N° 938	N° 355
ASSEMBLÉE NATIONALE	**SÉNAT**

CONSTITUTION DU 4 OCTOBRE 1958

DOUZIÈME LÉGISLATURE	SESSION ORDINAIRE DE 2002 - 2003
Enregistré à la présidence de l'Assemblée nationale Le 16 juin 2003	Annexe au procès-verbal de la séance du 12 juin 2003

OFFICE PARLEMENTAIRE D'ÉVALUATION
DES CHOIX SCIENTIFIQUES ET TECHNOLOGIQUES

RAPPORT (3ème partie)

sur

LES MÉTHODES SCIENTIFIQUES D'IDENTIFICATION DES PERSONNES À PARTIR DE DONNÉES BIOMÉTRIQUES ET LES TECHNIQUES DE MISE EN OEUVRE

Par M. Christian CABAL,
Député

Déposé sur le Bureau de l'Assemblée nationale	Déposé sur le Bureau du Sénat
par M. Claude BIRRAUX, *Président de l'Office*	par M. Henri REVOL, *Premier Vice-Président de l'Office*

Recherche

TABLE DES MATIERES

PREMIERE PARTIE DU RAPPORT

DEUXIEME PARTIE DU RAPPORT

TROISIEME PARTIE DU RAPPORT

Recommandations

Recommandation n°1 :

Des dispositions législatives devront préciser les conditions dans lesquelles des autorités publiques pourront être habilitées à accéder à des fichiers gérés par des personnes publiques ou privées et comportant des données biométriques ainsi que les conditions dans lesquelles elles pourront procéder au recoupement de tels fichiers. De telles dispositions devront être systématiquement portées à la connaissance des personnes dont une donnée biométrique sera enregistrée, sous réserve des dispositions spécifiques applicables aux fichiers de police.

Recommandation n°2 :

Le Parlement devra être systématiquement informé des travaux conduits, notamment, dans le cadre des groupes de travail du G8, de l'OACI et au sein de l'Union européenne et relatifs à l'introduction de données biométriques dans les documents et titres de voyage et de séjour ainsi que de la préparation de conventions internationales organisant le transfert de telles données.

Recommandation n°3 :

Un observatoire devra être constitué, associant les représentants des différentes administrations, des médecins, des universitaires et des chercheurs, des industriels, des associations de consommateurs ou d'usagers et la CNIL.

Cet observatoire sera chargé d'assurer une veille juridique, scientifique et technologique dans le domaine de la biométrie, de suivre l'évolution des dispositifs mis en oeuvre aux plans national, européen et international ainsi qu'à l'étranger et de veiller à ce que la France soit représentée dans les différentes instances techniques d'évaluation et d'élaboration des normes.

Un rapport public devra rendre compte régulièrement des évolutions constatées et des incidences financières et juridiques au plan national des mesures prises et envisagées.

Recommandation n°4 :

Devra être envisagée la mise en place d'un organisme associant des personnes publiques et privées et doté des moyens de financement nécessaires :

- pour faire réaliser par des laboratoires indépendants des travaux d'évaluation et de recherche sur les techniques biométriques d'identification des personnes ainsi que sur les procédés techniques de lutte contre la fraude documentaire,

- pour recueillir l'avis d'experts ou d'universitaires sur la fiabilité des résultats de travaux menés dans ce même domaine par d'autres organismes,

- pour diffuser les travaux conduits en son sein et gérer les ressources documentaires.

Examen du rapport par l'Office

Mardi 10 juin 2003 - Présidence de M. Claude Birraux, député, président de l'Office.

Les méthodes scientifiques d'identification des personnes à partir de données biométriques et les techniques de mise en œuvre – Examen du rapport

L'Office a examiné **le rapport** présenté par **MM. Christian Cabal, député**, sur la saisine émanant du Bureau de l'Assemblée nationale et portant sur **les méthodes scientifiques d'identification des personnes à partir de données biométriques et les techniques de mise en œuvre.**

M. Christian Cabal, député, rapporteur a indiqué que, face à l'ampleur du sujet, il avait limité ses travaux aux systèmes automatisés qui, sur la base d'une donnée biométrique, anatomique telle qu'une empreinte digitale, une image du visage, d'un œil, la forme d'une main par exemple, ou comportementale, comme un geste, une voix, permettent de reconnaître un individu, quasiment en temps réel, les méthodes reposant sur un travail d'expertise ou des procédés d'observation plus complexes étant néanmoins évoquées, sans faire l'objet d'une étude approfondie.

Les débats en cours portent en effet sur les systèmes qui identifient rapidement des personnes, sans être « intrusifs » et qui peuvent, le cas échéant, traiter une masse parfois importante de données biométriques.

Schématiquement, les systèmes biométriques se proposent de comparer deux (authentification) ou plusieurs (identification) échantillons et de déterminer s'il y a ou non ressemblance. A partir de cette ressemblance ou de cette différence, on conclut que les deux échantillons apparentés proviennent de la même personne ou, au contraire, en cas de non apparentement, que les échantillons proviennent de personnes distinctes.

M. Christian Cabal, député, rapporteur, a formulé plusieurs constats à partir des entretiens qu'il a eus, de l'audition publique qu'il a organisée le 15 mai 2003 et des missions qu'il a effectuées aux Etats-Unis et au Japon.

D'une part, dans le domaine de l'évaluation des systèmes biométriques, il n'y a pas vraiment de consensus :

- les travaux sont fragmentés et la plupart des pays européens ont pris du retard,

- les travaux réalisés aux Etats-Unis et au Royaume-Uni restent controversés, ce qui explique que l'on recherche des normes d'évaluation admises par tous et suffisamment fiables,

- peu d'évaluations font intervenir de manière systématique des experts médicaux. Ceci est regrettable, car l'analyse du corps humain, comme l'examen de l'innocuité des procédés d'observation, nécessitent des compétences médicales,

- enfin, les évaluations se heurtent à deux écueils : le secret des algorithmes de reconnaissance et l'existence de « technologies propriétaires » d'une part, et, d'autre part, la constitution de bases de données presque exclusivement liées à la sécurité publique. Cependant ces obstacles ne sont pas intangibles : le National Institute of Standards and Technology (NIST) américain a pu ainsi réaliser récemment, grâce à la collaboration notamment du FBI, des tests d'évaluation portant à la fois sur les empreintes digitales, la reconnaissance faciale et l'iris.

D'autre part, les besoins tant collectifs qu'individuels d'authentification et d'identification vont se développer, dans le monde physique, comme électronique, et les enjeux politiques, sociaux, financiers et économiques des choix sont importants, ce qui justifie à la fois un contrôle parlementaire réel, une plus grande transparence et une meilleure collaboration des acteurs privés et publics. Beaucoup de gouvernements, d'institutions et d'industriels mènent actuellement des réflexions sur les identifiants et sur les moyens de lutter efficacement contre la fraude documentaire et informatique dont le coût est loin d'être négligeable.

M. Christian Cabal, député, rapporteur, a ensuite précisé le contenu de son rapport, lequel est organisé sur deux plans.

Dans une première partie, sont présentés les principales techniques, leurs principes de fonctionnement et les appréciations portées à leur sujet, tant en ce qui concerne leurs performances que les avantages et les risques liés à leur utilisation.

On assiste à une diversification croissante des produits, qu'il s'agisse des données physiques ou comportementales prises en compte - empreinte

digitale, face, main, iris, rétine, voix, odeur, oreille, démarche, frappe sur le clavier…- comme des procédés de capture de ces données - rien que pour l'empreinte digitale, sept techniques différentes d'acquisition ont été ainsi recensées – ou encore des algorithmes de comparaison.

Cette diversification rend d'autant plus difficiles les travaux d'évaluation ainsi que l'interopérabilité et la compatibilité des différents systèmes.

Mais, quelle que soit la technique utilisée, la performance d'un système dépend de deux facteurs, l'un humain, l'autre technique.

Toutes les études insistent sur le caractère crucial de la phase de prélèvement des échantillons (« enrôlement ») et il convient de gérer la relation homme/machine qui fait intervenir des éléments psychologiques (acceptabilité et apprentissage du processus) et démographiques, la généralité et la permanence de la donnée biométrique constituant à la fois un gage d'efficacité et de simplicité.

Les systèmes biométriques reposent par ailleurs sur une assise statistique. Il faut donc gérer les « taux d'erreurs », les techniques biométriques n'étant pas exactes à 100 %. Actuellement, parce que les critères et les méthodes d'évaluation n'ont pas été véritablement normalisés, on assiste à une véritable « guerre des taux » qui reflète la concurrence qui s'exerce entre les producteurs. L'unicité de telle ou telle donnée biométrique et donc son caractère plus ou moins discriminant sont encore débattus. En tout état de cause, le seuil de tolérance jugé acceptable dépend de la finalité du système que l'on souhaite implanter : par exemple, pour le contrôle d'accès à une zone hautement sécurisée, le taux de fausses acceptations devra être le plus bas possible, au risque d'augmenter le taux de rejets erronés.

Face à la variété des critères de comparaison et des méthodes d'évaluation, les utilisateurs préfèrent actuellement adopter une démarche empirique et expérimentale. C'est le cas de différents aéroports et, dans le rapport, sont décrites la démarche retenue par Aéroports de Paris pour le contrôle d'accès des personnels aux zones d'accès limité ainsi que celle adoptée par l'administration pénitentiaire pour le contrôle à distance des détenus placés sous surveillance électronique et pour l'accès aux parloirs des détenus.

M. Christian Cabal, député, rapporteur, a souligné que, même si les systèmes biométriques ne constituaient pas une panacée, ils apportaient des garanties bien supérieures aux systèmes actuels d'identification ou d'authentification.

Il a observé que l'utilisation des systèmes biométriques faisait aussi l'objet de prises de position contradictoires, parfois extrêmes, surtout dans les sociétés anglo-saxonnes où tout système d'identification, biométrique ou autre, tel

que les systèmes d'immatriculation ou les cartes d'identité, n'est pas facilement accepté.

Dans le rapport, est dressée une sorte d'état des lieux des opinions exprimées à ce sujet qui, tantôt sont de nature technique, tantôt se placent sur le plan éthique.

