enquêtes de l'observatoire des publics vise à obtenir un retour sur la perception de l'exposition elle-même, l'intérêt des visiteurs et les techniques qu'ils ont pratiquées. J'aborderai peu ce point et me contenterai de rapporter ce qu'ils évoquent sur la biométrie elle-même.

Il s'agit d'un sondage par enquêteur en face à face à la sortie des expositions. On n'interroge donc pas particulièrement les visiteurs de telle ou telle exposition mais les visiteurs, représentatifs de l'ensemble des visiteurs de la

Cité de 12 ans et plus, auxquels on pose des questions particulières quand ils ont visité telle ou telle exposition temporaire. Ces questions sont en général au nombre de deux : on leur demande quelles sont leurs impressions, les temps de visite passés, puis on leur pose quelques questions fermées, et une deuxième question ouverte sur les éléments qui ont retenu leur attention, pour obtenir des détails.

La biométrie est l'exposition temporaire la plus visitée après *« Star Wars »*, mais la plupart des visiteurs donnent l'impression de découvrir la biométrie, à part une petite proportion des visiteurs qui sont venus spécialement pour l'exposition et qui ont un comportement un peu particulier dans l'exposition. Bien que l'on entende parler de cette thématique dans les médias, cela n'est pas comparable au réchauffement climatique sur lequel la Cité des sciences avait organisé, il y a quelques années, une exposition centrale que le public visitait en étant concerné d'avance. Pourtant, la thématique de la biométrie a retenu ces visiteurs dans l'exposition : la durée de visite moyenne est de 30 minutes. Un tiers des visiteurs a passé trois quarts d'heure ou plus. Par comparaison avec d'autres expositions de moyen format, il s'agit d'une durée de visite longue. Il y a énormément d'expositions différentes à la Cité des sciences et les durées moyennes de visite tournent plutôt autour de 15 ou 20 minutes. L'exposition Biométrie a donc retenu les visiteurs.

C'est essentiellement, pour la très grande majorité des visiteurs, le côté expérimental et ludique de l'exposition qu'ils ont apprécié : le fait, notamment, de pouvoir passer la porte en étant enregistré. En revanche, la partie portant sur les usages et les débats a été beaucoup moins visitée. Les éléments ayant retenu l'attention sont la reconnaissance par les empreintes digitales, la reconnaissance faciale, et le fait que l'exposition soit accessible aux enfants bien qu'il y ait un peu moins de visiteurs avec enfant dans cette exposition. Malgré cela, ceux qui l'ont visitée avec des enfants ont trouvé des choses qui les intéressaient.

Cela signifie-t-il que l'on aurait pu se passer de la partie débat ? Certainement pas puisque c'était d'abord un des buts de l'exposition. Pour la Cité des sciences, le fait d'organiser des présentations ludiques est un moyen d'intéresser des visiteurs qui peuvent être rebutés par un sujet austère.

Par ailleurs, d'autres évaluations effectuées par le passé concernant surtout des sujets un peu polémiques, et en général des sujets impliquant l'industrie, montrent qu'il est essentiel que les visiteurs sentent que la Cité des sciences est garante du contenu de l'exposition. Un des signes de cela est l'existence d'une place pour les débats, y compris avec des positions différentes. La participation des industriels est parfaitement acceptée à la Cité des sciences, comme l'indiquent les réactions figurant dans le livre d'or citées par Madame Lahalle; mais il faut que la Cité commente et donne des possibilités de recul, même si finalement une grande partie des visiteurs n'ira pas jusque-là.

En revanche, il existe un moyen sur lequel une évaluation particulière a été faite : une animation consistant à amener les visiteurs à discuter et à voter sur des cas concrets d'utilisation de la biométrie. Certains retours de visiteurs ayant participé à cette animation montrent que c'est vraiment un moyen par lequel on parvient à participer au débat. Certains visiteurs disent, par exemple, qu'ils se rendent compte que leur opinion peut varier assez vite, après avoir entendu l'un ou l'autre.

Enfin, sur la nécessité et l'importance du débat, une petite minorité qui ne fait pas partie des visiteurs venus spécialement pour l'exposition a trouvé gênant, voire a été choquée que l'on traite sur un mode ludique un sujet aussi grave. Cela les hérisse car il s'agit pour eux de l'image de l'État policier : ils sont partagés sur la biométrie et mettent en cause le fait de s'y habituer en s'amusant, sans creuser assez le fond. On peut considérer que les réactions des autres visiteurs leur donnent partiellement raison, puisque la majorité s'amuse, mais aussi partiellement tort car l'aspect ludique est également un moyen de rentrer dans le débat.

M. Christian CABAL, Député de la Loire : Je vous remercie de cette présentation des réactions du public, un public un peu biaisé puisqu'il se rend déjà spontanément à la Cité des sciences. Je vais donner la parole à mon collègue Jean-René Lecerf, Sénateur, membre de la Commission des Lois qui a présenté récemment un rapport sur « L'identité intelligente et le respect des libertés » ayant certains points en relation avec la biométrie.

Enjeux des applications des systèmes d'identification biométrique

M. Jean-René LECERF, Sénateur, Rapporteur de la mission d'information du Sénat sur « Identité intelligente et respect des libertés »

Monsieur le Président, je vous remercie beaucoup pour votre rapport et nous avions eu l'occasion et le plaisir de vous auditionner. Etant juriste, et pas du tout un spécialiste des problèmes de biométrie comme les personnes qui se sont exprimées jusqu'à présent, je suis venu à la biométrie un peu en consommateur et parce que le besoin s'en est effectivement fait sentir lors du rapport qui m'avait été confié par la Commission des Lois du Sénat. Celle-ci m'avait chargé d'être rapporteur d'une mission d'information concernant au départ, la fraude documentaire. C'est surtout en travaillant sur la fraude documentaire que l'on en est arrivé à travailler sur la nouvelle génération de documents d'identité et donc sur les aspects biométriques.

En effet, on a constaté que la fraude documentaire était importante, bien que difficile à mesurer, et que déjà la partie émergée de l'iceberg conduisait à une situation tout à fait inacceptable. Je vais citer quelques chiffres sur la fraude documentaire, ne serait-ce que pour vous distraire et expliquer le besoin de biométrie qui était le nôtre : 90 000 titres vierges avaient été volés entre 1999 et 2004 (pour l'essentiel des passeports et des visas), 90 000 passeports avaient été déclarés perdus ou volés par leur titulaire sur la même période. Quant aux pertes ou vols de cartes nationales d'identité, leur nombre était passé de 37 000 en 1997 à 527 000 en 2003. C'est une multiplication par 14 mais, entre temps, le 1er septembre 1998, la gratuité des cartes nationales d'identité est intervenue. On peut supposer que les 527 000 cartes d'identité n'étaient pas perdues pour tout le monde.

A partir de là, les collègues de la Commission des Lois ont fait des suggestions de bon sens pour essayer de remédier quelque peu à cette situation qui laisse supposer une fraude encore plus importante. Ces suggestions consistaient par exemple à faire en sorte que la réalisation des documents d'identité et la personnalisation de ces documents soient réalisées dans un même lieu, pour éviter les vols de documents vierges entre les lieux où on les fabrique et l'accès dans les préfectures. Il n'y a pas de solution miracle : en changeant les structures chargées du transport de ces documents, on a rendu un peu plus compliquée la tâche des

malfaiteurs, mais visiblement des braquages récents montrent que devant l'importance de l'enjeu, cette solution n'était pas une parade idéale.

De même, on a également recommandé de conserver les sécurités traditionnelles et même parfois de les activer : on a par exemple été assez surpris d'observer que pour la carte nationale d'identité sécurisée certains éléments de sécurité comme les luminophores n'étaient pas utilisables, faute d'avoir distribué à la police ou à la gendarmerie les appareils permettant de s'en servir. Cela peut prêter à sourire dans un premier temps très court. On a parfois l'impression que la fraude documentaire en France, c'est un peu « Zorro » ou « Robin des bois » alors que cette fraude documentaire se révèle être un sas pour des infractions extrêmement importantes.

On pense d'abord bien sûr à des activités certes coupables comme la fraude aux examens ou au permis de conduire par exemple : on a découvert comme cela qu'une même personne avait passé 50 fois le permis. Elle devait conduire très bien, mais c'était une façon effectivement assez pratique pour les autres de l'obtenir. Il existe aussi la fraude aux droits sociaux, avec les coûts que cela engendre. Surtout il faut savoir que cette fraude documentaire est un sas vers la grande criminalité, vers le trafic des êtres humains ou le terrorisme. Systématiquement, lorsqu'il y avait activités terroristes, on décelait au départ la fraude documentaire, l'usage de faux papiers d'identité et la multiplication des identités. C'est la raison pour laquelle on s'est très vite retrouvé devant l'obligation d'orienter le travail vers la biométrie, vers le traitement informatisé de la biométrie, vers la notion d'identité biométrique.

Le Sénat a essayé de rendre un rapport qui soit très largement consensuel et « œcuménique » : ce rapport a été voté par la quasi-totalité des Sénateurs de la Commission des Lois, quel que soit le groupe auquel ils appartiennent. Seul le groupe communiste s'est simplement abstenu, il n'a donc pas voté contre. Si l'on est parvenu à cet accord quasi général, c'est parce qu'on a essayé, plutôt que de recommander telle ou telle solution, d'envisager les différentes solutions, et à chaque fois d'exprimer pour chacune ce qui paraissait être les avantages et les inconvénients et par voie de conséquence, les précautions qu'il convenait à notre sens de prendre.

Dans un premier temps, on a estimé qu'il fallait soigneusement distinguer, pour les documents d'identité, la biométrie visant à authentifier, de la biométrie tendant à identifier. Dans le cadre de ce qu'on appelle le « un contre un », la biométrie pour authentifier, il est apparu qu'existaient des techniques apportant « un plus » en termes de sécurité, sans léser en aucune manière les libertés publiques. On a donc globalement pensé qu'on aurait tort de s'en priver.

La première hypothèse est celle de la carte à puce biométrique sans fichier central, la puce étant simplement embarquée sur la carte, ce qui permet de s'assurer de manière certaine que la personne qui présente la carte d'identité ou le passeport est bien la personne à qui on a délivré ces titres. La seule utilité est

celle-là, elle est déjà considérable par rapport à ce que l'on constate aujourd'hui. Bien sûr, en raison des coûts de la technique biométrique, il paraissait utile et même nécessaire de tenter d'aller un peu plus loin ; on s'en est rendu compte.

Des conversations suivies avec des spécialistes qui se trouvent d'ailleurs dans cette salle ont montré qu'il existait techniquement des solutions que Monsieur Didier évoquait tout à l'heure. Sur ce point, n'étant pas moi-même spécialiste technique ni ingénieur, je fais confiance à l'ensemble des spécialistes que nous avons rencontrés. Il existait des systèmes à liens faibles qui permettaient d'obtenir un avantage supplémentaire, particulièrement dans le cadre de la biométrie pour authentifier, sans pour autant porter atteinte, de quelque manière que ce soit, aux libertés car le système à liens faibles ne permet pas de passer de la biométrie à l'identité, ou de l'identité à la biométrie, mais inclut malgré tout un fichier central. L'intelligence du système permet de détecter l'existence possible d'une autre identité avec les mêmes caractéristiques biométriques. Autrement dit, on peut éviter de cette façon l'usurpation d'identité, élément particulièrement ravageur au niveau de la délinquance et posant aux personnes dont l'identité a été usurpée des problèmes qui ne doivent pas être négligés.

Au sein de la Commission des Lois du Sénat, un accord très général sur cette biométrie existe, tant que l'on utilise des solutions d'authentification, et dès lors que, par le biais du système à liens faibles, on obtient à la fois la certitude que la personne qui présente son document d'identité est bien la personne à qui il a été délivré, et qu'en outre, elle ne peut pas avoir d'autre identité basée sur ses références biologiques dans le système. Si l'on respecte bien sûr tous les principes, les textes, la compétence de la Commission nationale informatique et libertés (CNIL) sur les données personnelles, pourquoi être réticent ? Ce système ne nous paraît pas devoir mériter d'être particulièrement encadré.

En revanche, il en va différemment de la biométrie pour identifier. Il ne s'agit plus du « un contre un » mais du « un contre n ». On peut effectivement supposer obtenir des utilisations encore bien plus nombreuses. On dispose en outre de la possibilité d'identifier des personnes : la possibilité par exemple, au moment du Tsunami d'identifier des cadavres, d'identifier des malades d'Alzheimer, de jeunes fugueurs, une personne ayant accompli un forfait et refusant de décliner son identité. On a également la possibilité d'utiliser les empreintes retrouvées sur la scène d'un crime ou délit pour aider très largement dans le cadre des opérations de police judiciaire. Ce type de technique recèle un danger pour les libertés. La Commission des Lois du Sénat l'expose aussi unanimement car ce n'est plus un système neutre en termes de libertés publiques. Selon cette dernière, si l'on veut réfléchir à ce système, il est de la responsabilité du seul législateur et non pas du pouvoir réglementaire de décider éventuellement de l'autoriser.