Sur ce point, le rapporteur a formulé trois observations.

D'une part, que l'on se place sur le plan de la sécurité, ou sur celui des libertés, la valeur des systèmes biométriques devrait s'apprécier de manière relative, c'est-à-dire par rapport aux autres procédés d'identification ou d'authentification actuellement utilisés. Or, force est de constater que cette évaluation fait défaut. La fraude informatique et la fraude documentaire existent car les systèmes actuels, qui reposent sur ce que l'on sait (code, mot de passe) ou ce que l'on a (carte) restent vulnérables et les systèmes biométriques apportent un niveau de sécurité supplémentaire. Ils peuvent donc constituer un instrument efficace de protection des données personnelles et un moyen de se prémunir contre l'usurpation d'identité qui peut être très préjudiciable aux individus.

D'autre part, la plupart des arguments avancés par les détracteurs des systèmes biométriques ont été pris en compte par les producteurs :

- du côté de la sécurité, des travaux ont été engagés pour lutter contre les risques de falsification (plusieurs produits permettent de détecter le caractère « vivant » ou artificiel de l'élément corporel présenté) ; la biométrie « multimodale » qui associe plusieurs données biométriques ou une donnée biométrique et un code ou un mot de passe fait l'objet de diverses études ou réalisations ; des standards de sécurité garantissant l'intégrité et l'inviolabilité des données traitées sont recherchés pour aboutir à une certification,

- du côté des libertés, il convient tout d'abord de noter que l'implantation des systèmes biométriques doit obéir aux règles définies en matière de protection des données et aux Etats-Unis, où cette législation fait défaut, l'International Biometric Industry Association (IBIA) a elle-même défini des principes visant à préserver la vie privée. En outre, il existe une variété de systèmes de stockage ; une base de données n'est pas nécessairement constituée et la donnée peut être conservée sur un support portable comme une carte. Enfin, la cryptographie à clé biométrique peut, semble-t-il, constituer une solution intéressante, mais les avis semblent néanmoins partagés sur ce point.

La troisième observation a porté sur les domaines opérationnels d'application des techniques biométriques. En fait, les craintes exprimées reposent

largement sur la connotation policière de ces techniques. Dans le rapport, sont recensés les différents domaines d'application. S'il est vrai que l'identification judiciaire constitue historiquement le domaine privilégié de l'utilisation généralisée des données biométriques (fichiers d'empreintes digitales, d'ADN, de photographies, reconnaissance vocale), le domaine « civil » ne doit pas être pour autant sous-estimé et il connaît depuis plusieurs années un développement réel, qu'il s'agisse de la gestion des titres (titres d'identité, permis de conduire, cartes de sécurité sociale, titres de réfugiés ou de séjour pour les étrangers, cartes électorales…) – et, à cet égard, les réflexions en cours sur « le titre fondateur » en France montrent que cette dimension est importante – ou qu'il s'agisse de la gestion des accès physique ou logique, voire des horaires de travail ou des usages strictement domestiques.

La deuxième partie du rapport traite des conditions dans lesquelles il paraît possible d'assurer un développement maîtrisé des techniques biométriques.

Sur le plan interne, le cadre juridique actuel apporte des garanties suffisantes, mais demeurent toutefois certaines incertitudes.

La loi « Informatique et libertés » de 1978 actuellement en vigueur et le code de procédure pénale, notamment depuis l'intervention de la loi du 18 mars 2003 pour la sécurité intérieure, encadrent les dispositifs utilisés à des fins de sécurité publique, même si la coexistence de deux corps de règles distincts nuit à leur clarté et probablement à leur mise en œuvre.

Pour les autres dispositifs, la directive européenne de 1995 apporte aussi des garanties suffisantes, comme la loi de 1978, un consensus existant sur le fait d'assimiler une donnée biométrique à une donnée personnelle. La seule réserve, liée à la technique, concerne le droit d'accès et de rectification, puisque d'une part, cette donnée ne sera pas forcément communicable « sous une forme intelligible » ou « en langage clair » et que, d'autre part, le droit des personnes de prendre connaissance de la logique qui sous-tend leur identification automatique sur la base de ses données biométriques n'est pas expressément prévu.

Néanmoins, le cadre juridique actuel comporte un certain nombre d'incertitudes qu'il conviendrait de lever.

D'une part, il s'agit des conditions dans lesquelles, dans le cadre d'une procédure judiciaire, les autorités policières ou judicaires pourraient avoir accès à des données biométriques collectées à d'autres fins que celles directement liées à la sécurité publique et à la sûreté de l'Etat.

L'autre incertitude, qui résulte en grande partie de la précédente, porte sur l'opportunité éventuelle d'un régime spécifique applicable aux systèmes biométriques mis en place pour répondre à des finalités qui ne seraient pas directement liées à la sécurité publique.

Le projet de loi en cours de discussion modifiant la loi de 1978 et transposant la directive de 1995 soumet à un régime d'autorisation de tels systèmes - disposition semble-t-il introduite dans le projet initial à la demande de la CNIL -, mais ne précise pas les critères pris en compte.

La « doctrine » de la CNIL, se fondant sur le principe de proportionnalité tel qu'elle l'interprète, repose notamment sur la notion de « trace » et réserve aux systèmes répondant à un impératif particulier de sécurité les fichiers d'empreintes de même nature que celles enregistrées dans les fichiers automatisés actuels de police, à savoir essentiellement les empreintes digitales.

M. Christian Cabal, député, rapporteur, a souligné que l'audition publique avait montré que cette interprétation était contestable sur les plans technique (d'autres données laissent des « traces », la voix et le visage par exemple) et politique, dans la mesure où il s'agit de questions liées à la souveraineté qui relèvent de la compétence du Parlement, mais aussi sur les plans économique et administratif. Il s'est demandé si les utilisateurs potentiels publics ou privés ne seront pas incités à choisir une technique biométrique moins performante ou moins bien adaptée à leurs besoins réels, s'ils ne seront pas finalement encouragés à renoncer à implanter un système biométrique et si la CNIL elle-même disposait des moyens nécessaires pour examiner dans des délais raisonnables la multitude de demandes qui émaneront tant du secteur public que du secteur privé.

La troisième incertitude concerne les conditions dans lesquelles des transferts transfrontaliers de données biométriques pourraient intervenir, mais il ne s'agit pas d'incertitudes propres aux données biométriques, comme le montre l'actualité récente concernant le transferts de données sur les passagers des vols vers les Etats-Unis.

Enfin, **M. Christian Cabal, député, rapporteur,** a indiqué qu'il avait abordé dans son rapport la question des conséquences juridiques d'une utilisation des techniques biométriques, même si la « preuve biométrique » n'a pas, en principe, vocation à se substituer aux autres moyens de preuve et fait part de son sentiment, corroboré par les évolutions que l'on constate aux Etats-Unis - même si leur système juridique est différent du système français - que le recours à de telles techniques aboutira à une multiplication d'expertises et de contre-expertises techniques, surtout si aucune norme n'est communément admise.

Or, compte tenu des évolutions perceptibles à l'échelle européenne et internationale, **M. Christian Cabal, député, rapporteur,** a jugé urgent de définir un cadre juridique adapté. Des décisions importantes sont en préparation ou viennent d'être prises.

Ces décisions concernent essentiellement le contrôle biométrique de la circulation transfrontalière des personnes, qui vise à remédier à la fraude des documents de voyage et des titres de séjour.

Les Etats-Unis, depuis plusieurs années, envisagent d'utiliser la biométrie pour renforcer la sécurité de leurs frontières. Depuis les attentats du 11 septembre 2001, des dispositions législatives ont été prises, prévoyant, avant octobre 2004, l'introduction de données biométriques sur les passeports et les visas.

Les administrations américaines se préparent activement, notamment dans le cadre de la nouvelle structure dont le gouvernement s'est doté, le Department of Homeland Security (DHS). Cette politique très volontariste du gouvernement américain dont les composantes sont détaillées dans le rapport repose sur une mobilisation très forte des administrations fédérales et un engagement financier important pour la recherche et l'évaluation, même si cette politique ne fait pas l'unanimité, comme en témoignent notamment les réserves émises par le General Accounting Office (GAO) et l'American Civil Liberties Union. En janvier 2003, le NIST, le Département de la Justice et le Département d'Etat ont remis un rapport conjoint qui préconise l'empreinte digitale et la photographie.

L'OACI vient également de rendre ses premières conclusions. Un groupe de travail a été constitué dès 1999 pour étudier les conditions dans lesquelles peuvent être introduites des données biométriques dans les documents de voyage lisibles par machine. Le dispositif retenu en mai dernier propose la généralisation de la photographie numérisée et laisse la possibilité pour les Etats d'opter entre l'iris et l'empreinte digitale.

Du côté de l'Europe, des réflexions sont également en cours. EURODAC, le système de gestion reposant sur l'empreinte digitale des documents délivrés aux demandeurs d'asile, a constitué la première réalisation ; il est entré en vigueur en janvier dernier. Le système commun d'échange des données relatives aux visas devrait lui aussi comporter des données biométriques et le 27 février dernier, une déclaration commune franco-allemande sur l'utilisation de la biométrie pour les passeports, les visas et les titres de séjour a été présentée. Il n'est pas non plus exclu que d'autres dispositifs, tels que le Système d'information Schengen (SIS), voire EUROPOL, recourent à terme à la biométrie.

M. Christian Cabal, député, rapporteur, a insisté sur les enjeux économiques de ces initiatives qui sont considérables, tant pour les Etats qui devront supporter des dépenses importantes pour sécuriser les titres qu'ils délivrent (le Visa information System européen concernera, hors élargissement, quelque 10 millions de visas par an et, pour les Etats-Unis, le chiffre de 7 millions par an a été avancé) que pour les producteurs de systèmes.

S'il est difficile d'obtenir des chiffres précis et incontestables sur le marché de la biométrie, il est évident que les mesures en préparation vont assurer une croissance, qui était d'ailleurs annoncée depuis plusieurs années.

M. Christian Cabal, député, rapporteur, a noté qu'à cet égard la standardisation constituait un enjeu essentiel, tant politique qu'économique, et que des efforts importants étaient déployés dans ce domaine, pour définir des normes de sécurité sur la base des « critères communs » de sécurité des technologies de l'information, des normes d'interface et d'intégration et des normes de compatibilité.

C'est ainsi qu'en 2002 les Chefs d'Etat présents au sommet du G8 se sont entendus pour formuler des recommandations sur les normes minimales dans le domaine de la biométrie et que le 5 mai 2003, lors de la réunion des ministres de l'intérieur et de la justice du G8, l'intérêt de disposer de tests probants a été affirmé.

Dans ce domaine, le NIST américain mène une politique très active, tant au plan national qu'international, sous l'impulsion du gouvernement américain. Les acteurs publics et privés, américains et d'autres nationalités, y collaborent au sein du Biometric Consortium. Une cohérence des normes nationales et internationales est structurellement assurée. Des liens sont établis entre, d'une part, le secteur de la biométrie et, d'autre part, les secteurs de la sécurité informatique et des cartes.

M. Christian Cabal, député, rapporteur, a rappelé que, sur le marché de la biométrie, la France n'était pas absente et qu'elle disposait de nombreux atouts, tels que le groupe SAGEM, leader mondial de l'empreinte digitale ou encore la société THALES qui intègre des systèmes biométriques, ces sociétés ayant d'ores et déjà remporté d'importants marchés, même si la concurrence reste très forte.

Surtout, à la différence des Etats-Unis, la France n'a pas encore élaboré une politique industrielle de la sécurité et les réflexions menées par les administrations, les experts et les producteurs français restent extrêmement dispersées et généralement sectorisées. Le suivi de ces réflexions ne semble pas non plus correctement assuré, la France n'étant pas toujours représentée dans les groupes techniques.

M. Christian Cabal, député, rapporteur, a observé que l'audition publique qu'il avait organisée avait mis ainsi en évidence la nécessité d'instituer un lieu d'échanges entre tous les acteurs, en assurant l'information du public sur les débats en cours.

Quatre recommandations ont ensuite été présentées :

- la première propose de définir dans un cadre législatif précis et transparent les conditions dans lesquelles des autorités publiques peuvent être, le cas échéant, habilitées à accéder à des traitements comportant des données biométriques ;

- la deuxième vise à garantir l'information préalable du Parlement sur les travaux conduits aux niveaux européen et international relatifs à l'introduction ou au transfert de données biométriques ;

- la troisième suggère la constitution d'un observatoire associant les différents acteurs concernés et les utilisateurs et chargé d'assurer une veille juridique et technique et l'information du public ;

- la quatrième envisage la mise en place d'un organisme associant des partenaires publics et privés et doté des moyens de financement nécessaires pour faire réaliser par des laboratoires indépendants des travaux d'évaluation scientifiques et techniques, recueillir l'avis d'experts ou d'universitaires sur la fiabilité des travaux menés par d'autres organismes et diffuser les résultats des études conduites en son sein.

M. Claude BIRRAUX, **député, président de l'Office,** après avoir remercié le rapporteur pour sa contribution à la réflexion portant sur les données biométriques, l'a interrogé sur les risques de surveillance des individus à leur insu, sur les conditions dans lesquelles l'interopérabilité des systèmes pouvait accroître les risques de telles dérives et sur la pertinence d'une législation nationale dans un domaine où une réglementation européenne, voire des instruments internationaux, semblent nécessaires.

M. Christian Cabal, député, rapporteur, a répondu que le « traçage » des individus reposait sur des systèmes n'utilisant pas nécessairement des données biométriques, comme en témoignent les exemples relatifs aux téléphones portables ou aux cartes bancaires ; cela pose la question plus générale de la conservation des données et des moyens techniques permettant une « traçabilité » de celles-ci. S'agissant du croisement des fichiers éventuellement constitués, sur le plan juridique, les conditions d'interconnexion ou d'accès doivent être correctement définies. En tout état de cause, la donnée biométrique n'est pas plus « liberticide » que d'autres données reposant sur un code, un numéro ou toute autre clé ; en revanche, elle constitue le meilleur moyen, à l'heure actuelle, pour empêcher l'usurpation d'identité qui peut nuire gravement à l'individu et repose sur une démarche volontaire à travers la procédure d'enrôlement. L'interopérabilité doit être recherchée, en particulier dans le domaine de la circulation transfrontalière des personnes, compte tenu de la diversité des choix qui seront arrêtés par les différents pays et si l'on ne veut pas

que des monopoles se constituent, limitant la liberté des Etats. L'existence d'une législation nationale garde tout son intérêt, parce que les domaines d'application de la biométrie sont extrêmement diversifiés et que, même dans le domaine des documents de voyage, les compétences nationales subsistent, notamment pour les passeports.

M. Henri Revol, sénateur, après avoir noté que le marché de la biométrie allait se développer et que les industriels français y étaient bien implantés, a demandé au rapporteur s'il en était de même des instituts de recherche nationaux et des experts français.

M. Christian Cabal, député, rapporteur, a indiqué que dans le domaine de la biométrie, dans son acception scientifique, la recherche française tenait son rang, mais que dans le secteur des systèmes biométriques d'identification, les études étaient fragmentées et généralement temporaires. Surtout, les chercheurs ont peu de contacts avec les industriels et les financements sont parfois problématiques, ce à quoi une recommandation tente de remédier.

A une question posée par **M. Christian Kert, député,** sur les applications de la biométrie dans le domaine hospitalier, **M. Christian Cabal, député, rapporteur,** a répondu qu'aux Etats-Unis la biométrie était d'ores et déjà utilisée pour les contrôles d'accès, mais aussi pour les cartes d'assuré social ; l'usurpation d'identité peut représenter un coût pour la collectivité, ce qui devrait conduire à envisager son introduction dans les cartes « SESAM-vitale ».

M. Jean-Yves Le Déaut, député, a proposé l'utilisation de l'indicatif et non du conditionnel dans les recommandations, proposition qui a été retenue par les membres de l'Office, et demandé au rapporteur si ses interlocuteurs avaient été coopératifs.

M. Christian Cabal, député, rapporteur, a indiqué que l'information n'avait pas été instantanément délivrée et que des demandes réitérées avaient été dans certains cas nécessaires, cette réticence initiale pouvant s'expliquer par le fait que les choix n'avaient pas été définitivement arrêtés, mais aussi par la volonté de réserver à un « cercle d'initiés » le processus de décision ; progressivement néanmoins une meilleure collaboration s'est instaurée, dès lors que les personnes entendues ont pris conscience que le travail parlementaire pouvait constituer aussi une source d'informations qui ne leur était pas directement accessible.

A deux interrogations formulées par **M. Jean-Louis Lorrain, sénateur,** sur la discrimination biométrique des jumeaux et le système de contrôle d'accès mis en place par le CEA, **M. Christian Cabal, député, rapporteur,** a répondu qu'il avait été démontré que de vrais jumeaux ne possédaient pas la même empreinte digitale, ni le même iris et que dans les zones de haute sécurité, en particulier les sites nucléaires, l'empreinte digitale était généralement choisie.

Après que **M. Claude BIRRAUX, député, président de l'Office,** eut souligné la nécessité d'assurer un suivi du développement de la biométrie, l'Office **a adopté le rapport à l'unanimité des membres présents** et autorisé sa publication.

ANNEXES

Annexe 1

Liste des personnes auditionnées

MISSIONS À L'ÉTRANGER

Le Rapporteur tient à remercier tout particulièrement Messieurs les Ambassadeurs de France aux Etats-Unis, au Japon ainsi que le Représentant permanent de la France auprès de l'Union européenne, pour le concours efficace qu'ils ont, ainsi que leurs collaborateurs, apporté à l'organisation de ces missions.

Japon

Parlementaires

M. Shinya ONO	Député du PLD
M. Yutaka TAKEYAMA	Sénateur, Président du Comité Spatial du PLD
M. Kisburo TOKAI	Vice ministre du MEXT
M. Yukio HATOYAMA	ex-Président du Parti Social Démocrate
M. Tetsuo SAITO	Parti Komei
M. Jin MURAI	Ex-Ministre chargé de la prévention des sinistres et ex-Président de la Commission Nationale de la Sécurité Publique, Député au PLD

Japan Biometric Authentification Association

M. Yoshiki ASHIKAYA	Directeur du Sous-comité de marketing
M. Takeshi HAJIKA	Directeur du Sous comité de Service/Business
M. Masumi SHIROI	Directeur adjoint du Sous-comité de Service/Business
M. Masanori AKASHI	Secrétariat

Sony

Bionics Device Promotion Department, Network Media Business Developement Division, Recordins Media Company

M. Yoshio KUBO	Senior General Manager
M. Takeshi FUNAHASHI	Senior Manager
M. Kazuhiko AKIYAMA	Senior Manager

Omron Corporation

M. Hirofumi MIYATA	Marketing Manager, Social Systems Solutions Business Company, Business Incubation Department, New Business Development Center
M. Makoto ARAI	Assistant Manager SE

National Institute of Informatics (NII)

Professeur Shinichi SATO	
Professeur Masao SAKAUCHI	Directeur general adjoint

Gaimusho *(Ministère des affaires étrangères), Division de passeport*

M. Toyoei SHIGEEDA,	Directeur
M. Hidehiro YOSHII	Assistant Directeur
M. Hiroshi GOKAN	Assistant Directeur
M. Nobuyuki KOYAMA	Assistant Directeur
M. Kozo KOJIMA	Official
M. Susumu KITAMURA	Official
Mme Seiko KIYOHARA	Official
M. Jun ONO	Official

OKI Electric Industry

M. Takeshi HAJIKA	Senior Manager
M. Kazuaki EBARA	Manager
M. Toshio NAKAMURA	Assistant Manager

Ministry of Land, Infrastructue and Transport (MLIT)

M. Takanori SUZUKI	Deputy Director, Information Planning Division
M. Asao TOBA	Special Assistant to Director, Information Planning Div.