Si on s'orientait néanmoins vers ce système, il faudrait prendre des précautions nombreuses. Premièrement, seul un magistrat pourrait autoriser l'utilisation de données personnelles à des fins d'identification. Deuxièmement, l'ensemble du système devrait être placé sous le contrôle de la CNIL, en donnant à

cette autorité administrative indépendante les moyens d'assumer cette mission supplémentaire. On pourrait profiter d'un système particulièrement ambitieux pour tenter d'inverser le syndrome *« big brother »* et faire en sorte qu'en même temps l'on donne à chaque citoyen la possibilité de contrôler le système, ce qui revient à donner gratuitement la possibilité à chacun d'avoir accès à n'importe quel moment à ses données personnelles de façon à pouvoir rectifier les erreurs éventuelles, à pouvoir connaître les personnes qui ont accédé aux dites données personnelles, et avoir la possibilité de soumettre à la justice les cas où des personnes y auraient accédé, en n'en ayant pas le droit, et de les sanctionner.

Tel est brièvement résumé le travail réalisé par la Commission des Lois du Sénat, qui a souhaité que l'on ne s'aventure pas, du moins en l'état actuel des choses, vers des systèmes de puces sans contact suscitant le développement d'une industrie dans ce domaine, en estimant que, sur ce point, les libertés publiques n'y trouveraient pas leur compte.

M. Christian CABAL, Député de la Loire : Je vous remercie de cette présentation brève, et néanmoins complète et suffisamment intéressante pour donner envie de lire l'ensemble du rapport. Je vais donner tout de suite la parole à Monsieur Melchior, qui est Co-Directeur de la mission interministérielle sur les visas biométriques au Ministère de l'Intérieur.

M. Philippe MELCHIOR, Co-Directeur de la mission interministérielle sur les visas biométriques au Ministère de l'Intérieur

Si vous m'y autorisez, Monsieur le Président, je vais commencer par un mot personnel. Quand, il y a deux ans et demi, le Ministre de l'Intérieur de l'époque m'a demandé de travailler sur la biométrie et de coordonner les projets biométriques du Ministère de l'Intérieur, il m'a un peu effrayé parce que je ne connaissais absolument rien à ce sujet. Votre rapport est l'un des premiers documents que j'ai lus, et est sans conteste celui qui m'a le plus apporté. Je saisis donc l'occasion de vous remercier.

Pourquoi un Ministère de l'Intérieur a-t-il besoin de biométrie ?

C'est tout simple, et Monsieur Lecerf, l'a expliqué on ne sait pas attester autrement de l'identité des personnes. On n'a pas le choix.

Il y a quelques années, le Ministère des Affaires Etrangères m'a envoyé en Afrique pour étudier les problèmes d'état civil. Dans les pays avec lesquels nous avons des rapports, moins de 10 % de la population dispose d'un état civil. Mais

ceci n'est pas du tout leur problème. Il y a un pays d'Afrique où l'on m'a proposé un état civil de ce pays pour 5 000 FCFA : je n'ai pas accepté mais un de mes collègues de la Commission Européenne l'a fait. Il est maintenant né de parents de ce pays, dans une commune de ce pays : il est donc un national de ce pays.

Pour les Français, il n'est pas très difficile d'avoir une vraie-fausse carte d'identité. C'est simple. Vous aurez une carte d'identité ; elle sera faite avec beaucoup de précautions, comme l'a dit Monsieur Robin, mais il n'empêche qu'elle est fausse.

Si on se place du point de vue d'un Ministre de l'Intérieur, la tâche est assez complexe. Pour tout le monde, il est le Ministre de la police et du point de vue de la police judiciaire, on a besoin de l'empreinte digitale et de la photo des délinquants, et si possible d'autres données parce qu'on peut trouver sur les traces d'un délit ou d'un crime une indication qui permet de remonter une piste.

Des personnes qui ne sont pas françaises entrent sur le territoire français. Du point de vue du contrôle de l'application de la loi en matière d'immigration, - quelle qu'elle soit, si ouverte et si bienveillante soit-elle-, il faut contrôler qu'elle est appliquée. 10 % des ressortissants des pays avec lesquels on a des rapports disposent d'un état civil. 10 % cela veut dire zéro, parce que ces 10 % peuvent aussi bien acquérir un faux état civil. Concernant les faux papiers si vous venez dans notre service, à la police de l'air et des frontières, on vous montrera les faux papiers de certains groupes industriels. C'est vraiment du travail industriel, du très beau travail.

On a besoin de données pour des raisons de police judiciaire, mais aussi pour la police administrative, pour des personnes non ressortissantes de la France, qui y viennent et qui quelquefois veulent y rester sans en avoir l'autorisation, avec des motifs que parfois on comprend tous, mais que parfois on ne souhaite pas. Il faut alors des données.

Le Ministère de l'Intérieur ne représente alors plus seulement la police au sens de la police judiciaire mais également la police au sens de la réglementation concernant surtout le travail des Préfectures et des mairies : le sens que lui donnent les professeurs de droit public. Traditionnellement, quand l'État et les préfets délivrent une carte d'identité, ils donnent un document à, par exemple, Monsieur Bernard Didier pour certifier qu'il est bien Monsieur Bernard Didier, document qui ne va pas être utilisé dans ses relations avec les services de police - les contrôles d'identité sont extrêmement difficiles en France, heureusement - mais lui servir quand il veut faire un chèque pour que le commerçant ait une garantie.

Cependant on ne vit plus comme cela, on ne fait plus de chèques, on achète sur Internet. 240 millions de lettres recommandées sont envoyées chaque année en France ; comme vous, j'en reçois mais je travaille la journée. Bien sûr le facteur met un papier dans la boite aux lettres, ma femme est à la maison, mais le

facteur ne monte plus. Il faut donc que j'aille à la poste, qui est ouverte quand je travaille. Je serais tellement content s'il y avait un système de certification d'identité qui me permettrait de la recevoir sur mon ordinateur. Cela me ferait gagner de l'argent. Les modes de vie sont différents et cette certification par l'État de l'identité d'une personne, il nous faut la faire autrement. Or, on ne voit pas bien comment on pourra la faire sans recours à une donnée biométrique et à une base de données.

S'agissant des *process* dans un aéroport ou un port, on peut faire les choses de façon complexe. Lorsque l'on quitte l'espace Schengen, on passe devant un fonctionnaire de police, à l'aller et au retour. Pourquoi ne pas dire à ceux qui le souhaitent : « nous sommes prêts, grâce à la biométrie, à vous dispenser de ce mode de contrôle, nous sommes prêts à vous dispenser de faire la queue si vous le voulez. »

Les applications sont de natures différentes. Certaines sont des applications de police, au sens « service de police », d'autres sont des applications de type réglementaire, éventuellement non obligatoires, qui intéressent peu les services de police : la carte d'identité est facultative, personne n'est obligé d'avoir un passeport. Il existe des applications qui n'intéressent pas tout le monde mais facilitent la vie. En fonction de l'objectif de l'application concernée qui utilise la biométrie, on aura des exigences, et on devra respecter des règles différentes.

En ce qui concerne la police criminelle, on disposera d'une base de données, on va trouver une trace et on aura du temps pour comparer, c'est-à-dire une à trois heures. Quand on contrôle des voyageurs dans un aéroport et qu'ils sont 2000 à sortir des quatre ou cinq avions arrivant en même temps, on ne dispose pas de temps, sauf à créer une émeute ou à mépriser vraiment les usagers. De sorte qu'en s'adressant aux industriels, on leur demande dans certains cas des dispositifs qui peuvent être lents, et dans d'autres cas d'apprendre à appliquer la biométrie à la gestion de flux. On a fait ensemble des progrès considérables, mais on n'est pas au bout du chemin.

Tout à l'heure, Monsieur Didier expliquait qu'on ne plaque pas la biométrie mais qu'on l'intègre : il a complètement raison, et c'est probablement le plus difficile. Les questions techniques ne paraissent pas très importantes dans cette affaire. On sait que la reconnaissance faciale ne fonctionne pas, que cela fonctionnera peut-être un jour en trois dimensions, mais elle est complètement incompatible avec la gestion des visas. 10%, 20% de taux de faux rejet, ce n'est pas acceptable. Alors, un jour peut-être… On sait qu'il faut utiliser le multimodal pour certaines applications relevant de prérogatives de puissance publique, c'est indispensable.

Ce sont des problèmes industriels, des spécifications fonctionnelles et des obligations de prudence, de précaution dont dépendent les applications. Les obligations de précaution sont différentes selon les applications, mais il faut les prendre très au sérieux parce qu'il s'agit du corps, de nous, d'un sujet qui fait

fantasmer et qui, si on ne le traite pas sérieusement, entraînera des réactions légitimes. Si on est en présence de petites applications concernant des volontaires, il est possible d'admettre qu'on prendra un peu moins de précautions. La doctrine de la CNIL classique pour les étudiants de droit administratif d'autrefois, pose le principe qu' « il faut proportionner à l'intérêt, la restriction, la mesure » est excellente. On peut avoir de temps en temps des divergences de vue sur l'application de la doctrine, mais le principe est excellent ; on doit toujours faire attention et déplacer le curseur selon la nature de l'application.

Cependant, on se trouve dans le cadre d'une souveraineté nationale devenue très limitée, puisque les passeports et les visas ne sont plus de compétence nationale. Si on nous demande de faire, nous sommes obligés de faire. Pour les cartes d'identité qui sont aussi des documents de voyage, bien sûr que nous ferons. Monsieur le Député, Monsieur le Sénateur, je ne sais pas quand le Parlement de la République votera la loi, mais inéluctablement, il la votera. Les Français n'accepteront pas qu'il en aille autrement. Par moments, certains disent qu'il ne faut pas, mais on le fera, dans un ou trois ans. Nous ne serons pas le seul pays développé à ne pas introduire la biométrie. En matière de police des étrangers, on s'est lancé dans les visas biométriques. En application de la loi votée, cela sera fait pour les non admis. Cela se fera pour les reconduites à la frontière. Cela existe aussi pour l'asile politique.

Enfin, je n'ai aucune instruction du Ministre, mais mon avis privé est qu'on le fera pour les permis de conduire. Je ne sais combien de faux permis de conduire sont utilisés en France, mais le centre de recherches universitaires de Paris a indiqué qu'il y avait un million de faux permis de conduire en France. Ce chiffre est discuté dans son ampleur, mais ce n'est pas 10 000, ce n'est pas 100 000. Pensez-vous que ce soit raisonnable ?

Inéluctablement un mouvement se développera. Il faut essayer de profiter des progrès techniques, en faisant préalablement des évaluations rigoureuses et en étant auparavant très prudent sur la réalité d'un risque d'atteinte aux droits de l'Homme, avec une communication attentive, pour éviter les fantasmes dans cette matière.

M. Christian CABAL, Député de la Loire : Je vous remercie beaucoup pour cette interprétation personnelle qui s'inscrit aussi dans une logique rationnelle et d'ordre public. Vous avez permis de lancer le débat, juste après l'exposé technique précédent.

Je donne maintenant la parole à Mme Josiane Couratier, Co-Directeur de la mission interministérielle sur les visas biométriques, au Ministère des Affaires Étrangères.

Mme Josiane COURATIER, Co-Directeur de la mission interministérielle sur les visas biométriques, au Ministère des Affaires Étrangères

J'enchaînerai sur les propos de l'orateur qui m'a précédée, et qui est également mon collègue. Il a évoqué une évolution inéluctable. Je pense que c'est au législateur de trancher sur ce point. Il est cependant certain que si nous allons dans le sens d'une généralisation de la biométrie à de si nombreux aspects de la vie du citoyen, il faut y aller en examinant tous les aspects, d'où l'intérêt d'un projet pilote. C'est ce qui m'a été confié ainsi qu'à Monsieur Melchior, à propos des visas par deux ministres : le Ministre de l'Intérieur et le Ministre des Affaires Étrangères. Nous y avons travaillé depuis deux ans.

Monsieur le Président, dans le rapport extrêmement détaillé que vous aviez présenté il y a trois ans, vous définissiez déjà un certain nombre d'enjeux. Puisque cette deuxième table ronde s'intitule « enjeux », il m'apparaît qu'à travers le projet pilote que je vais vous décrire, nous avons tenté de répondre à trois types de défis. Premièrement un défi technique et industriel, à travers l'étude de la faisabilité et de la performance du processus biométrique. Ensuite un deuxième défi de caractère diplomatique : quelle serait la place de la France dans cette « course à la biométrie » au plan international et européen ? Enfin un défi ou un enjeu de société, à savoir comment concilier les enjeux de sécurité collective (lutte contre le terrorisme, l'immigration illégale, la fraude documentaire, etc.) et les libertés individuelles, c'est-à-dire, la protection des données personnelles. Je mentionnerai également un autre défi, c'est le défi financier, qui mérite examen et qui a parfois été occulté.

L'étape juridique et la protection des données personnelles

Pour mener ce projet pilote, il nous fallait l'autorisation par décret en Conseil d'État. Nous avons également décidé de consulter la CNIL.

- Lors de l'audition par la CNIL, deux points ont été examinés. Un aspect technique en premier lieu, consistant à étudier les moyens de s'opposer à la captation frauduleuse des données sur les matériels utilisés. En second lieu, comment limiter l'accès à ces données à travers le nombre et la qualité des personnes qui les capturent, qui les transmettent, et qui les contrôlent ?

- Le Conseil d'État, lui aussi s'est penché sur la question de la protection des libertés individuelles et notamment à travers la question de la sécurité associée à l'utilisation d'une puce comme support de stockage des données. Nous avons également examiné la durée de conservation des données. Nous avons obtenu l'autorisation de procéder à l'expérimentation.

Le projet européen

Au moment où la France se décidait à lancer un projet pilote, une conjoncture très favorable a fait qu'au plan européen la Commission Européenne – qui ne dispose pas d'experts – souhaitait elle aussi mener une expérience pilote sur la biométrie dans les visas. Comme suite logique aux initiatives américaines dans ce domaine, l'Union européenne a entrepris depuis 2004 la négociation d'un projet de système d'information sur les visas dans lequel tous les consulats et postes frontières de l'espace Schengen seront reliés et pourront à tout moment échanger des informations. Pour mener à bien ce chantier la Commission Européenne avait besoin d'une expérience pilote. La France a donc été le chef de file de ce projet aux côtés d'autres partenaires, la Belgique en premier lieu, qui a fourni une participation très active, mais aussi l'Allemagne, les Pays-Bas, l'Italie, le Danemark et la Finlande, de même que la Pologne et la Hongrie. Nous avons donc mené le projet national à l'intérieur, en même temps que le projet européen : il y a eu interconnexion permanente.

Les objectifs de l'expérience

a) Il s'agissait tout d'abord de tester la faisabilité technique du processus biométrique, à travers tous les aspects de la procédure, depuis l'arrivée du demandeur au consulat pour déposer sa demande, avec la capture de ses données biométriques, la transmission, puis le stockage, jusqu'au bout de la chaîne, avec le contrôle à la frontière. C'est l'ensemble du processus technique et ses performances devaient être testés.

Quels sont les éléments techniques qui ont été envisagés puis retenus pour l'expérience?

-S'agissant des modalités biométriques tout d'abord, La France a retenu deux modalités : la photo numérisée et les dix empreintes digitales des doigts posés à plat.

-Une autre question portait sur le support de stockage des données biométriques : devait-on utiliser. le composant électronique - « la puce » - ou bien fallait-il donner la préférence à une base centrale de données ? . On le sait, l'utilisation de la puce permet à l'individu d'emporter avec lui ses données personnelles et donc d'en contrôler l'accès. Un élément essentiel pour choisir entre les deux supports était la performance en termes de rapidité et fiabilité, pour éviter les faux rejets et les fausses acceptations, afin de ne pas freiner le processus tant au moment de la capture dans les consulats, qu'à celui du contrôle à la frontière.

b) En deuxième lieu, à côté de la faisabilité technique, on devait tester l'aspect organisationnel. Quelles seraient les conséquences en termes de matériel, d'agencement des locaux, de personnel ? Quels coûts et aménagements en résulteraient ?

c) Le troisième champ d'investigation est constitué par les aspects humains. L'aspect diplomatique était un élément essentiel nous allions introduire la biométrie dans les visas, c'est-à-dire une nouvelle procédure sur le territoire de pays tiers. Nous avions donc un devoir d'information et de conviction pour éviter les réactions hostiles, même si les Américains avaient ouvert la voie avec leur propre procédure déjà généralisée au plan mondial depuis presque deux ans. Le deuxième aspect à tester était de savoir comment réagirait le public de demandeurs de visas. Enfin, comment réagiraient les personnels concernés ? On a conduit notre propre évaluation, et confié à l'Institut national des télécommunications (INT), une évaluation de caractère plus sociologique.

En ce qui concerne le cadre géographique de l'expérience, nous avons couvert la planète et pris un poste consulaire sur chaque continent. En Amérique, nous avons expérimenté à San Francisco pour la France, et à Washington pour la Belgique. En Afrique nous avons expérimenté à Bamako (France) et à Kinshasa et Lubumbashi (Belgique). En Asie la France a expérimenté à Colombo et en Europe orientale à Minsk. L'expérience a également porté sur le contrôle aux frontières, qui correspondent à l'arrivée sur le territoire Schengen depuis les pays d'origine des demandeurs de visas, c'est-à-dire pour la France, Roissy-CDG, Orly, Lyon, Marseille,pour les aéroports et le port de Marseille. Les Belges ont testé le contrôle à l'aéroport de Zaventem.

La durée de l'expérience au plan européen a été de 15 mois. Elle a commencé en janvier 2005 et s'est terminée en Avril. Nous disposons donc d'un recul de 15 mois, ce qui n'est pas négligeable.

Quels sont les résultats de cette expérience à la fois nationale et européenne?

- Faisabilité technique

Les visas biométriques, version franco européenne, existent depuis la fin du mois de mars 2005. Plus de 60 000 visas ont été délivrés dans les consulats pilotes et plusieurs milliers ont été contrôlés. Il y a forcément une différence entre les deux chiffres puisque tous les voyageurs n'arrivent pas nécessairement dans les postes où le contrôle est exercé. S'agissant de l'opérateur industriel, Monsieur Didier l'a mentionné, SAGEM a été retenu à l'issue d'un appel d'offres européen.

- Performance

Plusieurs logiciels et matériels ont été testés et la durée de performance a été divisée par deux. D'un temps d'enregistrement des données biométriques dans les consulats de trois minutes, nous sommes passés à une minute trente. Au contrôle à la frontière, nous sommes maintenant à moins de dix secondes, ce qui est tout à fait remarquable. S'agissant des modalités, nous avons validé le système basé sur la prise d'empreintes des dix doigts posés à plat. Jusqu'à présent les Anglo-Saxons s'étaient basés uniquement sur deux doigts. Il a été prouvé que

c'était insuffisant, notamment en prévision du nombre de requérants qui sont enregistrés dans la base de données. Pour éviter les faux rejets ou les fausses acceptations, et donc réduire les marges d'erreurs, nous sommes passés à dix doigts. Cela a été validé et retenu pour la suite de l'expérimentation.

Un autre élément validé à travers ce projet pilote est le stockage sur une base de données centralisée. La puce a longtemps fait l'objet d'un débat pour les raisons qui ont été évoquées. Il s'est avéré que c'était, d'une part coûteux, et cela le demeure aujourd'hui, et d'autre part, que l'utilisation de la puce, compte tenu des contraintes légitimes de sécurité contre la captation frauduleuse, nécessitait de passer par la base de données au contrôle, donc d'allonger le temps de contrôle, ce qui nous a conduits à écarter ce moyen à ce stade.

- Aspects organisationnels

Une des conclusions tirées de ce projet pilote est que désormais tous les demandeurs de visas devraient se présenter en personne, car on n'a pas encore pris d'empreintes digitales par téléphone, ni par télécopie. Jusqu'à présent, un certain nombre de requérants ne se présentaient pas au consulat et passaient par des agences de voyages. Désormais, cette obligation entraînera une augmentation de la fréquentation des locaux consulaires, jusqu'à 40 %. Ceci influe sur la taille des locaux d'accueil, sur le matériel utilisé, sur les effectifs des services. C'est également le cas à la frontière : il y a dorénavant un contrôle systématique qui influe sur les locaux, sur le matériel, sur les effectifs. La conséquence pratique est que la biométrie a un coût, il convient d'insister sur ce point.

Nous avons essayé de rationaliser et d'externaliser une partie de la procédure, de mettre en commun les moyens avec d'autres partenaires. A Bamako, nous avons accueilli les personnels belges dans nos locaux. Nous avons délocalisé le processus à plus de deux heures d'avion à Seattle pour nous rapprocher des demandeurs de visas dans la circonscription de San Francisco. Nous avons aussi expérimenté le système mobile avec une mallette portable. Quoi qu'il en soit, on ne répond pas à toutes les difficultés et donc on constate que la biométrie a un coût. Comment financer les coûts induits ? C'est pour répondre à ces questions que la France a sollicité et obtenu des institutions européennes l'augmentation de 35 à 60 euros du tarif du visa Schengen.

- Les réactions des personnes

Les autorités locales ont compris qu'il y avait un mouvement inéluctable, et il n'y a donc pas eu d'obstacles. Là encore, la voie a été ouverte par un autre pays, les Etats-Unis, ce qui a permis la compréhension des interlocuteurs. D'ailleurs, souvent ces États tiers utilisent eux-mêmes la biométrie pour d'autres applications (état-civil, vote…). Grâce à une politique d'information et de sensibilisation assez développée, nous avons pu prévenir les réactions hostiles.

Pour les personnels des services (consulats, frontières) nous avons également mené une action de sensibilisation en leur démontrant les avantages du nouveau système en termes de lutte contre la fraude documentaire. Ces personnels se sont donc ralliés à cette procédure. Il n'y a pas eu d'opposition de principe. Nous avons naturellement insisté sur la formation.

- L'avenir

La Commission Européenne a jugé les résultats du projet pilote si intéressants qu'elle a autorisé le lancement d'une deuxième expérimentation qui commence maintenant. Elle avait financé à 80 % le premier projet qui est terminé, elle finance également le nouveau. Cette fois, les partenaires sont tous impliqués de manière très active et vont tous « biométriser » plusieurs consulats et postes frontières associés. Nous essayerons également de rationaliser en mettant davantage en commun les personnels et les locaux. Enfin, nous testerons l'interopérabilité de systèmes informatiques avec des appareils et des équipements provenant de pays différents. Ceci en prévision de l'interopérabilité qui sera la règle dans le système européen, et qui devrait être opérationnelle à partir de l'année prochaine.

M. Christian CABAL, Député de la Loire : Je vous remercie beaucoup de cette présentation synthétique et complète. On aura quelques questions à vous poser tout à l'heure sur cette expérimentation et sur le calendrier que vous venez d'évoquer. Pour terminer techniquement cette présentation, je donne la parole à Madame Sophie Planté qui est Adjointe au Directeur du programme d'Identité nationale électronique sécurisée (INES) et qui complétera l'intervention de Monsieur Melchior en prenant l'exemple pratique de INES.

Mme Sophie PLANTÉ, Adjointe au Directeur du programme INES

Mon intervention concerne la Carte nationale d'identité électronique, projet en cours d'élaboration au Ministère de l'Intérieur. Ceci pour en préciser les quelques différences avec le projet de visa biométrique.

1/ La carte d'identité est un document sur lequel ne pèse aucune obligation juridique internationale à ce jour, ce qui ne veut pas dire qu'il n'y ait pas des évolutions politiques à prendre en compte (travaux de la commission européenne sur les cartes d'identité notamment).

2/ Évidemment, la problématique liée à l'usage de la biométrie dans les cartes d'identité est proche de celle qui a conduit à l'expérimentation concernant

les visas, mais elle n'est pas identique. La problématique qui sous-tend l'introduction de la biométrie dans les cartes d'identité est celle de la preuve de l'identité déclarée lors de la demande de titre, et non, comme pour les visas, celle de s'assurer qu'une personne a quitté le territoire à l'expiration de son visa.

3/ C'est la raison pour laquelle, sur des aspects qui peuvent paraître mineurs mais qui en termes de symbolique ne le sont pas forcément, la conservation de la biométrie dans le projet de carte d'identité ne concerne pas les empreintes des dix doigts, mais seulement six ou huit doigts, parce que symboliquement, les empreintes de dix doigts font penser à un usage de police. La carte d'identité, comme le rappelait Monsieur Melchior, n'est pas un outil de police mais un outil de la vie quotidienne des citoyens pour prouver leur identité à leurs concitoyens, aux commerçants, lors de tous les usages qui le nécessitent dans les services publics ou privés, et très rarement face à un policier ou un gendarme.