NEC Corporation

M. Masahiro UCHIBORI	Assistant General Manager, 2nd Government Solutions Division
M. Hiroshi NAGANUMA	Executive Manager
M. Kenji KIKUCHI	Senior Manager

Université de Waseda
Laboratoire du Professeur KOMATSU

Etats-Unis

International Biometry Industry Association (IBIA) :

M. Richard E. NORTON	Executive Director
Mme Rebecca DORNBUSCH	Deputy director

Federal Bureau of Investigation (FBI)

M. John BEHUN	Chief FSSU
Mme Erin B. ROGERS	Liaison Analyst

General Services Administration (GSA) – Federal techgnology Service

M. Mickey FEMINO	Director – Center for Innovative Business Solutions – IT Solutions
Michael R. BROOKS	Director – Center of Smart Card Solutions – IT Solutions
M. William "Bill" WINDSOR	Program Specialist – Innovative Business Solutions – IT Solutions

Immigration and Naturalization Service (INS) :

M. Robert A. MOCNY	Director – Entry Exit Program
M. Sergio R. MESA	Assistant Chief Inspector – Office of Inspections

Transportation Security Administration (TSA)

M. James E. SOLARSKI	Special Agent
M. Richard T. LAZARICK	Aviation Security Research and Development – Access Control and Analysis Tools Technology

Department of Commerce – National Institute of Standards and Technology (NIST) :

M. Fernando PODIO	Co-Chair Biometric Consortium
M. Charles L. WILSON	Manager, Image Group – Information Access Division
M. Michael D. HOGAN	Standards Liaison – Information Technology Laboratory
M. Jeffrey S. DUNN	Co-Président du Biometric Consortium

American Civil Liberties Union (ACLU) :

Mme Katie CORRIGAN	Legislative Counsel

Bruxelles

M. Philippe CONDUCHE	Conseiller, représentation permanente de la France auprès de l'Union européenne
M. Yann De CEUSTER	Chef de l'unité « Politique des visas, frontières extérieures, Schengen » de la Direction générale Justice et Affaires intérieures de la Commission européenne

FRANCE

Ministère de l'Intérieur

M. Daniel CANEPA	Directeur adjoint du cabinet
M Bernard DELIAS	Chargé de mission auprès du Directeur central de la Police aux frontières
M. Patrick DALLENNES	Chef du Bureau de la circulation transfrontière et des visas à la direction des libertés publiques et des affaires juridiques, Responsable du groupe de travail biométrie pour cette direction
M. DARCY	Chef du projet biométrie
Visite du Laboratoire de Police scientifique de Lyon, sous la direction de	
M. Christian JALBY	Contrôleur général de la Police nationale

Gendarmerie nationale

Capitaine Marc SOULAS	Chef du département Signal Image de l'Institut de Recherche Criminelle de la Gendarmerie nationale
Chef d'escadron Jérôme SERVETTAZ	Adjoint au Chef de la DCRA, IRCGN
Adjudant François DRILLET	Responsable du groupe traces pour le fichier automatisé des empreintes digitales, Service technique de recherches judiciaires et de documentation
Chef d'escadron Jean-Michel CEDE	Chef de la section des études transversales et prospectives du Bureau de la police judiciaire de la Direction générale de la gendarmerie nationale

Ministère de la Justice

Direction de l'Administration pénitentiaire :	
M. Xavier RONSIN	Chef de service, Adjoint au Directeur de l'administration pénitentiaire
M. Bruno HAURON	Responsable de la cellule Sécurité
Visite de la prison de la Santé	

Aéroports de Paris	
M. Bruno LAVEISSIERE	Chef du service Etudes de projets opérationnels de la Direction de l'exploitation
Sagem	
M. Jean-Paul JAINSKY	Directeur de la Division Sécurité
M. Bernard DIDIER	Directeur Technique et du Développement des Affaires
M. Hervé JAROSZ	Chef de produit Biométrie
M. Samuel HAILU-CROSS	Responsable Marketing
M. Enrique DELGADO	Ingénieur Systèmes
Thalès	
M. Philippe KARNAUCH	Président Directeur Général
M. Etienne PAHIN	Directeur Commercial
M. Marc FABREGUETTES	Products et marketing Manager
M. Emmanuel-Alain CABANIS	Professeur des Universités, Chef du Service de Neuro- Imagerie du Centre hospitalier national d'Ophtalmologie des Quinze-Vingts, Président de la Compagnie des Experts médecins près les cours d'appel de la région parisienne, Président de la Société de Biométrie Humaine
Mme Yvette DELOISON	Docteur d'Etat ès Sciences, Chargé de recherche au CNRS, Expert judiciaire près la Cour d'appel de Paris, Secrétaire Générale de la Société de Biométrie Humaine
M. Franck LEPREVOST	Professeur à l'Université Joseph Fourier de Grenoble
Mme Bernadette DORIZZI	Professeur, Chef du Département Electronique et Physique de l'Institut national des télécommunications
M. Philippe LEMOINE	Membre de la Commission nationale Informatique et Libertés

M. Christophe PALLEZ M.Yann LE HEGARAT	Secrétaire général de la CNIL, Expert informaticien à la CNIL
M. Alain PUTZ	Vice-Président du Tribunal de Grande Instance de Paris
Mme Monique HEROLD	Responsable du groupe de travail sur la bioéthique à la Ligue des droits de l'homme

Annexe 2

Compte rendu de l'audition publique du 15 mai 2003

OFFICE PARLEMENTAIRE D'EVALUATION DES CHOIX SCIENTIFIQUES ET TECHNOLOGIQUES

LES METHODES SCIENTIFIQUES D'IDENTIFICATION DES PERSONNES A PARTIR DE DONNEES BIOMETRIQUES

JEUDI 15 MAI 2003

SOMMAIRE

OFFICE PARLEMENTAIRE D'EVALUATION DES CHOIX SCIENTIFIQUES ET TECHNOLOGIQUES

Les méthodes scientifiques d'évaluation des personnes à partir de données biométriques

JEUDI 15 MAI 2003

La séance est ouverte à 9h10 sous la présidence de Monsieur CABAL, député de la Loire, Rapporteur.

M. LE PRESIDENT, Pr Christian Cabal, rapporteur OPECST - Comme je vous l'avais déjà indiqué, l'Office parlementaire m'a confié la charge, sur proposition du Bureau de l'Assemblée nationale, d'effectuer une étude portant sur les méthodes d'identification des personnes à partir des données biométriques. Cette étude a été demandée il y a de cela presque un an, à l'issue d'une autre étude que j'avais réalisée.

Du fait de la tenue des élections, c'est seulement à la rentrée parlementaire que l'Office a engagé cette étude. Le calendrier est très précis puisque le rapport doit être déposé le 10 juin, donc à une échéance maintenant assez rapprochée.

Ce n'est pas tout à fait un hasard mais une nécessité car ce travail s'inscrit dans une actualité presque brûlante. Au plan international et au plan national la mise en œuvre des techniques d'identification biométriques s'inscrit dans une réalisation proche, ou prochaine, compte tenu d'un certain nombre d'impératifs qui, ces derniers mois ou années, se sont imposés auprès des autorités publiques.

Par ailleurs, dans un autre domaine de la biométrie, c'est-à-dire l'accès aux systèmes informatiques, le marché s'est rendu compte de la nécessité ou de la possibilité d'utiliser les techniques biométriques pour contrôler les accès aux systèmes informatiques. La perspective d'utilisations quotidiennes est venue encore enrichir ces derniers mois le panel d'utilisation de la biométrie.

Nous sommes donc en plein dans l'actualité ; les plus hautes autorités des grands pays de la planète, notamment du G8, sont actuellement en train d'étudier un certain nombre de propositions et d'expertises afin de mettre en œuvre, dans des domaines très particuliers, ces nouvelles mesures.

Un certain nombre d'entre vous ont déjà été auditionnés par l'Office individuellement ou par nature d'activité. Notre procédure comporte régulièrement, au terme des auditions individuelles de personnalités qui se sont déroulées depuis le mois de septembre, une procédure d'audition publique - au sens qu'elle est ouverte au public - qui regroupe les différentes personnalités, experts ou industriels ou utilisateurs des techniques que nous évaluons.

C'est la procédure que nous mettons en œuvre ce matin, l'intérêt n'étant pas uniquement d'écouter de nouveau un certain nombre d'entre vous effectuant une mise à jour des informations qu'ils nous ont antérieurement communiquées mais d'échanger, sinon confronter le cas échéant, un certain nombre de recommandations et de répondre aussi à quelques interrogations que nous avons élaborées à l'issue des différentes auditions précédentes.

Comme nous avons pris un peu de retard, je ne reviendrai pas sur l'historique de la biométrie et les problématiques qu'elle soulève. Je poserai ensuite un certain nombre de questions et nous échangerons. Je vais donner la parole au Professeur CABANIS qui va faire un exposé introductif.

Pr Emmanuel-Alain CABANIS, Président de la société française de biométrie humaine - Monsieur le Président, Monsieur le Député, mon cher collègue,

Merci de me faire l'immense honneur de m'asseoir à votre gauche, j'y vois là un signe d'alliance de cette activité qui nous est commune, la médecine ; la médecine qui a cet objectif majeur de faire en sorte que chacun d'entre nous de l'espèce homo homo soit en bonne santé ou, lorsqu'il ne l'est plus, redevienne dans cet état de santé, c'est-à-dire de paix et d'équilibre.

La médecine a expliqué que de son milieu ont pu émerger des hommes et des femmes depuis deux siècles préoccupés par la forme humaine.

Pourquoi est-on homme ? Comment reconnaît-on l'homme ?

Charles DARWIN a essayé, dans les îles Galápagos, de voir ce qui distinguait l'homme de l'oiseau, le chat du poisson. Est née cette extraordinaire publication sur l'origine des espèces en 1859 qui l'amenait à essayer de comprendre ce qu'il y avait de commun entre les formes animales, c'est-à-dire un objet animé par une âme (anima) qui faisait en sorte qu'on était mammifère, et animé par la pensée, c'est-à-dire que nous devenions homo homo dans ce qui s'appelle l'hominisation. La forme humaine est différente de celle des animaux parce que l'homme est debout.