4/ Je voudrais aussi apporter une précision à la suite des propos de Madame Couratier concernant le coût de la biométrie. S'il est vrai que pour les visas, l'introduction de la biométrie suppose l'augmentation de la fréquentation du public dans les postes consulaires, et donc engendre automatiquement un surcoût par rapport aux procédés antérieurs, pour la carte d'identité, la problématique est légèrement différente. Si le Ministère de l'Intérieur obtenait la possibilité de conserver les données biométriques dans son application informatique concernant les cartes d'identité, cela diviserait par deux ou trois le temps (et donc le coût) nécessaire à l'instruction d'un dossier ; on obtiendrait plutôt des économies significatives, pas immédiatement, mais une fois le processus bien rodé et quand les agents auraient acquis un certain savoir-faire. On ne se situe donc pas dans une problématique équivalente à celle des visas, en ce qui concerne les coûts.

L'introduction de la biométrie dans la carte d'identité

Ce que je développerai concerne essentiellement l'introduction de la biométrie dans l'application informatique de la carte d'identité, et non l'introduction de la biométrie dans les titres, parce qu'il semble que c'est sur ce premier point que les questions de protection des libertés sont les plus sensibles.

Mais je voudrais préalablement préciser que le réexamen dont a fait l'objet le projet de loi rédigé au printemps 2005 porte sur d'autres aspects que la biométrie, comme par exemple le caractère facultatif de la carte nationale d'identité que le Ministère de l'Intérieur souhaite maintenir. En effet, le projet s'inscrit dans le droit constant : la carte d'identité n'est pas obligatoire en France, contrairement à ce que la plupart des gens pensent. La preuve de l'identité se fait par tous moyens en France. Le réexamen a également porté sur les usages électroniques de la carte d'identité, qui ne concernent pas du tout la biométrie.

C'est sur l'application informatique support à la délivrance des titres, que se focalisent la plupart des questions relatives à l'introduction de la biométrie. C'est une des raisons pour lesquelles le projet de loi a fait l'objet d'un réexamen

puisqu'en juin dernier, à l'issue des rapports de la mission d'information sénatoriale présidée par Monsieur Lecerf et du rapport du forum des droits sur Internet, plusieurs critiques avaient été virulentes sur le bien fondé de la conservation des données biométriques dans une base. A l'issue de ces remarques et de ces critiques, le Ministre de l'Intérieur a souhaité que le projet soit réexaminé sur ce point, et la direction de programme a visité sept pays européens plus avancés que nous sur ces questions de titres d'identité électronique.

La question qui a guidé notre comparaison des exemples étrangers était : pourquoi a-t-on besoin d'une base de données biométriques pour fiabiliser les données d'identité alors que certains pays n'en ont pas aujourd'hui, ce qui ne veut pas dire qu'ils n'envisagent pas de le faire ?

Pour brosser à grand traits les conclusions de ces visites, on distinguera schématiquement deux types de pratiques sur la délivrance des cartes d'identité (souvent conjuguées à la délivrance des passeports car c'est la même application qui est utilisée).

Parmi les pays visités, en l'occurrence la Belgique, l'Espagne, l'Estonie, la Finlande, l'Italie, la Suède et le Royaume-Uni, il y a ceux (Europe du Nord) qui se fondent sur un registre de population pour garantir que le citoyen qui vient demander un titre est bien la personne qu'il déclare être. Ces registres de population contiennent souvent beaucoup plus d'informations que la simple donnée d'état civil : l'inscription n'est pas facultative. Le citoyen est d'office inscrit dans ce registre (qu'il soit ressortissant de ce pays ou ressortissant étranger vivant dans le pays). Les données dépassent largement le cadre de la donnée d'état civil et concernent par exemple à la fois la profession, la composition familiale, l'adresse, des données fiscales, et celles relatives aux administrations sociales. De ce fait, lorsqu'un citoyen est inscrit dans ce registre et qu'il déclare son identité et son numéro dans le registre de population, il lui est assez difficile de se faire passer pour quelqu'un d'autre, dans la mesure où cela impliquerait d'usurper l'ensemble des données concernant cet individu dans le registre. Lorsque l'on demande un titre, se faire passer pour quelqu'un d'autre, sur tous ces plans, est alors plus difficile qu'avec une simple donnée déclarative de l'état civil, comme c'est le cas en France.

Le deuxième type de pratique est le numéro d'identification unique, pérenne et souvent signifiant utilisé dans plusieurs procédures administratives et notamment la procédure concernant la délivrance d'une carte : c'est l'exemple italien ou espagnol, sachant qu'en Espagne, la carte d'identité est obligatoire, le numéro l'est donc également et suit l'individu tout au long de sa vie.

La France se distingue de ces deux types de pratiques sur cinq points

D'abord, ce qui permet de justifier d'une identité lorsqu'on fait une demande de carte d'identité à sa mairie est un document d'état civil reçu de la mairie de naissance, le plus souvent par la poste, bientôt par Internet, et que l'on

s'est procuré en déclarant simplement son nom, sa date et son lieu de naissance et de temps en temps sa filiation. Or ce type d'information, s'il n'est pas vraiment public, n'est pas très difficile à se procurer vis-à-vis d'un individu que l'on connaît et dont on veut usurper l'identité.

Le problème est donc que la source d'information relative à l'état-civil est extrêmement poreuse à la fraude. Si je sais où vous êtes né(e), que je connais votre date de naissance, et que je suis un homme ou une femme dans la même tranche d'âge que vous, je me présente avec votre état-civil, ma photo, mon justificatif de domicile, qui n'est pas très difficile à trafiquer pour mettre votre nom et mon adresse. Les préfectures ou les sous-préfectures n'ont absolument pas la possibilité de détecter que je ne suis pas la bonne personne, car le justificatif d'identité que vous produisez, l'extrait d'acte de naissance, est un acte authentique. Simplement, ce n'est pas le vôtre, mais celui de la personne dont vous usurpez l'identité.

On détectera qu'il y a eu usurpation éventuellement *a posteriori*, lorsqu'une fraude sera commise. Si elle porte un préjudice à l'individu dont l'identité est usurpée, il y aura alors enquête, mais on entre alors dans les domaines policier et judiciaire et cela peut prendre des mois, des années. Au plan administratif, un agent de préfecture qui traite un dossier et qui lance l'ordre de production de la carte n'est pas en mesure de s'apercevoir qu'il ne s'agit pas de la bonne personne. C'est fâcheux et surtout extrêmement préjudiciable à ce qui est, à notre sens, la première des libertés, celle de pouvoir jouir de son identité et des droits qui y sont affectés de manière exclusive. Pendant nos travaux, nous avons rencontré des personnes qui se sont rendu compte qu'elles étaient déjà mariées quand elles ont voulu se marier, parce que leur état-civil avait été utilisé par quelqu'un d'autre.

La première caractéristique en France est donc l'utilisation d'un mode de preuve de l'identité disséminé dans 36 500 communes différentes puisque l'état-civil en France est de la compétence des maires ; il n'existe pas de registre d'état-civil national et les pistes explorées en la matière demeurent encore assez vagues. Telle est la première différence avec les systèmes étrangers.

La deuxième est que la France ne dispose pas d'un recueil automatisé des données personnelles des citoyens contrairement aux cas belge, finlandais, suédois, estonien, et de manière générale aux pays nord européens : c'est le principe des registres de population.

La troisième différence est qu'en Espagne, en Italie ou dans des pays disposant d'un registre de population, ce registre est souvent couplé avec un deuxième dispositif : l'utilisation d'un numéro pérenne qui suit l'individu dans de nombreux actes de la vie administrative. C'est un peu le principe du numéro INSEE qui existe en France, mais dont l'usage est strictement réservé à la sphère sociale, médicale. On en a toujours exclu, ou en tous cas encadré, les usages hors de ces champs là, et notamment l'usage pour la carte d'identité. Il n'est pas envisageable que le numéro INSEE soit inscrit sur la carte d'identité.

Le quatrième élément est que, contrairement à la plupart des pays visités, nous ne pouvons pas à ce jour conserver la photographie, donnée lors de la délivrance, dans le fichier informatique des titres. Les données que nous avons la possibilité d'utiliser et de conserver sont uniquement des données alphanumériques, c'est-à-dire les données inscrites en caractère sur le titre. Certes, la photographie ne fait pas tout, mais si nous en disposions, quand un titre est renouvelé, l'agent pourrait s'assurer que la personne qui se présente est la même que celle venue quelques années auparavant, si la photo est relativement ressemblante, et avec toutes les limites que la photographie présente comme garantie. De nombreux pays utilisent cette possibilité, qu'il s'agisse de l'Espagne, de la Grande-Bretagne pour les passeports, et de la plupart des autres pays. Le Ministère de l'Intérieur n'a pas la possibilité de conserver cette donnée.

Cinquièmement, améliorer significativement la fiabilité de nos titres passe aussi par l'aménagement des procédures, notamment en faisant en sorte 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.

D'autres pistes de réflexion complémentaires sont explorées. Dans le contexte français, il est évident que la biométrie, c'est-à-dire conserver la photographie et les empreintes digitales dans l'application des titres, n'est pas la solution à tous les maux. Mais il est aussi clair que la biométrie est un élément fort pour lier un individu à une identité, pour éviter de délivrer à un même individu des titres sous différentes identités ou pour éviter qu'une même identité puisse être utilisée par plusieurs individus. Nous avons des cas réels de ces types de fraude dans le fichier des titres. *A posteriori*, puisque c'est une fois que la fraude est détectée que l'on peut faire ce constat en « remontant la chaîne », on voit qu'une même identité a pu être attribuée à 10 ou 11 individus différents dans 10 ou 11 préfectures et sous-préfectures différentes, dans un laps de temps assez court. Typiquement, c'est une fraude consentante, ce n'est pas une identité usurpée à l'insu d'un individu.

Y a-t-il d'autres moyens que la base de données pour la délivrance des titres ?

La conclusion après les travaux complémentaires que nous avons menés est assez clairement non, dans un système français où il n'y a ni registre de population, ni fichier central de l'état civil, ni numéro universel.

En revanche, cela nous a conduit à approfondir la réflexion sur les protections à mettre en œuvre pour assurer au citoyen que l'usage qui sera fait de ses données biométriques sera bien proportionnel à la finalité de l'application, à savoir la délivrance des titres, et surtout garantisse ses libertés. C'est la raison pour laquelle, au-delà des garanties juridiques que le projet de loi envisage, il y a également des garanties de procédures (notamment des modalités d'anonymisation des données, ce qui ne veut pas dire anonymat, et d'encadrement extrêmement strict des conditions dans lesquelles peuvent être opérés des « *matchings* »).

M. Christian CABAL, Député de la Loire : Je vous remercie. C'est très clair, très précis et complète bien l'intervention de Monsieur Melchior. Je vais maintenant donner la parole à Madame Sophie Meudal-Leenders qui est chef de l'unité de protection des données au Conseil de l'Europe.

Mme Sophie MEUDAL-LEENDERS, Chef de l'unité de protection des données au Conseil de l'Europe

Il n'est pas inutile de commencer cette intervention en resituant le Conseil de l'Europe qui, s'il est l'une des organisations internationales les plus anciennes sur le continent européen, n'est certainement pas la plus connue. Le Conseil de l'Europe a été fondé à Strasbourg au lendemain de la Deuxième Guerre mondiale. Il compte aujourd'hui 46 États membres, c'est-à-dire la quasi-totalité du continent européen à la seule exception de la Biélorussie. Les missions principales du Conseil de l'Europe sont de promouvoir et de renforcer dans les États membres la démocratie, les droits de l'Homme et l'état de droit. En application de ses missions, il a élaboré plusieurs instruments juridiques, notamment son instrument phare, la Convention Européenne des Droits de l'Homme. Toutefois, le Conseil de l'Europe est également à l'origine de l'élaboration de quelque 200 autres conventions dans des domaines très divers du droit.

J'évoquerai plus particulièrement la Convention de protection des données, Convention 108, ouverte à la signature en 1981, un des instruments pionniers de la protection des données en Europe, aujourd'hui ratifiée par 37 États européens, signée (et non encore ratifiée) par 4 autres. Cette convention établit les principes de base de la protection des données de manière assez synthétique, et qu'il revient ensuite aux États qui la ratifient, de mettre en œuvre dans leur droit interne. Il revient également à un comité établi par la convention de veiller à l'interprétation et à l'application de ces principes dans divers domaines du droit ou à diverses technologies. C'est en vertu de cette mission que le comité de protection des données (T-PD), en est venu à s'intéresser à la question de la biométrie. Le T-PD a publié en février 2005 un rapport d'étape sur l'application des principes de la convention à la collecte et au traitement des données biométriques.

Pourquoi un rapport d'étape ? Parce qu'il est apparu à l'époque de la publication de ce document qu'il était trop tôt encore pour parvenir à des conclusions définitives sur la biométrie, par manque d'exemples d'application d'identification à grande échelle. On a essayé de contribuer au débat en cours au niveau des États membres, au niveau international, et de fournir une sorte de guide à ceux qui sont amenés à décider d'utiliser ou non un système biométrique. Si oui,

quelles sont les conditions et garanties qui doivent être envisagées en termes de protection des données ?

Spécificité de la biométrie

- Dignité humaine

La biométrie n'est pas une technologie comme les autres. Elle vient de la personne humaine et en tant que telle, elle peut être ressentie par certains comme une atteinte à la dignité humaine. Les perceptions sont très variables : certaines personnes peuvent être indifférentes à cette idée, d'autres éprouver une résistance psychologique à l'idée que le corps est utilisé comme une source d'information, est banalisé.

- Caractère unique et permanent

Les données biométriques possèdent en principe un caractère unique et permanent qui suit l'individu tout au long de sa vie. C'est un des buts recherchés par les concepteurs de systèmes biométriques. Il devient difficile de dissimuler son identité que ce soit à des fins légitimes (témoins, repentis…) ou à des fins illégitimes, pour des délinquants.

- Probabilité

La biométrie repose de façon inhérente sur les probabilités. De là découlent les taux de faux rejets et de fausses acceptations. Il apparaît qu'il revient au concepteur et au responsable du système d'assumer ce caractère faillible de la biométrie. Il convient pour lui d'adapter le taux de faux rejets et de fausses acceptations en fonction de la finalité attribuée au système. Ceci est particulièrement important pour les applications à grande échelle. Il lui appartient aussi de tester régulièrement le système pour vérifier qu'il est toujours en accord avec la finalité qu'il remplit.

La conséquence de la spécificité de la biométrie fait qu'à notre avis, elle ne devrait pas être utilisée pour de simples questions de confort. Les personnes qui souhaitent utiliser des systèmes biométriques devraient d'abord en évaluer les avantages et les inconvénients pour la vie privée, pour savoir s'il existe d'autres façons moins attentatoires à la vie privée d'arriver au même but.

- Critères de sélection de l'architecture du système

Concernant les critères de sélection de l'architecture du système, la biométrie peut être envisagée dans différentes architectures et toutes ne sont pas égales du point de vue de la protection des données et de la vie privée.

- Distinction entre l'authentification et l'identification

On peut comparer cela à l'emploi d'une voiture ou d'un avion : on peut rouler sur une route avec un avion mais ce n'est peut-être pas la façon la plus économique d'y parvenir. Quand un responsable de traitement veut simplement

authentifier l'identité d'un individu, mieux vaut qu'il utilise un système de vérification et non d'identification.

- L'enrôlement et le stockage de la totalité de l'image biométrique ou simplement du gabarit

Pour la police, il est tout à fait légitime de vouloir stocker l'ensemble des empreintes digitales d'un individu, puisqu'on ne sait jamais quelle partie d'empreinte on retrouvera sur une scène de crime. En revanche, dans le cas d'autres applications où la coopération de la personne concernée est assurée, le stockage du gabarit peut s'avérer suffisant.

L'autre élément important en termes d'architecture concerne le stockage sur un support local comme une carte à puce - on se limite alors aux applications d'authentification - ou dans une base de données. Cette base de données peut être centrale; elle peut également être locale comme en Allemagne où la législation sur les passeports ne permet pas la création d'une base de données biométriques au niveau fédéral ; les bases de données existent au niveau des autorités locales de délivrance des passeports. De même les autorités fédérales n'ont pas un accès automatique aux données. En revanche, pour d'autres finalités, notamment les visas au niveau européen, il est tout à fait légitime d'envisager une centralisation ou alors l'interconnexion de plusieurs bases de données locales

Respect des principes de protection des données

- Collecte et le traitement des données

La dernière partie du rapport envisage plus particulièrement l'application des principes de protection aux données biométriques et les détaille. La collecte et le traitement des données doivent bien sûr s'effectuer dans le cadre de la loi. Dans le domaine privé, elles doivent reposer sur le consentement des personnes.

- Le principe de transparence

Le principe de transparence signifie que la collecte ne doit pas en principe se faire à l'insu des personnes concernées. Les applications de vidéo surveillance déjà évoquées consistant à filmer des gens et à essayer de les identifier devraient se faire dans le cadre strict de la loi.

- Le principe de finalité

Le principe de finalité est essentiel au moment du choix d'un système biométrique pour déterminer la finalité de la collecte et du traitement afin, entre autres, de pouvoir opter entre un système d'authentification et un système de vérification.

- Le principe de proportionnalité

Le principe de proportionnalité est un des plus importants en termes de biométrie puisqu'il a été utilisé par la plupart des autorités de protection des données pour justifier l'autorisation ou le rejet de certains systèmes. On a pu observer plusieurs différences parmi les États membres. Au Danemark, l'autorité danoise de protection des données a autorisé un système basé sur des empreintes digitales pour des cartes de transport en ferry. D'autres autorités, en Italie par exemple, ont refusé ce même système pour l'accès à une banque. Dans plusieurs États européens, il existe des systèmes d'identification des passagers dans les aéroports, basés le plus souvent sur le volontariat. Mais un tel système a été refusé par l'autorité grecque de protection des données. Enfin, en Suisse, l'emploi d'empreintes digitales a été refusé pour le calcul du temps de travail dans une entreprise.

Les données sensibles

Certaines données biométriques, même si ce n'est pas leur finalité, peuvent révéler certaines informations, d'une part sur l'origine raciale des personnes, et d'autre part sur leur état de santé. De telles données sont qualifiées par la convention de « données sensibles », et impliquent à ce titre des garanties particulières de protection. On reconnaît que ce n'est pas le but du système biométrique de chercher à capturer ces données mais quelquefois on ne peut pas l'éviter. Aussi appelle-t-on, les concepteurs de systèmes biométriques à essayer d'éviter dans la mesure du possible la collecte de ces données sensibles.

Le droit d'accès des personnes à leurs données

Toute personne doit pouvoir accéder aux données biométriques qui la concernent et doit pouvoir en demander la rectification ou l'effacement si elles sont erronées. En termes de biométrie, cela implique qu'on lui donne accès à ces données sous une forme intelligible : si on lui donne simplement une empreinte digitale, elle ne reconnaîtra pas forcément que c'est la sienne et *a fortiori* si elle a simplement accès à un gabarit, cela ne signifiera rien pour elle. Cela devrait impliquer qu'elle ait accès à une machine capable de lire ces données ou à une personne qui peut les interpréter pour elle.

M. Christian CABAL, Député de la Loire : Je vous remercie. C'est une approche particulièrement intéressante d'autant qu'elle va être confirmée ou infirmée par Monsieur Christophe Pallez, Secrétaire général de la Commission nationale Informatique et libertés (CNIL).

M. Christophe PALLEZ, Secrétaire général de la Commission nationale informatique et libertés (CNIL)

Ma mission est de faire le point, trois ans après ma dernière intervention dans le même cadre. Je voudrais donc indiquer quels sont les éléments nouveaux, les éléments d'évolution de cette période du point de vue de la CNIL, face à la progression fulgurante de la biométrie que l'on a constatée.

Un cadre légal a été fixé par la loi du 6 août 2004 modifiant la loi « informatique et libertés » de 1978. Ce cadre légal fait que la biométrie est soumise à autorisation de la CNIL 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 le Programme d'expérimentation et de gestion sécurisée et automatisée (PÉGASE).

Lors de la précédente audition, j'avais exposé la doctrine de la CNIL : cette approche reste identique, elle a été maintenue et consolidée. Elle constitue une sorte d'arbre de décision.

Première question : la biométrie laisse-t-elle des traces ou non ? Si la biométrie ne laisse pas de traces, il n'y a pas de difficultés et il y a autorisation de la CNIL, quel que soit le mode de stockage. Si la biométrie laisse des traces, tel est le cas de l'empreinte digitale essentiellement et de l'ADN -mais on n'en est pas encore là dans la pratique-, cela pose une deuxième question : la donnée est-elle conservée sur un support individuel détenu par la personne concernée qui dispose ainsi de la maîtrise du support ou est-elle conservée dans une base de données gérée par le responsable du traitement ? Le support individuel permet d'obtenir le feu vert de la CNIL, alors que la base centrale pose une troisième question : y a-t-il un impératif fort de sécurité ou est-ce que le motif est autre, légitime ou pas ? Cela peut se regarder au cas par cas mais il n'y a pas jusqu'à présent de cas où la CNIL donne une autorisation en l'absence d'impératif de sécurité. C'est donc une progression dans la décision, une grille d'analyse que la CNIL continue d'appliquer actuellement et qu'elle a même poussée jusqu'au bout de sa logique.

En effet, la CNIL vient d'adopter, au cours de sa séance du 27 avril, ce qu'on appelle des autorisations uniques. C'est-à-dire qu'elle a, de manière générale et d'un seul coup, autorisé tout système biométrique reposant sur le contrôle de la main, quelle que soit la finalité. Elle a autorisé spécifiquement le contrôle de la main pour l'accès aux cantines scolaires, qui est un cas particulier avec une

réserve spécifique : le droit des parents et des enfants, s'ils sont majeurs, de s'opposer à cette biométrie pour l'accès à la cantine scolaire. La CNIL a également autorisé une fois pour toutes, tout système biométrique d'empreintes digitales avec cartes à puce, lorsqu'un tel système sert à l'accès aux locaux. Voilà trois décisions structurantes et globales qui montrent l'état de la réflexion de la CNIL.

Par ailleurs d'autres décisions intéressantes ont été prises : ainsi a t-elle autorisé l'usage des empreintes digitales contenues dans une carte individuelle pour l'accès logique, c'est à dire l'accès à une application informatique ou à un poste de travail via un lecteur. Tels sont les éléments de doctrine et de position maintenant bien affirmés et consolidés au travers d'une série de décisions globales.

Ceci n'est qu'un volet du débat dans lequel on se situe. On change incontestablement d'échelle et de problématique, même si on retrouve les mêmes questions de principe, lorsqu'on se penche sur les titres d'identité tels qu'ils ont été évoqués : passeport, visas, carte d'identité électronique. Les enjeux sont bien plus considérables car, comme l'a indiqué Monsieur Bernard Didier, il s'agit de bases de données de dizaines de millions de personnes.

La CNIL ne s'est pas prononcée sur le projet INES. Elle a été saisie de ce projet de loi, mais avant qu'elle ne rende son avis, le gouvernement a décidé de revoir le projet. Elle attend donc une nouvelle saisine à ce sujet. L'essentiel du débat porte sur l'existence ou non d'une base de données. Il est peut-être un peu simpliste de considérer que l'authentification sous-entend l'existence d'un support individuel et que l'identification implique nécessairement celle d'une base de donnée. Il faut se garder de ce schématisme car l'identification peut s'effectuer aussi à travers un support individuel, lorsque la biométrie est combinée à un support dont la fiabilité est assurée par différents moyens, en particulier des moyens de signature électronique, que ce support contient également des données d'identification et d'état civil, et qu'on procède à une opération de contrôle sur ce support, sans recours à une base de données. La combinaison des éléments permet d'obtenir de manière sûre l'identité de la personne. Evidemment il n'en va pas de même pour l'identification d'une personne n'ayant pas de titre ou de carte et qui ne veut pas donner son identité … Mais l'identification n'est pas complètement du côté de la base de données.

La base de données est-elle nécessaire s'agissant de la carte d'identité électronique ? C'est une question fondamentale à laquelle est confrontée la CNIL et qu'elle devra examiner lorsque le projet lui sera de nouveau présenté par le Ministère de l'Intérieur. Cette question renvoie à une autre question, celle de la finalité. Comme Madame Meudal-Leenders l'a évoqué, le principe de finalité implique qu'il convient *a priori* de définir dans quel but on constitue une application stockant les empreintes digitales des personnes.

On a le choix entre deux options. Soit l'application a pour seule finalité la délivrance simple de titres fiables, l'établissement et la vérification de titres d'identité, soit l'application a une autre finalité, qui est une finalité d'identification policière. Le problème est de savoir si ces deux finalités sont retenues et si celles-ci et en particulier la deuxième sont clairement affichées. Pour la première cela ne fait pas de doute, mais la deuxième est le nœud du problème. Si on se borne à une finalité d'établissement et de vérification des identités, une base de données d'empreintes digitales et de photographies est-elle nécessaire ?

Après avoir entendu Madame Sophie Planté, on notera que le raisonnement qui met en avant le lien entre une telle base de données et la fraude à l'identité n'est pas totalement convaincant quand on regarde le cas d'une personne qui entre pour la première fois dans cette base. Lorsqu'une personne entre pour la première fois dans une base, avec éventuellement un état-civil trafiqué, la biométrie n'est d'aucun secours. C'est un point qu'on peut admettre, et inversement, on peut admettre que l'unicité de la délivrance du titre fait nécessairement appel à une base de données.