Premier événement dans l'alignement des espèces, il est debout sur ses pieds, il a libéré ses mains de la locomotion et son cerveau s'ouvre vers l'avant : par le lobe frontal, il a la mémoire et l'imagination ; en même temps, par le lobe temporal, il entendra et aura des humeurs comportementales.

Bref, les racines de ce savoir qui va devenir l'anthropologie (*anthrôpos*, homme, et *logos*, savoir) naissent au 19ème siècle. C'est une volonté de rigueur qui va essayer d'animer un certain nombre de scientifiques parmi lesquels le premier s'appelle Paul BROCA. Cet homme, plus rigoureux que les autres, va utiliser un double-décimètre et des compas pour essayer d'amener une classification à l'intérieur de cette espèce extraordinaire homo sapiens sapiens devenue homo homo.

Paul BROCA va fonder une école qui s'appellera « Ecole d'anthropologie » sise rue de l'Ecole de médecine qui réunira autour d'elle beaucoup de gens de cette même époque qui se qualifieront d'anthropologues, c'est-à-dire

essayant de mesurer la longueur du membre supérieur puis du membre inférieur, rapportant l'un à l'autre, et faisant des découvertes intéressantes aux plans statistique et mathématique.

Par exemple, un certain CUVIER nous rappellera que notre forme d'homme, d'hominidé, est définie par des rapports et non pas par des mesures. Nous ne sommes pas un ensemble de mesures objectives, nous sommes une suite de rapports. *Tous pareils, tous différents*, tel était d'ailleurs le titre de l'exposition au Musée de l'Homme il y a trois ans.

Cet événement nous rappelle le résultat de cette anthropologie, de ce savoir accumulé au fil des années, savoir croisé par le savoir des statistiques et le savoir des mathématiques, et même si certains ont dit que les statistiques sont à la médecine ce que le piano mécanique est à la musique, il n'empêche que ces règles majeures sont définies, des ratios de longueur, des ratios de surface définissent cette forme individuelle qui fait de nous une espèce parmi celle des mammifères dans l'embranchement des vertébrés homo homo. Notre forme est définie.

Dans ce même 19ème siècle explosent des données de volonté scientifique poussée notamment dans les domaines de la police, de la reconnaissance de l'individu. Nous voyons apparaître en 1835 la photographie, la définition même de ce qui va se passer au quai des Orfèvres, dans ce qui va devenir l'identité judiciaire, grâce à ces hommes qui vont distinguer les uns des autres, les bons des mauvais, premier tri d'espèce sociétal.

Ce tri va nous rappeler une chose essentielle qui est que, dans l'espèce humaine, la race n'existe pas puisque nous sommes dans une particularité génomique. Nous sommes entre nous des gens qui ne peuvent pas être définis en catégorie par la couleur de leur peau, la forme de leurs cheveux ou la longueur de leurs membres. C'est la vieille lune du 19ème siècle, cette anthropologie physique a disparu.

Notre véritable identité est celle du génome, nous le savons tous désormais, et ce morphotype n'a pas grand-chose à faire avec le génotype.

En tout cas, en m'entretenant avec certains à l'entrée de cette pièce, je reconnaissais comme chaque citoyen de ce pays que trois objets anatomiques de la forme humaine émergeaient : le dermatoglyphe, l'iris et la photographie. Tous les trois ont en commun au plan anatomique une chose, c'est ce que nous qualifions d'anatomie de surface, elle est directement accessible.

La forme du visage d'autrui est la chose la plus difficile à numériser. Reconnaître un visage parmi les mille voyageurs qui descendent d'un train est la chose la plus difficile à mathématiser. Comment notre cerveau individualise-t-il instantanément (environ sept à dix millisecondes) notre frère, notre cousin ou l'ami ?

C'est une supériorité de l'outil biologique cérébral définitive. La machine ne le fait pas encore, mais on tente et on avance.

Ces anatomies de surface ont en commun de profiter d'un outil majeur (l'informatique), d'avoir une certitude, un archivage et une comptabilisation plus précise qu'elle ne l'a jamais été, mais des questions me taraudent.

L'anatomie de surface est une bonne chose mais il y a d'autres anatomies : l'anatomie de la croissance, un enfant n'est pas un vieillard et cette anatomie est une anatomie plastique. Contrairement à ce qu'on croyait au 19ème siècle, nous savons que même les cellules cérébrales se remodèlent pendant toute l'année et toute la vie. Nous savons que nous sommes aussi plastiques que l'amibe sur une surface plane ou rugueuse. Nous sommes plastiques avec le temps, nous ne sommes pas les mêmes.

Par ailleurs, nous varions aussi avec la fonction. Si nous passons notre vie à préparer des jeux olympiques, nous n'avons pas le même morphotype que votre très humble serviteur vieux, gros, avachi, obèse, forme absolument pas démonstrative de ce qu'est l'athlète dans notre stade de l'Olympe !

En troisième lieu, cette anatomie est également viscérale, une anatomie quantitative de la forme cachée.

Nous sommes une enveloppe corporelle, on reconnaît le visage, la peau à travers le dermatoglyphe, les poils (il existe une biométrie du poil, des cheveux).

Mon activité quotidienne est celle de la neuro-imagerie, c'est-à-dire d'observer des cerveaux en coupe avec un scanner à rayons X numérique ô combien, une imagerie par résonance magnétique numérique ô combien ! Ma visée est d'accumuler des fichiers de la reconnaissance individuelle de la forme humaine de ce qui est caché : l'intérieur de la tête, le cerveau. Nous allons chercher l'hippocampe qui est le lieu où se localise la mémoire, nous essayons de comprendre pourquoi ce monsieur qui a des petits signes d'Alzheimer a un hippocampe réduit en volume.

Nous croyons profondément que nous sommes à l'aube d'une connaissance qui réjouit l'humble scientifique, par définition humble, société d'anthropologie devenue société de biométrie humaine au début du siècle ; l'humble médecin aussi. Nous sommes au service de l'homme et nous ne sommes qu'au début de quelque chose qui me semble important, non pas comme le disent les gens, du flicage, mais qui est au contraire l'avenir de l'homme, car on met en lumière ce caractère extraordinaire d'homo sapiens : il est un, unique et indivisible.

Pour nous, cela s'appelle le croisement de fichiers, l'incertitude (même en croisant quatre fichiers, nous ne sommes jamais certains d'avoir raison à 100 %, pour nous le 100 % n'existe pas). Il existe une marge d'erreur parce que tout ce qui appartient à la vie a une part d'aléatoire qui ne sera jamais futur de l'indicatif, c'est la seule certitude que l'on peut avoir dans le respect de l'individu lui-même et de son génome spécifique, la liberté de chacun d'entre nous.

Merci Monsieur le Président.

M. LE PRESIDENT – C'est moi qui vous remercie, cher confrère, parce que cet exposé a d'emblée cadré la problématique de notre question avec la connaissance scientifique indispensable et l'humour qui vous caractérise et qui permet d'aborder des sujets sérieux avec la distanciation nécessaire, mais avec toute sa profondeur également.

Cela dit, l'athlète de l'Olympe ou la personne mûre bedonnante sont amenés à franchir différentes étapes dans leur vie sociale et dans notre société moderne en passant les frontières, en montant dans un moyen de transport ou au travers de différents événements. A ce titre, leur identification est une nécessité et s'impose à nos sociétés contemporaines ou même peut-être du passé sous d'autres formes.

A cet égard, l'utilisation de la biométrie apparaît comme un élément utile voire indispensable aux autorités publiques de l'Etat ou des Etats dans la nécessité qui est la leur, conformément aux lois qui régissent nos sociétés, de savoir si tel individu est bien celui qu'il prétend être et s'il est habilité à entreprendre un certain nombre d'actions correspondant à notre vie sociale en général.

A cet égard, il est particulièrement utile de pouvoir nous informer et nous interroger sur les méthodes et moyens biométriques qu'entend utiliser le département de l'Intérieur en charge d'un certain nombre de responsabilités, ô combien variées, au plan intérieur du territoire et au plan des relations internationales, dans le présent et surtout dans le futur et sur la doctrine qui s'élabore à ce titre.

Avec cette perspective, nous avons aujourd'hui, autour de cette table, Monsieur Bernard SCHMELTZ, chef du service de la circulation transfrontière au Ministère de l'Intérieur, Monsieur David MARTINON, conseiller diplomatique au cabinet du Ministre SARKOZY, et Madame GRANDJEAN, conseiller au cabinet du Ministre.

Je me tourne vers eux, Monsieur MARTINON est plus directement en charge des questions biométriques qui ont été l'objet d'un certain nombre de thèmes de réflexion et d'actions entreprises par son ministère, peut-être pouvez-vous introduire cette question.

M. David MARTINON, Conseiller diplomatique du Ministre de l'Intérieur, de la sécurité intérieure et des libertés locales – Avec votre autorisation, je vous donnerai le contexte politique et le sens de notre démarche.

Nous nous sommes saisi de la question de la biométrie (c'est une question qui traîne depuis un certain temps dans essentiellement deux départements ministériels, le ministère de l'Intérieur et celui des Affaires étrangères) dès que les urgences les plus fortes ont pu être traitées. En réalité, nous avons constaté que pour être en mesure de continuer à traiter les urgences plus efficacement et avec des solutions plus durables, il était indispensable de changer nos méthodes.

Les urgences que nous avons eu à traiter au tout début étaient en premier lieu Sangatte. Très vite, des questions très concrètes sont apparues pour lesquelles

nous avons constaté que les seules bonnes réponses à long terme que nous pouvions y apporter étaient techniques, notamment par l'utilisation de techniques biométriques.

Sur Sangatte, une difficulté est apparue très rapidement dans nos négociations avec les Britanniques qui ont duré six mois. Dès les premiers jours, nous avons constaté que se posait la question du partage de la population des réfugiés de Sangatte. Immédiatement, les Britanniques nous ont dit être prêts à faire un partage sous un certain nombre de conditions mais que, pour le mettre en œuvre et vérifier que les mouvements secondaires de réfugiés ne se perpétueraient pas, il fallait être capable de les identifier avec certitude et fiabilité.