En revanche, en ce qui concerne les modalités de contrôle de l'unicité de la délivrance du titre à l'aide d'une base de données, différentes options sont possibles - on a évoqué en particulier les notions d'anonymisation, de mouvements unidirectionnels de l'information, etc… pour assurer l'unicité du titre tout en préservant un usage bien délimité des données.

Dans l'hypothèse où une base de données d'empreintes digitales pour la carte d'identité électronique n'aurait que cette finalité de délivrance de titres fiables, on ne peut pas exclure que, dans certaines situations graves, il soit nécessaire d'avoir un accès pour la justice. Dès lors il importe de définir les conditions d'accès restreint faisant que la police agissant dans le cadre judiciaire ou dans un cadre exceptionnel (terrorisme), puisse avoir accès ponctuellement, au cas par cas, à des données figurant dans la base de certification des titres d'identité. C'est une réflexion à mener.

Si on examine maintenant l'autre finalité (non seulement une base de données biométriques du citoyen pour son identité, mais aussi une base servant d'instrument de police reconnu comme tel), une telle finalité doit être très clairement affirmée par le législateur, qui prendra ses responsabilités et qui prendra en compte les risques potentiels et les garanties indispensables liées à une telle finalité.

Il n'est pas toujours évident de faire apparaître ces risques car ce sont des risques potentiels, des risques d'évolution possible. L'un de ces risques est par exemple que, à partir d'un outil aussi puissant qu'une telle base de données, la carte d'identité puisse devenir inutile, c'est-à-dire que l'identification s'effectuera directement par les empreintes, par le corps et non à travers un support, comme on le voit dans certaines expériences. Je laisse de côté toute la problématique pourtant

fondamentale qui fait que chaque citoyen pourrait être considéré comme un suspect …

En ce qui concerne les garanties, si cette finalité policière était admise et décidée par le législateur, on peut imaginer toutes sortes de précautions et de garde-fous figurant dans les procédures d'accès et la manière dont elles sont contrôlées, dans la limitation des contenus, dans la limitation des liens entre les différents contenus, dans les sécurités informatiques et organisationnelles qui font que les accès indésirables ne se feront pas. Tel est l'état du débat actuel qui reprendra dans quelques semaines ou plus tard.

M. Christian CABAL, Député de la Loire : Je vous remercie Monsieur Pallez de cette présentation très condensée. C'était parfait. Je donne la parole à Me Alain Weber, avocat membre de la Ligue des droits de l'homme (LDH)et membre du collectif Droit Et Libertés face à l'Informatisation de la Société (DELIS) et qui intervient fréquemment dans des procès liés à des utilisations abusives de données. Vous donnerez des exemples précis de cas qui motivent votre intervention.

Me Alain WEBER, Avocat, membre de la Ligue des droits de l'homme (LDH) et du collectif Droit et libertés face à l'informatisation de la société (DELIS)

La LDH et le collectif DELIS regroupent une cinquantaine d'organisations de tous les horizons qui s'intéressent à l'informatisation de la société et donc à la biométrie.

Un auteur a écrit que la géographie ça sert d'abord à faire la guerre ; nous, nous disons que la biométrie ça sert d'abord à faire du sécuritaire. Il faut le souligner. Lorsque Monsieur Didier, que j'écoute toujours avec beaucoup d'attention, explique qu'aujourd'hui on dispose d'une technique permettant de prendre des images faciales des individus « à la volée », cela veut dire qu'effectivement on en est là.

Lorsque le Ministère de l'Intérieur, pour lequel j'ai le plus grand respect, explique que la biométrie serait justifiée par le fait qu'on ne sait pas comment identifier quelqu'un, on peut se demander «mais que fait la police ? » et comment a-t-elle fait jusqu'à aujourd'hui en 2006 ? Plus sérieusement – en ce moment même – des milliers de contrôles d'identité sont effectués, dont certains irréguliers sont d'ailleurs condamnés par la Cour de Cassation ; en réalité, l'usage de la biométrie n'est pas nécessaire pour procéder au contrôle de l'identité d'une personne.

On soutient ensuite du côté du Ministère de l'Intérieur qu'il faudrait une certification biométrique pour faire des opérations sur Internet. Je trouve le propos un peu court puisque le Code civil a été enrichi de dispositions concernant la signature électronique et la preuve électronique. Toutes les entreprises ici représentées savent que, depuis le 1er janvier 2006, la TVA est payable avec des certificats électroniques. Il n'y a pas d'éléments biométriques dans ces procédures, et ce sont des milliards d'euros que l'État encaisse par ce biais. Sur ce sujet, l'argument est donc court.

Cinq points seront développés : BIODEV, INES, PNR, RFID, le Support unique.

1. BIODEV

La Ligue des droits de l'homme a constaté des dérives dès l'origine. Il en est ainsi pour le projet BIODEV d'expérimentation, des visas biométriques, selon le décret de novembre 2004. La loi « informatique et libertés » que les Français ont donnée au monde entier implique que lorsqu'on effectue un traitement, on doit déclarer une finalité précise. La finalité précise affichée était d'écarter la fraude documentaire. Cela implique qu'une personne bénéficiaire d'un visa valide peut démontrer – par comparaison de ses empreintes avec les informations la concernant enregistrées dans le composant associé à son visa – qu'elle est bien celle qui en est bénéficiaire. La finalité affichée à savoir, combattre la fraude documentaire et protéger les titulaires de visas n'exige pas la constitution d'une base centralisée des données biométriques collectées.

Cependant le projet BIODEV avait, sans aucune justification pertinente au regard du principe de finalité, procédé à la création d'une base de données biométriques. Cette création était à titre expérimental et les Ministères de l'Intérieur et des Affaires Etrangères devaient procéder à une évaluation du système. Cependant, sans évaluation, un nouveau décret qui a été promulgué le 25 avril 2006, étend très substantiellement le champ d'application du précédent système.

La LDH a attaqué le premier décret, et il en ira de même pour le deuxième puisque à l'évidence, en partant d'une situation de fraude documentaire justifiant la protection des titulaires de visas biométriques, on aboutit à un fichier de police dirigé contre ceux-là mêmes que l'on prétendait protéger.

Désormais, 2600 Officiers de Police Judiciaire (OPJ) sont habilités, selon ce décret, à aller vérifier à l'occasion d'un contrôle quel est l'état de la base. D'un problème d'authentification de titres, on est passé à l'identification d'une personne, d'une population et de flux de populations. Cette dérive est constante en matière de biométrie. La Ligue des droits de l'homme s'interroge sur la façon dont on pourrait l'empêcher. Or il semble qu'il ne soit pas possible de l'empêcher ; manifestement la biométrie recèle cette dérive.

2. Le projet d'Identité nationale électronique sécurisée (INES)

L'autre dérive concerne le projet caméléon d'identité nationale électronique sécurisée (INES). On sait simplement que ce projet est présenté à l'origine pour lutter contre la fraude documentaire. En France, Madame Planté l'a rappelé, il n'existe aucune obligation légale de disposer d'une carte nationale d'identité pour justifier de son identité. Le Code civil ne le prévoit pas. Aujourd'hui pour un citoyen français il n'est pas obligatoire de posséder ce titre, on peut justifier de son identité par différents moyens. On évoque un problème de fraude documentaire - même si on a des difficultés du côté du Ministère de l'Intérieur et de Monsieur le Rapporteur Lecerf à identifier et à chiffrer le phénomène - pour justifier le projet INES.

Mais de cette problématique d'authentification de titres, on bascule de nouveau vers une identification des personnes : c'est-à-dire que l'on ambitionne de créer une base de données de la totalité de la population, ce qui s'appelle un fichier de population. C'est là encore une dérive virtuelle. Il ne s'agit pas de faire un procès d'intention, mais lorsqu'on demande au Ministère de l'Intérieur pourquoi il aurait besoin de ce fichier de population puisque – à supposer INES en place – toute personne pourrait attester de son identité par comparaison de ses empreintes avec les informations la concernant enregistrées dans le titre dont elle est le titulaire, il n'y a pas de réponse. Ce sont donc manifestement des dérives inhérentes à ce système.

3. Le problème des données biométriques à l'étranger : la question des Personal name records (PNR)

Un problème se pose également concernant l'utilisation faite de ces données biométriques ; on constate des situations de « trou noir ». La France et l'Europe ont été contraintes, sous le diktat des États-Unis, à la fois de donner certaines informations concernant les passagers se rendant aux Etats-Unis au travers des PNR ainsi que de fabriquer des passeports biométriques, selon le règlement du Conseil européen du mois de décembre 2004.

La LDH reconnaît que le passeport français est « propre » quand il est lu par les autorités françaises : on a en effet « endormi » les fonctionnalités qui permettraient de se connecter sur la puce d'identification par radiofréquence, - *Radio frequency identification* (RFID) - et de récupérer des éléments biométriques qui y figurent. Mais – la CNIL le relève dans son avis relatif au passeport électronique – il n'en va pas de même concernant les autorités étrangères sur lesquelles il n'y a aucun contrôle. La LDH estime que lorsqu'un État souverain met en circulation un titre, fût-il un titre de nature communautaire, il a l'obligation de garantir à ses nationaux que les données qu'on l'a contraint à y mettre sont utilisées avec transparence et loyauté et que l'on dispose d'accords au niveau international permettant d'obtenir des États tiers, notamment des Etats-Unis, des informations et des garanties sur le stockage de ces données, leur détention, leur

circulation, la durée de conservation etc. Or, en l'espèce, on n'a absolument aucune réponse à ces questions.

Toute personne qui est allée ou qui va aller aux États-Unis avec un passeport biométrique confiera ses données à des inconnus ; ces données sont stockées sur des bases dont on ne sait pas qui les traite, comment elles circulent et comment elles sont stockées ni pour combien de temps. L'État français se montre plutôt cavalier avec ses nationaux alors que c'est l'une de ses obligations impérieuses: s'assurer de la sécurité des donnée personnelles de ses nationaux. Il existe un gros trou noir, sur lequel on n'a aucune réponse et qu'il va falloir combler à bref délai.

4. La puce d'identification par radiofréquence (RFID)

Abordons un sujet que l'on n'a pas beaucoup évoqué : le support lui-même, la puce RFID, puce intelligente que l'on connaît tous : le problème est d'abord sa lisibilité à distance. Pour le passeport français, il faut qu'il soit ouvert, première sécurité, et toutes les données sont cryptées. Cependant, ces barrages existent parce qu'un risque potentiel de lecture à distance existe. Les techniciens expliquent que pour éviter cette lecture, il faut simplement mettre un petit fil d'aluminium empêchant la connectique. On devrait se satisfaire du fait qu'il faut une distance très proche – de l'ordre de quelques centimètres – entre l'émetteur et le lecteur, pour collecter les informations stockées sur la puce. La technique de la RFID consiste, en effet, à titiller un émetteur qui va transmettre les informations biométriques. Un récepteur éloigné serait impuissant à recevoir des informations d'un émetteur distant. La LDH ne se satisfait pas de ce discours. Il est en effet constant que le gouvernement américain vient de mettre en place un système pour ses propres nationaux, concernant les Américains qui veulent voyager au Canada et au Mexique, avec une puce RFID dont la lisibilité atteindra 9 mètres. On est loin des quelques centimètres évoqués auparavant.

On ne peut pas, dans cette matière où la loi de Moore est connue de tous – on double les capacités de stockage / on réduit les délais de traitement par deux tous les dix-huit mois – soutenir qu'on se limitera, en France, à de petites préconisations salvatrices alors que l'on est tous sous la pression des Etats-Unis dans ces domaines. J'ai participé récemment à un débat où l'on m'a dit « si vous ne voulez pas aller aux Etats-Unis, vous restez là ». Je réponds que je suis citoyen européen, et que j'ai envie de voyager de par le monde parce que c'est ma liberté de circuler. Le fait que l'on me contraigne un jour à disposer d'un titre, lisible à une distance que personne ne peut aujourd'hui honnêtement limiter, dont les données seront captables à distance, à mon insu, pour des usages secrets, est une vraie problématique des droits de l'Homme, des droits de la vie privée, et de la liberté de circulation des personnes.

Prenons l'exemple excellent de Monsieur Didier qui expliquait qu'on peut capter « à la volée » des images faciales, car cela fonctionne techniquement. La loi contre le terrorisme récemment votée permet de filmer les grands rassemblements,

c'est-à-dire notamment les manifestations républicaines comme ont pu l'être les manifestations contre le Contrat première embauche (CPE). Dès lors que le droit l'autorise et que la technique le permet, la LDH entend expliquer qu'il existe un danger éminent que tous les gens manifestant en France finissent un jour dans un fichier de police, quels que soient les motifs de leurs manifestations, puisque la finalité affichée de ces traitements est de trouver éventuellement dans ces grands rassemblements des personnes susceptibles de commettre des infractions. La biométrie, que l'on connaît depuis plusieurs siècles, associée aux supports RFID dont personne aujourd'hui ne peut dire la limite, crée un outil qui recèle une vocation totalitaire. La Ligue des droits de l'homme se bat pour faire entendre ce message de précaution.