Comment voulez-vous identifier des gens qui n'ont plus de papiers ou qui ont, éventuellement, des états civils mais que ces états civils se trouvent en Afghanistan ou en Irak, dans la situation que connaissaient ces deux pays, il y a six mois et qu'ils connaissent encore. La difficulté existe pour parler avec modération. C'est la première à laquelle nous avons été confrontés.

Nous nous sommes ressaisi du dossier dès que nous avons pu fermer le centre pour éviter ces problèmes à l'avenir.

Au fur et à mesure sont apparus d'autres problèmes concrets. Quand nous nous sommes attachés à travailler sur les flux d'immigration en provenance d'Afrique, nous nous sommes rendu compte qu'un visa Schengen délivré à Bamako servait à quatre ou cinq personnes qui se renvoyaient le visa par la poste. C'est une sorte de « mutualisation »du visa.

Comment faire à l'arrivée à l'aéroport Charles de Gaulle pour vérifier que le ressortissant d'un Etat tiers qui vous présente son passeport et donc son visa est bien la personne à laquelle a été délivré ce passeport ou ce visa ?

Comment faire dès lors que l'état civil est incertain et que personne n'a intérêt à ce qu'il soit plus rigoureux ? C'est culturel, beaucoup de questions sociologiques sont liées. N'avons-nous pas les moyens de travailler à la source dans les pays africains avec lesquels nous avons de très bonnes relations pour les aider à rebâtir des états civils fiables ? Nous allons le faire mais, à court terme, il n'est pas sûr que ce soit la voie la plus efficace.

Troisième constat concret et simple : aujourd'hui, l'immigration en Europe est de plus en plus régulière d'abord irrégulière ensuite. Un certain nombre de ressortissants d'Etats tiers rentrent dans la zone Schengen en toute légalité soit avec un visa tourisme qui leur a été délivré selon des procédures normales, soit sans visa sur la simple présentation du passeport quand il s'agit de ressortissants d'Etats ayant vocation à adhérer à l'Union européenne à moyen terme.

Je ne choquerai personne en disant que c'est le cas de la Roumanie depuis que la France a convaincu ses partenaires de l'Union européenne de lever l'obligation de visa en décembre 2001. A partir du 1er janvier 2002, nous avons vu un afflux massif de Roumains qui se sont maintenus sur le sol de l'espace Schengen, sans ressources, et qui ont rapidement posé des problèmes à l'ordre public.

Comment faire lorsqu'on interpelle ces ressortissants roumains pour les éloigner, s'il n'y a pas eu un contrôle minimal à leur entrée sur le territoire Schengen pour qu'au moins court le délai des trois mois autorisé par le règlement communautaire ?

La seule solution est de pouvoir se mettre en situation, à toutes les frontières terrestres et aéroportuaires, de contrôler tous ces passeports et de les composter.

Nous avons obtenu cela de nos partenaires européens, mais nous nous sommes rendu compte que nous-mêmes n'étions pas capables de contrôler 100 % des passeports à l'entrée, 100 % des documents de voyage parce que la Police de l'air et des frontières n'a pas les effectifs suffisants et que c'est très difficile en termes d'organisation.

Quelle solution peut-on apporter ?

Vraisemblablement, on peut s'en sortir en automatisant ces contrôles, en prévoyant un système de portiques qui pourraient s'ouvrir sur la zone Schengen, au propre et au figuré, dès lors que le passager pourrait, en déposant son passeport, en posant sa main ou en mettant son visage devant un appareil, prouver qu'il est bien le titulaire du passeport. Ce serait une fiabilité du contrôle et en même temps une systématisation et une automatisation.

Dernier constat dans un autre registre, les auteurs des attentats du 11 septembre les ont préparés en Allemagne, cela ne les a pas empêchés de se rendre aux Etats-Unis. Si nous voulons lutter efficacement contre la menace terroriste, il y a intérêt à renforcer et fiabiliser les contrôles aux frontières.

Pour toutes ces raisons, nous nous sommes rendu compte que nous ne serions efficaces pour traiter ces problèmes qui se posent régulièrement dans l'urgence mais souvent avec une ampleur particulière que si nous étions capables de changer nos méthodes. Pour cela, nous avons constaté que la seule méthode était l'utilisation de la technique biométrique.

Premier constat : il est indispensable que nous avancions sur ce terrain.

Deuxième constat : c'est très difficile.

On ne peut pas s'arrêter à dire cela mais c'est très difficile parce que si on veut fiabiliser les contrôles, cela veut dire des investissements considérables, des techniques fiables, vérifiées, et que l'on s'accorde sur ces techniques. Il est très difficile de demander l'extension des visas Schengen avec les empreintes digitales si d'autres pays n'acceptent que la reconnaissance faciale. Il faut arriver à un choix limité de techniques ou/et à des techniques interopérables.

Une autre difficulté se pose pour « imperméabiliser » le système. Il va de soi que les réseaux de passeurs, les organisateurs de filières d'immigration clandestine et les réseaux terroristes vont beaucoup plus vite que la police de façon générale, et ils savent s'installer là où les contrôles sont plus faibles et passer par les

endroits les plus simples pour taper dans le « ventre mou ». C'est une expression désormais consacrée dans les services de lutte antiterroriste, les terroristes font toujours un choix en termes de coût et d'efficacité ; ils taperont là où c'est le plus simple et où cela demande un investissement le plus réduit.

Il nous faut donc « imperméabiliser » tous les contrôles. Cela signifie se mettre d'accord sur les visas Schengen et sur les passeports. Deux ou trois enceintes sont concernées dont le Comité Schengen pour les visas et l'Organisation de l'aviation civile internationale (OACI) pour les passeports. Cela signifie que plusieurs négociations se superposent, d'où la difficulté de cette démarche et la longueur de ces travaux.

M. Nicolas SARKOZY a proposé à son homologue allemand une démarche communautaire qui s'est concrétisée lors du Conseil Justice affaires Intérieures du 23 février à Bruxelles, l'initiative franco-allemande a consisté à proposer à tous nos partenaires de l'Union d'avancer sur ce thème (ce n'était pas si simple) et d'essayer de mettre en œuvre des tests à grande échelle pour que les ministres soient en situation de décider en connaissance de cause de la meilleure technique.

Pour nous, il existe plusieurs critères : la fiabilité, la simplicité d'emploi, l'existence de bases de données qui permettent des recoupements. Encore une fois, les objectifs ne sont pas les mêmes suivant les pays. Pour nous, c'est un objectif de lutte contre l'immigration clandestine et contre le terrorisme ; aux Etats-Unis, l'objectif numéro un est la lutte contre le terrorisme.

Comme l'a dit le Professeur CABANIS, les techniques biométriques sont ce qui nous permet de vérifier qu'une personne est bien le titulaire du titre de transport qu'elle présente, ce qui est déjà considérable.

Cette initiative franco-allemande a été suivie d'effets puisque la Commission européenne s'est chargée de lancer ces tests à grande échelle. Le commissaire VITORINO, lors de la réunion informelle des ministres de l'Intérieur et de la Justice, en mars, a déjà donné quelques enseignements de ces tests qui ont été confirmés le 8 mai dernier lors du dernier Conseil Justice Affaires Intérieures à Bruxelles puisque la commission est désormais sur le point de sortir cette étude qui porte à la fois sur la base de données des visas et sur sa mise en œuvre grâce aux techniques biométriques.

Le 8 mai, il nous a dit que, selon cette étude, la meilleure technique, suivant ces critères, était la technique de l'empreinte digitale. C'est une bonne nouvelle pour nous parce que nous sommes plutôt sur l'empreinte digitale, parce que c'est une technique éprouvée, séculaire, pour laquelle il n'est pas nécessaire de constituer des bases de données, facile d'emploi et vraisemblablement qui ne nous pose pas trop de problèmes psychologiques et culturels, ce qui n'est pas le cas partout dans le monde.

Voilà Monsieur le Président où nous en sommes. Lundi dernier, le ministre de l'Intérieur a abordé, lors de la réunion des ministres de l'Intérieur et du

G8 à Paris, la question de la biométrie. Pourquoi était-il important d'en parler en G8 ? Simplement parce qu'en parler à l'OACI est utile mais plus difficile parce que c'est une organisation universelle ; l'avantage avec le G8 est qu'il n'y en a que sept à convaincre, ce qui n'est déjà pas simple.

Là encore, la position de Monsieur SARKOZY a été de dire que nous n'étions fermés sur aucune technique, que si on nous convainquait de la plus grande fiabilité et de la plus grande efficacité de l'iris ou de l'empreinte faciale, nous pouvions changer de doctrine, mais nous avons pu constater néanmoins que des ministres se sont montrés un peu plus ouverts sur les empreintes digitales, que le collègue britannique de Monsieur SARKOZY, après avoir été très favorable à l'iris, était plus ouvert sur l'empreinte digitale.

Quant aux Américains, il est difficile de connaître leur position parce qu'en réalité il y en a plusieurs ; plusieurs agences fédérales se concurrencent. Les Japonais n'ont pas vraiment pris position, on sait qu'ils ont des réserves culturelles sur ces techniques même s'ils veulent avancer.

Voilà où nous en sommes.

Monsieur SARKOZY a obtenu, sur une proposition conjointe allemande et britannique, qu'un groupe de travail, sous coprésidence franco-américaine, se réunisse le plus rapidement possible pour travailler sur ces questions. Un groupe « Biométrie » existait au sein du G8, nous avons souhaité y élever la représentation technique et politique des délégations pour qu'avant la fin de la présidence française et le début de la présidence américaine au 1er janvier des propositions soient faites aux ministres pour qu'une position forte puisse être dégagée pour essayer d'accélérer ensuite les négociations au sein de l'OACI.

Je pourrai compléter en disant que M. Nicolas SARKOZY se rend ce week-end à une réunion en Espagne à l'invitation de son homologue espagnol où seront présents les ministres britannique, allemand, italien, français et espagnol ; ils aborderont les questions d'immigration pour essayer d'avancer et cette question sera également à l'ordre du jour. Nous espérons pouvoir avancer de cette manière.