Le groupe 29 du Conseil de l'Europe, c'est-à-dire tous les Commissaires aux données des CNIL des états membres, considère qu'il faut faire attention et regarder toutes les applications et toutes les implications. Il est sûr qu'un lobby industriel français de la biométrie existe, qu'il veut ses parts de marché et qu'il se bat pour y parvenir ; c'est tout à fait son rôle, ce n'est pas critiquable. Il n'en demeure pas moins qu'existent des enjeux extrêmes sur le terrain des libertés et de la citoyenneté, d'autant plus que la donnée biométrique elle-même, unique, pérenne, irrévocable, permettra un jour toutes les interconnexions.

5. Le support Unique

On apprend, et on peut s'en étonner, que le Ministère de l'Intérieur ne connaît pas la fraude sur les permis de conduire et qu'il lui faut se tourner vers le monde universitaire pour obtenir des informations. On parle d'un million de faux titres. Il n'en demeure pas moins qu'avec ce million prétendu de faux titres, si un jour on a des éléments biométriques à l'intérieur, on va le coupler avec une carte d'identité, puis pourquoi pas avec la carte Vitale et éventuellement avec une carte fiscale et puisque cela fera quatre cartes, dès lors pourquoi ne pas unifier tout cela puisque la donnée biométrique est unique et donc constitue un outil idéal pour interconnecter des fichiers. Il y a ainsi un glissement quasi-inéluctable quand la biométrie est appliquée aux citoyens vers un support unique. On tend alors vers un régime policier. C'est contre cette tendance que la LDH et que DELIS se battent.

M. Christian CABAL, Député de la Loire : Je vous remercie beaucoup. Pour clore ces présentations, je donne la parole à Monsieur Beland qui est Expert sécurité et sûreté de l'Organisation internationale de l'aviation civile (OACI). Nous aurons des explications sur l'origine et le développement des techniques biométriques, qui sont largement utilisées puisque je crois que vous allez nous donner des statistiques sur le nombre de voyageurs aériens et les différents problèmes que cela entraîne.

M. Michel BELAND, Expert sécurité et sûreté de l'Organisation internationale de l'aviation civile (OACI)

Monsieur le Président, Mesdames et Messieurs, je vais essayer de vous présenter un survol rapide du cheminement de l'OACI vers l'utilisation de données biométriques.

Pourquoi l'OACI s'intéresse-t-elle à la biométrie ?

L'OACI s'intéresse à la biométrie à cause de la convention relative à l'aviation civile internationale de Chicago, qui date de 1944. Cette convention a été ratifiée par 189 États qui ont convenu de certains principes, exigences et arrangements régissant l'aviation civile. Trois de ces exigences traitent de la simplification des procédures d'entrée et de congé du territoire d'un État : respect des lois relatives à l'immigration, aux douanes, aux passeports (Art. 13), simplification des formalités relatives à la navigation aérienne (Art. 22), établissement des procédures harmonisées en matière de douane et d'immigration (Art. 23).

L'OACI a donc publié des normes relatives aux passeports, aux visas et aux documents de voyage officiels. Évidemment, elle ne l'a pas fait uniquement pour l'aviation, ni dans un cadre isolé. Elle a collaboré avec d'autres organisations internationales comme Interpol et l'Organisation Internationale du Travail (OIT) en ce qui concerne les documents de voyage des marins.

Depuis 1980, l'OACI publie également des spécifications relatives aux documents de voyages lisibles à la machine, *Machine readable travel documents* (MRDT), c'est-à-dire les passeports, les visas et les documents officiels de voyage. On retrouve ces spécifications dans le manuel OACI « Documents de voyage lisibles à la machine » (DOC 9303), publié en trois parties, soit une pour chaque type de document.

Depuis quelques années le passeport lisible à la machine a été mis en place. Je concentrerai mon exposé uniquement sur le passeport parce que c'est intéressant au niveau des données biométriques. La majorité des administrations nationales connaissent bien les spécifications de base pour les passeports lisibles à la machine émis par au moins 110 États.

Sur le passeport lisible à la machine, le format standard comporte une zone d'inspection visuelle (ZIV) et une zone de lecture automatique (ZLA) lisible à la machine qui répète les informations contenues dans la zone d'inspection visuelle. La zone de lecture automatique présente l'avantage de pouvoir être lue à la fois à la machine et à l'œil nu. Elle recoupe les informations figurant dans la zone d'inspection visuelle, et lui est complémentaire. Y figurent : le numéro du

passeport, la citoyenneté, le sexe, la date de naissance, la date d'expiration du passeport, et quelques chiffres pour contrôler la validité du document, ce qui correspond aux données figurant dans la zone d'inspection visuelle.

Pourquoi un passeport et pourquoi lisible à la machine ?

Un passeport est utile pour confirmer l'identité du détenteur qui se déplace d'un pays à l'autre sur un plan international. La photographie sur le document facilite évidemment l'identification du porteur du document. Au fil des années, l'OACI a publié des spécifications de plus en plus strictes et précises sur la qualité des photographies. On en est même arrivé à recommander très fortement que la photographie soit imprimée directement sur la page du document de voyage, et non pas collée, pour que l'identité soit plus facilement vérifiable.

Pourquoi une vérification d'identité plus précise ?

Au fil des ans, et ce même avant le 11 septembre 2001, les États ont reconnu les difficultés liées à l'usurpation d'identité. Ils ont jugé nécessaire d'élaborer des méthodes plus efficaces pour vérifier les informations contenues sur les documents de voyage. En effet, les failles au niveau de l'identification et donc de la sécurité des documents de voyage peuvent avoir des conséquences sociales assez sérieuses, allant de l'usurpation d'identité jusqu'au terrorisme, en passant par les déplacements illégaux, les trafics, la contrebande. Finalement la question de l'usage de la biométrie s'est posée.

La biométrie peut-elle faciliter la vérification ou l'authentification de l'identité du détenteur du document ?

L'OACI s'est penchée sur cette question pendant neuf ans. De 1997 à 2003, le groupe consultatif technique sur les documents lisibles à la machine a étudié les possibilités offertes par la biométrie pour une identification plus fiable des détenteurs de passeports. En 2003, le groupe a soumis une recommandation en quatre volets au Comité des transports aérien (CTA) du conseil de l'OACI. Le Comité a approuvé la recommandation et l'a déférée pour inclusion dans un amendement à l'annexe 9, à la douzième session de la division de facilitation qui constitue vraiment le forum international pour discuter de ces données et décider si on doit ou non en venir à une norme.

En 2004, les 474 représentants de 87 États de la deuxième session de la division ont étudié la recommandation et ont jugé prématuré de proposer une norme. Ils ont opté pour une pratique recommandée invitant les États à incorporer les données biométriques dans les passeports. Cette pratique recommandée a été inscrite à l'annexe 9 avec le 19ème amendement adopté en 2005. Les spécifications techniques pour l'intégration des données biométriques dans les passeports seront publiées avant le début de l'automne 2006. La recommandation prévoit l'utilisation de données biométriques dans les documents de voyage lisibles à la machine (MRTD), l'utilisation de puces sans contact pour stocker ces données,

l'élaboration d'une structure logique des données et que, celles-ci soient protégées par une signature numérisée sur la base du système de gestion des clefs publiques, *Public key information (*PKI), pour en garantir l'inviolabilité.

Pour les documents de voyage, le passeport a été établi qu'il n'était pas souhaitable de choisir la biométrie la plus performante pour ensuite ajuster les exigences en matière de document de voyage. L'OACI a donc décidé d'évaluer la technologie disponible en fonction des exigences précises de délivrance et d'inspection des documents de voyage, que ces données soient stockées, liées aux documents de voyage, et non de se satisfaire de l'évaluation de la technologie disponible. Par cette approche, l'OACI s'est distinguée des principaux courants de pensée.

Les exigences

Pour les documents de voyage, pour le passeport, l'OACI a préféré procéder à partir des exigences précises. Ces exigences étaient les suivantes :

- compatibilité avec les exigences d'émission et de renouvellement de documents de voyage,

- compatibilité avec les exigences de vérification d'identité à la machine lors de l'émission et de l'inspection du document,

- vérification par redondance, c'est-à-dire par complémentarité en recoupant avec l'information déjà inscrite sur le passeport,

- perception publique, non seulement au niveau de la fiabilité de l'information mais surtout sur la sécurisation des données,

- exigences de stockage des données posant la question de leur protection,

- performance au niveau des points d'entrée des contrôles de police dans les pays pour accélérer l'accès des voyageurs sur les territoires.

Un choix s'est imposé face à ces considérations.

- La reconnaissance faciale

La reconnaissance faciale est arrivée en tête de compatibilité avec un taux évalué à 85 %, suivi au même niveau par l'empreinte digitale et l'iris avec une compatibilité des besoins identifiés à 65 %. La reconnaissance faciale ou le visage sera publié dans les spécifications techniques comme étant l'élément essentiel pour l'intégration de données biométriques sur le passeport en laissant l'option aux États qui le désirent d'ajouter l'empreinte digitale et l'iris.

Pourquoi le visage ? Finalement, le visage facilite l'authentification par l'observation, l'engagement ou la coopération de l'individu n'est pas requis comme tel, et cette technique permet de confirmer l'identité du détenteur de document à 100 %, en comparant avec la photo. La photo est utilisable pour les vérifications à la machine, et même de façon visuelle si l'équipement ne

fonctionne pas. Le visage constitue l'élément principal, donc obligatoire pour l'identification biométrique sur les passeports. Chacun a une image faciale facile à capter. La vérification de l'identité peut être effectuée quel que soit le niveau de sophistication de la méthode utilisée.

Comment stocker toutes ces données? La puce sans contact dite "de proximité" qui est lisible jusqu'à une distance de 10 cm offrait les meilleures possibilités ; la puce sans contact permet de comparer la donnée stockée sur la puce et la photo, au visage de la personne.

- La puce sans contact

Pourquoi a-t-on choisi la puce sans contact ? Il fallait un médium de stockage qui offrait une certaine fiabilité, suffisamment d'espace et certaines garanties au niveau de la sécurisation. L'utilisation d'une puce sans contact offrait suffisamment de capacité pour stocker les images, une technologie offrant une interopérabilité globale impliquant qu'une puce programmée dans un État puisse être lue par un autre État et une compatibilité avec les passeports de type livret.

Pour ce faire, il faut donc organiser la structure des données enregistrées, selon la recommandation, de façon à obtenir une interopérabilité globale. Les données inscrites sur une puce pouvant être remplacées, on a exigé une signature numérisée, cryptée, sur la base du système de gestion des clefs publiques (Public key information (PKI). Avec la signature numérisée, les données sont enregistrées, cryptées à l'état A et sont lues dans l'état B avec le décryptage. Il est évident que la technologie PKI offre certaines faiblesses et il peut y avoir certains piratages de données, même si la spécification choisie pour la puce l'est pour une lecture à une distance de 10 cm, et non pas de 9 m.

Lors de la vérification des puces et des lecteurs, on a jugé nécéssaire de pallier une faible éventualité d'écoute indiscrète ou de piratage. On a décidé qu'il fallait contrôler l'accès qui s'effectue par l'insertion d'une clé. Située à même le passeport, cette clé recoupe les données lisibles à la machine avec les données de la puce. Cette clé ne peut être lue que par un lecteur légitime qui fera la lecture numérisée du passeport avec la puce, dans la zone de lecture automatique. Il faut donc que le passeport soit ouvert et qu'il soit sous le lecteur pour que la clé donne accès aux données biométriques numérisées. Le détenteur peut être assuré que les données sont protégées tant et aussi longtemps que le passeport est fermé et tant et aussi longtemps que le passeport n'est pas remis à l'officier de police pour contrôle. Ces spécifications de l'OACI seront publiées dans la 6ème édition du manuel « traitement des documents de voyage lisibles à la machine », en première partie.

La première partie du manuel sera publiée en deux volumes. Le premier volume traite uniquement du passeport lisible à la machine qui contient toutes les données requises sur un passeport, qu'il soit lisible à la machine ou non. Il y a évidemment la bande au bas du passeport qui est lisible à la machine. Le

deuxième volume, contiendra des spécifications pour le passeport électronique, c'est-à-dire le passeport lisible à la machine qui incorporera les données biométriques. La donnée biométrique obligatoire est le visage, et en option pour les États qui désirent utiliser ces données : l'iris et l'empreinte digitale. Ce manuel sera disponible à la fin de l'été. Des informations additionnelles sur les documents lisibles à la machine sont disponibles sur un site web, uniquement en anglais : www.icao.int/mrtd (*Machine readable travel documents*). Il y a de nombreuses informations sur ce site.