M. LE PRESIDENT. - Merci beaucoup pour ces informations qui sont importantes et essentielles, qui montrent l'actualité de cette question. C'est un peu le fait du hasard. Cela me complique un peu la tâche car, pour un rapport qui doit être présenté début juin, nous sommes rattrapés par l'actualité. Nous le présenterons peut-être de façon temporaire, des mises à jour seront nécessaires plus tard.

Je ne l'ai pas indiqué dans mon introduction, mais il est compris par vous tous qu'il ne s'agit pas pour le Parlement de faire une étude pour une étude mais, après avoir tiré un certain nombre de conclusions techniques et les implications concernant le droit de façon générale, de proposer d'éventuelles modifications législatives ou de nouveaux textes dont certains seront prolongés par des décrets administratifs.

La vocation d'un rapport de l'Office ne se limite pas à l'évaluation scientifique d'une technique donnée à un instant donné, elle est de préparer les travaux législatifs soit à l'initiative du gouvernement soit dans le cadre éventuel d'une initiative parlementaire.

Merci beaucoup Monsieur MARTINON pour cette présentation très complète sur le cadre d'intervention du ministère de l'Intérieur.

Avant d'entamer une discussion que nous pourrons commencer après la fin de prise de parole du ministère, Monsieur SCHMELTZ, je pense que vous avez des informations complémentaires à apporter.

M. Bernard SCHMELTZ, sous-directeur des étrangers et de la circulation transfrontière, Direction des libertés publiques et des affaires juridiques, Ministère de l'Intérieur - Je ne reviendrai pas sur le contexte de politique de sécurité évoqué par Monsieur MARTINON, je voudrais ajouter quelques éléments de contexte juridique, administratif et technique.

Sur les aspects de sécurité, je me permets d'ajouter deux points.

En matière d'immigration clandestine, on a à faire de plus en plus à de véritables filières à caractère mafieux. Il s'agit bien de mettre à mal ces organisations à caractère "mafieux" très proches des systèmes de traite que nous avons pu connaître dans notre histoire. C'est important et essentiel. Nous avons clairement constaté ces dernières années une évolution de ce type.

Il faut remarquer aussi l'évolution des pratiques de fraude. La fraude documentaire connaît une évolution inquiétante ; les fraudeurs sont organisés dans des filières équipées de matériel, des systèmes de récupération, de vol de documents authentiques performants, ce qui nous oblige à introduire dans les titres d'identité, en dehors des éléments de biométrie, des éléments de sécurisation supplémentaires. Cela a un effet sur les processus industriels de fabrication et les processus administratifs de gestion de cette fabrication.

Il y a également derrière tout cela l'idée que la sécurisation des titres (passeport, carte d'identité) vise à rendre un service éminent à nos concitoyens : il s'agit de faire en sorte qu'ils soient protégés de l'usurpation d'identité. L'expérience prouve malheureusement que ce sont des hypothèses qui ne sont pas rares. Les personnes dont l'identité a été usurpée se trouvant dans une situation inextricable, il faut à toute force les protéger.

Dans le même temps, un autre impératif à prendre en compte est celui de la qualité du service public. Nos concitoyens y sont très attentifs, le ministre de l'Intérieur aussi. Il s'agit de faire en sorte qu'en augmentant le degré de sécurité du titre, on ne dégrade pas la qualité du service rendu par l'administration et qu'on préserve les objectifs d'accessibilité aux services de proximité et de rapidité dans la délivrance.

C'est parfois difficile à concilier, mais c'est une préoccupation forte du ministre de l'Intérieur. Je crois qu'il faut mettre en lumière cette notion de service

rendu à nos concitoyens quant à la qualité du service et la qualité du titre qui leur est remis.

Les représentants de la CNIL en parleront, le contexte juridique est clair pour nous, des règles précises s'appliquent à la gestion des fichiers : le principe de proportionnalité, le droit d'accès, l'habilitation des personnes qui manipulent ces fichiers. Le ministère de l'Intérieur entend les respecter scrupuleusement.

Je me borne à remarquer sur ce point qu'au regard de la situation dans d'autres pays européens, nous avons en France une législation très protectrice en la matière.

Par exemple, depuis le début de l'année 2003, a été mis en place à l'échelle européenne un fichier des empreintes digitales des demandeurs d'asile, le fichier Eurodac, et un certain nombre de partenaires nous sollicitent régulièrement pour qu'il soit utilisé à des fins policières. Notre droit ne nous le permet pas aujourd'hui. C'est un point qu'il faut souligner, nous avons un système juridique protecteur de l'individu.

Pour mémoire, l'évolution intervenue le plus récemment pour accroître la qualité du service pour nos concitoyens a consisté à permettre que les mairies puissent être des guichets de dépôt d'une demande de carte d'identité ou de passeport au moyen d'un formulaire unique en place depuis quelques mois, les préfectures étant chargées pour la carte d'identité d'opérer un contrôle du dossier avant envoi à un centre de fabrication. Pour le passeport, les mairies récupèrent le dossier, le contrôle et la fabrication étant prévus dans les préfectures ou certaines sous-préfectures.

L'évolution à venir du passeport conduira à revoir ce système en ce sens qu'il ne sera plus possible de procéder à sa fabrication dans les préfectures et sous-préfectures compte tenu de la difficulté des process industriels à mettre en place.

Il y aura de ce point de vue une évolution (je ne suis pas en mesure d'en dire plus aujourd'hui), de la même manière qu'il sera porté une attention plus forte par les services du ministère de l'Intérieur à la lutte contre la fraude documentaire, ceci afin de protéger nos concitoyens.

S'agissant du contexte technique, Monsieur MARTINON en a parlé, il existe en France une pratique ancienne de la technique des empreintes digitales. Toutefois, une réunion du groupe de travail l'OACI s'est tenue à Montréal ces derniers jours annonçant une réunion du Comité Transport fin mai.

Pour l'instant, on s'acheminerait au niveau de l'OACI vers un standard international qui serait non pas la reconnaissance faciale en ce sens qu'il y aurait mise sous algorithme d'une photo numérisée mais l'introduction d'une photo numérisée, dans une puce sans contact, c'est-à-dire qui pourrait être lue par un lecteur à courte distance dans les aéroports ou les postes frontières.

Voilà où nous en sommes sur ce contexte technique.

En conclusion, j'indiquerai que le ministère de l'Intérieur s'est engagé depuis quelque temps dans une réflexion désignée sous un vocable barbare, celui de « titre fondateur ». C'est l'idée d'accroître la sécurité des titres délivrés à nos concitoyens, tout en améliorant la qualité du service rendu par l'administration.

Le titre fondateur est une procédure d'établissement de cartes d'identité et de passeports en veillant à une meilleure qualité de sécurité des titres, en faisant en sorte qu'une fois sollicité une carte d'identité ou un passeport par le biais de cette procédure, on puisse de façon quasi automatique se refaire délivrer le titre lorsqu'il arrive à échéance.

Je ne peux pas en dire beaucoup plus sur la réflexion sur le titre fondateur, mais je souhaite attirer votre attention sur le fait que la question du passeport ne peut pas être traitée isolément de la question de la carte d'identité et qu'il faut aussi avoir en perspective, même si l'objectif du titre fondateur est la qualité de service et la sécurité des titres, les initiatives qui commencent à se développer de carte citoyenne ou de carte de vie quotidienne, qui seront des cartes à puces délivrées par les collectivités locales, permettant à nos concitoyens d'accéder plus facilement à une série de services (inscription en bibliothèque, en crèche, etc.).

Pour nous, les deux sujets sont disjoints, mais je ne peux pas non plus affirmer qu'ils ne sont pas liés.

M. LE PRESIDENT. - Merci pour ces informations complémentaires de l'état de la situation. Nous voyons bien que cette préoccupation qui est la nôtre au plan national est partagée par les autres pays puisque les individus sont mobiles par nature, même ceux qui n'ont pas des desseins inavouables. Il est donc nécessaire de les autoriser à faire ces différentes étapes de leur migration même si elle n'est que temporaire.

Je vais ouvrir quelques minutes de discussion avant de passer au sujet suivant. Est-ce que quelqu'un souhaite poser des questions complémentaires ?

Sur les conclusions de la réunion de Montréal, nous n'avons pas encore de documents écrits.

M. SCHMELTZ. – Nous étions représentés à cette réunion mais, à ma connaissance, il n'y a pas eu de communication officielle du côté de l'OACI.

M. LE PRESIDENT. - Ce n'est pas vraiment la reconnaissance faciale mais une photo numérisée sans contact direct. J'ai cru comprendre que des options complémentaires pourraient être mises en œuvre.

M. SCHMELTZ. – En effet, il a été évoqué la possibilité pour l'Etat, à titre optionnel, d'introduire, outre cette photo numérisée insérée dans une puce, d'autres données biométriques. Le choix est ouvert entre l'empreinte digitale et l'image de l'iris.

M. LE PRESIDENT. - Vous avez indiqué qu'il y aurait une réunion du Conseil Transport prochainement, le 22 mai.

Monsieur REGNIER nous apportera des éléments supplémentaires sur ces questions internationales. Il est question d'une échéance précise pour les passeports, du moins pour accéder sans visa aux Etats-Unis à l'automne 2004, avez-vous d'autres éléments d'information sur ce point ?

M. MARTINON. - Nous avons eu l'information officiellement hier selon laquelle désormais, au 1er octobre 2003, tout passeport qui ne pourra pas être lu par une machine devra comporter un visa. L'échéance de 2004 vaut toujours pour des passeports sécurisés, qui comprennent au moins une donnée biométrique.

M. LE PRESIDENT. - Ils ont encore raccourci la chronologie. Le nouveau passeport américain est d'une certaine qualité, mais on peut encore le truquer. Nous en avons eu la démonstration à l'aéroport de Tokyo dans la mesure où le système d'holographie peut être perturbé.

M. DIDIER. – Le gouvernement américain était très pressé puisque, dans les premiers textes, on avançait la date d'octobre 2003 pour mettre en place l'usage de la biométrie pour passer les frontières. En fait, à la demande du Congrès, ils ont décalé à octobre 2004 parce qu'ils pensaient qu'ils n'y arriveraient pas dans les délais.