M. Christian CABAL, Député de la Loire : Je vous remercie pour cette présentation qui vient compléter la journée compte tenu des différents thèmes évoqués, certains un peu rapidement. J'ouvre donc les débats sur l'ensemble de la journée, sans refaire une hiérarchie des différents thèmes parce que finalement plusieurs questions sont transversales, complémentaires ou se superposent. Vous avez la parole.

M. Bernard DIDIER, Directeur scientifique et du développement des affaires (division sécurité de Sagem Défense Sécurité) : J'aurais déjà une recommandation à faire : pour la prochaine audition, prévoyez une journée.

M. Christian CABAL, Député de la Loire : Je réponds tout de suite. C'est la disponibilité des salles de l'Assemblée, liée à des travaux qui commenceront dans quelques jours qui explique cela. Cette salle par exemple, sera fermée pour presque deux ans.

M. Bernard DIDIER, Directeur scientifique et du développement des affaires (division sécurité de Sagem Défense Sécurité) : Je voudrais revenir sur les propos tenus avec beaucoup de conviction par Me Alain Weber sur le thème « État cavalier ». Je ne me sens pas agressé puisque l'objectif de cet après-midi est que chacun des participants fasse connaître l'état de l'art et de la situation. Pour qu'il y ait échange, il faut savoir ce qui se passe. C'est pourquoi nous participons au débat citoyen. Si l'on reprend les termes « État cavalier », en tant qu'industriels, ce n'est pas ce que nous ressentons en France : le couple CNIL/ Administration fonctionne. Un véritable challenge existe sur les problèmes que vous évoquez. Je ne considère pas que des raccourcis soient faits. En tant qu'industriels, nous ne l'avons pas senti.

Vous expliquez que vous êtes inquiets sur l'accès aux données personnelles, j'aurais donc une recommandation à vous faire, et qui serait intéressante à regarder. En matière de biométrie, on parle du *match-on-card* (MOC) qui consiste à mettre dans une carte des données biométriques qui ne vont plus en sortir. Mais en donnant une information biométrique (empreinte digitale, iris) la carte pourra ou non se déverrouiller pour accéder à des informations pouvant être sensibles. Pourquoi ne pas utiliser la biométrie pour répondre aux inquiétudes que vous exprimiez tout à l'heure pour protéger directement l'ouverture des données du passeport ? Vous voyez la biométrie peut aussi répondre à des problèmes de protection des données personnelles.

Comme l'a évoqué Monsieur Beland, on constate que les États et les organisations se sont penchées sur la question du déverrouillage du passeport. D'autres États réfléchissent à des mécanismes encore plus compliqués que le *basic access control*. Une véritable réflexion de la part des acteurs pour assurer un équilibre entre protection des données individuelles et sécurité existe. Évidemment la discussion porte sur la position du curseur mais il n'y a pas de raccourci, je ne l'ai pas senti.

Me Alain WEBER, Avocat, membre de la Ligue des droits de l'homme (LDH) et du collectif Droits et libertés face à l'information de la Société (DELIS) : Quand je dis que l'État est cavalier, je ne mets pas la CNIL dans l'État. La CNIL est une autorité administrative indépendante, elle n'est pas l'État.

M. Bernard DIDIER, Directeur scientifique et du développement des affaires (division sécurité de Sagem Défense Sécurité) : J'évoquais ces échanges, ce challenge sur tous ces sujets, et j'ai le sentiment qu'il fonctionne.

Me Alain WEBER, Avocat, membre de la Ligue des droits de l'homme (LDH)et du collectif Droits et libertés face à l'information de la Société (DELIS) : Votre sentiment est tout à fait respectable. Je ne souhaite pas que la discussion soit perçue comme une agression. J'ai rebondi sur ce que vous évoquiez concernant la possibilité de prendre des images faciales « à la volée », ce qui est un élément qui nous inquiète énormément. Quelles que soient les garanties que vous pouvez prendre ensuite, cette possibilité existe, la technique l'autorise. Je ne peux pas penser que l'on aura toujours une utilisation démocratique de ces éléments captés à la volée.

M. Bernard DIDIER, Directeur scientifique et du développement des affaires (division sécurité de Sagem Défense Sécurité) : Si j'ai signalé cet élément, chacun doit le prendre en compte. Monsieur Christophe Pallez connaît depuis longtemps ma position sur le concept de traces qui évolue avec les évolutions technologiques. C'était simplement pour expliquer qu'une évolution technologique a eu lieu. Aujourd'hui, la trace n'est plus ce concept qui dans le passé correspondait à une trace physique qu'on a laissée. La trace devient numérique, vous laissez des traces sur Internet, dans les boites vocales, cela participe au débat. Pour moi, il n'y a pas de bonne ou de mauvaise biométrie, il y a de bons et de mauvais usages. On est ici pour en débattre.

Mme Sophie PLANTÉ, Adjointe au Directeur du programme INES : Je voudrais apporter une précision sur une crainte mentionnée par Me Weber, concernant la constitution d'un fichier de population. Dès lors qu'un titre n'est pas obligatoire, - et la France est un des rares pays européens dans lequel la carte d'identité n'est pas obligatoire -, on ne peut pas accuser le Ministère de l'Intérieur de vouloir constituer un fichier de population. Globalement aujourd'hui, deux tiers des Français possèdent une carte d'identité. Personnellement, je n'en possède pas. Si on ne veut pas que ses données soient utilisées dans le traitement, on peut

toujours se passer de carte. Le caractère facultatif de la carte est un élément fort par rapport à un équilibre à respecter entre la protection des données personnelles et la finalité du traitement, au regard des menaces potentielles sur les libertés individuelles.

Par ailleurs, la première délivrance du document pose une vraie question, et la biométrie n'est pas la solution miracle. Ce problème fait partie des travaux que nous menons et des garanties de procédure que je mentionnais de manière assez succincte, pour faire en sorte de ne pas figer une mauvaise identité lorsqu'on délivrera le premier document.

Me Alain WEBER, Avocat, membre de la Ligue des droits de l'homme (LDH) et du collectif Droits et libertés face à l'information de la Société (DELIS) : A l'origine, le projet prévoyait que la carte d'identité serait obligatoire. Maintenant c'est présumé non obligatoire. Il n'en demeure pas moins que le Sénateur Lecerf explique dans son rapport qu'il ne comprend pas comment on répondra à la finalité de combattre la fraude documentaire, voire accessoirement le terrorisme, en ayant un fichier facultatif. Il y a donc une interrogation.

En prospective, on peut penser que l'État, ne serait-ce que pour des motifs financiers, ne pourra pas gérer deux systèmes à la fois : le système actuel résultant de la carte Pasqua dite infalsifiable à l'époque, et un système biométrique. A court ou moyen terme, il est évident que cette dualité de système sera incompatible, et l'on se dirigera nécessairement vers une unicité de système. D'autant plus si des facilitations de la vie, des accès à des services sont liés à la détention d'un titre biométrique. Ce sera donc une obligation non écrite, mais indirecte.

M. Christian CABAL, Député de la Loire : Dois-je conclure de votre silence que votre information est suffisamment complète ou que la lassitude l'emporte sur la curiosité intellectuelle ? En fait, nous n'avons pas à convaincre tel ou tel d'entre nous. Nous avons à nous informer, certains ont à débattre. Il a été fait mention de la représentation nationale qui aura ses responsabilités à mettre en jeu, et de l'attitude compréhensive, mais ferme sur les principes qu'a adoptés la CNIL, entité que ceux qui n'en ont pas encore nous envient en raison de son expérience et de la qualité de ceux qui l'animent.

Conclusion par M. Christian Cabal, Député de la Loire

Je considère que nous avons pu apporter les éléments complémentaires utiles sur ce que doit être ou ce que devrait être la biométrie, pour la première fois à une échéance courte. En effet, on se trouve encore dans une phase expérimentale pour les visas, étendue à une partie très importante de la population.

S'agissant de la carte d'identité, le Parlement aura à prendre en compte et à approuver ou pas le projet de loi qui en toute hypothèse peut être amendé, si tant est que ce projet soit amené à être discuté avec la majorité actuelle, pour des raisons de calendrier.

Par conséquent, si nous n'avons pas d'autres éléments à ajouter à ces débats très intéressants où chacun a pu s'exprimer sans réserve ni retenue, je crois que nous pourrons faire notre miel des informations recueillies, en tirer toutes les conséquences fonctionnelles dans les responsabilités qui sont les nôtres, et nous retrouver peut-être avant trois ans, après une expérimentation grandeur nature pour dresser un bilan. Le principe de procéder à l'évaluation d'une nouvelle disposition législative est généralement acquis. Il y aura toujours la possibilité de corriger le tir, si cela est nécessaire, à une échéance moyenne.

Néanmoins, je souhaiterais revenir sur un point concernant le passeport électronique et notamment les informations qui y figurent. Même si celles-ci ne sont pas *a priori* accessibles à d'autres que ceux qui les contrôlent et veulent les contrôler, tel le service de l'immigration américaine, cela constitue une obligation de fait et de droit assez choquante pour certains. Si l'on se fonde sur les débats à ce sujet au Parlement Européen, qui est assez vigilant sur ces questions, la réponse habituelle est : si vous voulez vous rendre aux États-Unis, il faut bien accepter les conditions que mettent les Américains pour l'accès à leur territoire. Il faut reconnaître que compte tenu des événements qu'ils ont vécus dans leur chair, c'est un argument qui porte. Il ne faut pas non plus guider sa vie civique sur des sentiments et sur des émotions, cependant cet argument existe, et il est incontournable. La liberté de circuler n'est valable que pour autant qu'elle ne gêne pas la sécurité des autres, sinon on circulerait dans n'importe quelles conditions. On est vraiment effectivement aux limites de ce qui possible, mais je ne peux pas exiger la liberté d'aller aux États-Unis selon mes règles, en contradiction totale avec les lois et les impératifs de tel pays. C'est un point qui ne souffre pas beaucoup de discussions.

Néanmoins, cela ne dispense pas d'assurer le maximum de sécurité sur les informations contenues. Encore faut-il en mesurer le coût avantages / inconvénients, tout en sachant que ces discussions sont un peu théoriques. Les

grandes puissances disposent de moyens pour accéder à des informations confidentielles sans aucun problème. Si la CIA écoutait nos discussions aujourd'hui, elle s'étonnerait de notre réaction perfectionniste parce qu'elle sait très bien comment faire pour accéder à toutes les informations. Le problème est de savoir quel effort on fait, quel moyen financier on investit pour cela. Il est évident que ce qui est possible dans quelques cas, ne l'est pas à l'échelle d'une population. Pour autant, cela ne doit pas nous amener à baisser la garde, bien au contraire.

C'est pourquoi les avis de la CNIL sont lus avec intérêt et attention, notamment au niveau du Parlement. C'est un élément essentiel qui permet de prendre en considération les potentialités d'éventuelles dérives sécuritaires, et de faire en sorte qu'on puisse trouver le moyen de concilier la nécessaire sécurité s'imposant dans toute société dite moderne, avec les impératifs de liberté individuelle. Je suis convaincu, après avoir eu l'occasion de réfléchir sur ces questions, que c'est possible.

Il y a des règles à définir, des méthodes à respecter, des contrôles à effectuer régulièrement. Les différentes instances mises en place, même si elles ne sont pas toujours parfaites, peuvent être perfectionnées et atteindre un niveau de résultat qui satisfasse tout le monde. Les contacts se poursuivent régulièrement. En ce qui me concerne c'est le cas, et je pense que vous en faites autant.

La biométrie existe et existera, cela ne sert à rien de mener un combat d'arrière-garde qui serait un peu passéiste. Dans ce cadre et avec toutes les précautions qu'on vient d'évoquer aujourd'hui, il me semble très important que la France et l'Europe continuent d'occuper une position influente au plan international avec ce que cela comporte en termes d'exemplarité vis-à-vis des autres États, et en termes de retombées économiques importantes car des chiffres ont été donnés.

Il faudrait éviter que par excès de précaution, - mais où se situe un tel excès ? - on se trouve dans la situation où l'essentiel de l'activité se déroulerait à l'étranger, ce qui serait dommageable de manière globale. Ceci n'est pas la priorité, mais je crois qu'il faut éviter de se faire des crocs en jambe involontairement et de voir les autres passer devant. Dans le domaine de l'économie, il existe toute une série d'exemples d'application de technologies, pour lesquels nous payons très cher un terrain laissé vacant et qui ne le reste pas.

Tels sont donc les points ayant pu être abordés aujourd'hui. Je remercie chaque intervenant. Vous avez manifesté beaucoup de patience et votre contribution a été particulièrement utile et nécessaire pour compléter le rapport présenté, il y a deux ans et demi. J'espère que nous nous retrouverons tous dans cette distance de temps, que d'ici là des progrès auront été accomplis.