Cette date d'octobre 2003 qui revient sur les passeports lisibles par machine ne me surprend pas.

M. LE PRESIDENT. - C'était d'autant plus prévisible qu'en dehors des données strictement biométriques, ils ont accès aux informations des compagnies aériennes.

J'ai pu vérifier avant-hier qu'ils disposaient d'informations précises accessibles et demandées par les autorités américaines. Lorsque nous étions à Washington il y a un mois, ils nous avaient confirmé que la procédure était en route.

M. Christophe PALLEZ, Secrétaire général de la Commission Nationale Informatique et Liberté (CNIL) - Sur ce point précis, que la CNIL suit avec la plus grande attention, surtout au plan européen puisqu'il y a eu une réunion le 5 mai dernier entre les autorités européennes de contrôle et les autorités américaines, je peux vous confirmer que ce système fonctionne d'ores et déjà et que la transmission d'informations est faite par accès des autorités américaines aux systèmes centraux de réservation.

Il a été dit que les autorités américaines n'avaient pas toujours une position unie - c'est un dossier sur lequel nous constatons certaines divergences entre les agences américaines concernées - mais il n'empêche que le système mis en place par le service des douanes américain fonctionne. Je signale que la CNIL commence à être saisie de plaintes sur ce sujet émanant, non pas de passagers lambdas, mais d'associations bien structurées de défense des droits de l'Homme.

M. LE PRESIDENT. - J'ai cru comprendre que la Commission européenne avait donné son accord au terme d'une négociation assez.

M. PALLEZ. – La Commission européenne a négocié directement avec les autorités américaines. Un protocole préparatoire a été établi dans lequel la Commission engageait un processus pour reconnaître que cette transmission se faisait en adéquation avec les principes de protection des données.

Le Parlement européen a vivement réagi, considérant que la Commission avait outrepassé son mandat et dès lors la Commission est en net retrait.

La question va revenir au cours d'un sommet entre l'Union européenne et les Etats-Unis en juin. Il pourrait être établi un accord mais je pense que nous en sommes loin et que la situation est plutôt raidie. Cela dit, de fait, les Etats-Unis ont imposé la transmission des données et les compagnies aériennes se sont inclinées face à des menaces allant jusqu'à l'interdiction d'atterrir.

M. LE PRESIDENT. – Il était initialement prévu des filtres sur le système pour qu'ils n'aient pas accès à toutes les informations mais cela a été mis en route sans filtres.

M. PALLEZ. – Il n'y a pas de filtres. Les autorités américaines ont pris des engagements sur la conservation des données, l'absence de partage entre l'ensemble des administrations fédérales, sur l'information, mais ce n'est pas considéré pour l'instant par les autorités européennes comme suffisant. J'ajoute qu'en réalité la bataille juridique se déroule plutôt à l'intérieur des Etats-Unis.

Les mesures ayant leur pendant interne, c'est-à-dire les passagers des vols intérieurs américains faisant l'objet de recueil d'informations assez poussé, cela donne lieu à des protestations d'un certain nombre d'individus ou d'associations aux Etats-Unis, probablement à des contentieux.

Je pense que la bataille se jouera d'abord aux Etats-Unis plus qu'au niveau international.

M. DIDIER. – Comme Monsieur MARTINON va nous quitter, je voudrais réagir à son exposé que j'ai trouvé particulièrement clair, ce qui m'a réjoui puisque ces sujets dont nous débattons aujourd'hui recevaient peu d'écho il y a deux ans.

Je constate à travers les propos de Monsieur MARTINON qu'il se passe et qu'il s'est passé beaucoup de choses en très peu de temps, notamment cette année. Je trouve cela très positif.

Il a évoqué le problème des investissements. Tout a un coût. Il faut être attentif, quand on parle de biométrie et d'investissements, à étudier la globalité des coûts. Il existe un coût à la détection du terrorisme, mais très difficile à apprécier.

Un coût plus facile à apprécier est celui du contrôle de l'usage. Pour le passage des frontières automatisé grâce à des techniques biométriques, si la

technique n'est pas fiable, si elle a 20 % de fausses alarmes, soit on la débraye soit on ne peut pas payer le personnel nécessaire pour vérifier les faux rejets.

Il y a un équilibre à trouver entre un coût difficile à apprécier et un coût certain, et le choix des techniques biométriques doit s'appuyer sur des spécifications claires et précises.

Je ne dis pas que les investissements sont considérables, mais qu'il faut les apprécier dans leur globalité.

Je ferai un deuxième commentaire concernant ce qui se passe aux Etats-Unis. Les Etats-Unis n'avaient pas de « ministère de l'Intérieur » mais les événements qui se sont produits ont réuni plus d'une vingtaine d'agences qui essaient tant bien que mal de se mettre en ordre de marche. Autour est apparu la SARPA, sur le même modèle que la DARPA, qui est un organisme dont l'objectif est de définir une stratégie de recherche et développement, une stratégie industrielle autour de la sécurité.

Les Américains essaient de trouver des réponses à leur problème. En parallèle, la conséquence sera la construction d'un tissu industriel lié à la sécurité. Cette organisation peut se transformer en un outil économique dans quelques années et probablement assez rapidement.

M. LE PRESIDENT. - C'est un des points qui sera largement abordé dans le rapport avec un certain nombre de préconisations. Nous avons vu la mise en place de ces structures aux Etats-Unis et au Japon, avec des budgets représentant des milliards d'euros.

Le ministère est très vigilant quant aux décisions qui seront prises, étant entendu qu'en premier point, c'est l'efficacité du système, en second point son coût immédiat d'investissement puis de fonctionnement, et enfin les incidences économiques qui déterminent aussi l'action qui doit être menée.

Je ferai un certain nombre de recommandations auprès des sphères gouvernementales et des propositions concrètes pour la mise en place de structures travaillant sur cette nouvelle « technique ».

Pour compléter, l'harmonisation et la mise en place de dizaines de milliers de fonctionnaires ont semblé initialement chaotique mais, lorsque la machine américaine se met en route, elle est d'une efficacité certaine.

Nous avons pu constater la difficulté de la mise en ordre des différents types de fonctionnaires initialement car une bonne partie de ces personnes n'étaient pas fonctionnaires mais elles ont une motivation forte et une efficacité qui semble de plus en plus « redoutable » -entre guillemets puisque c'est notre sécurité qui est en jeu. La machine est en route et sans état d'âme, naturellement.

Je propose de poursuivre les interventions prévues. Monsieur PALLEZ a déjà pu nous apporter quelques éclaircissements sur un aspect ponctuel car la biométrie n'est pas liée uniquement aux questions de sécurité intérieure ou

internationale, les utilisations sont multiples et variées. Vous nous avez remis un document qui correspond à différents types d'utilisation, de matières et de circonstances diverses et variées[1].

Peut-être pourriez-vous nous éclairer davantage sur les principes fondamentaux qui guident les interventions de la CNIL[2], notamment sur cette question, et la façon dont vous envisagez ultérieurement -et sous quelle forme- ces interventions compte tenu de l'ampleur de la problématique de mise en œuvre.

M. PALLEZ. – La CNIL s'intéresse de près aux questions de biométrie. A l'heure où je vous parle, une délégation de la CNIL se rend à la prison de la Santé, conduite par un député, membre de la CNIL, pour prendre connaissance du système de biométrie qui va être mis en œuvre ou qui l'est déjà partiellement.

M. LE PRESIDENT. - Qui est déjà mis en œuvre.

M. PALLEZ. – Du point de vue de la CNIL, il ne l'est pas mais comme cela arrive souvent, l'expérimentation précède la régularisation juridique.

Il s'agit d'un système d'accès aux parloirs par reconnaissance du contour de la main. C'est typiquement un dossier sur lequel la CNIL se prononce régulièrement et se prononcera la semaine prochaine.

Il est peut-être utile de rappeler pourquoi la CNIL s'intéresse à la biométrie. C'est une évidence, mais je tiens à le rappeler. Tout simplement parce que les données biométriques sont personnelles et que la finalité des systèmes biométriques est l'identification ou l'authentification d'une personne. Nous sommes totalement dans le traitement des données personnelles ou nominatives.

Je rappellerai que cela ressort aussi des textes, et, en particulier, d'un texte fondamental pour nous, qui est la directive européenne d'octobre 1995, que la France n'a toujours pas transposée, selon lequel l'identification se fait par un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, psychique, etc…

Nous sommes au cœur du sujet. Il est bon de rappeler ce texte européen parce qu'il ne faut pas croire que la France et la CNIL sont isolées sur ce terrain ; nous sommes dans un contexte européen qui encadre l'ensemble des activités qui relèvent de la directive, étant précisé que les activités de sécurité publique ne relèvent pas de la directive.

Les mesures d'identification biométrique ou leur version numérisée sont des données personnelles, y compris les images lorsque la vidéosurveillance est couplée à un logiciel de reconnaissance du visage.

Comment la CNIL s'intéresse-t-elle à ces questions de biométrie ? De deux manières, la principale étant sous l'angle de décisions. C'est la raison pour

[1] Voir annexe p.
[2] Commission Nationale de l'Informatique et des Libertés

laquelle je vous ai communiqué un relevé des principales décisions prises dans ce domaine.

Par ailleurs, la CNIL essaie d'avoir une vue d'ensemble parce que même si on a beaucoup parlé de sécurité publique, la biométrie se répand dans bien d'autres domaines et va du policier au civil ou du civil au policier par des allers et retours qui conduisent, d'une certaine manière, à une sorte de banalisation.

Je donnerai quelques éléments d'ensemble mais c'est nécessairement abstrait. Monsieur SCHMELTZ a eu l'occasion de rappeler les principes fondamentaux évoqués par la CNIL lorsqu'elle se prononce sur des dossiers de biométrie, il s'agit des principes de finalité et de proportionnalité.

Pour les décrire simplement, qu'est-ce que la finalité ? C'est le fait que si on fait un traitement biométrique, on définit un objectif, un but, c'est-à-dire les raisons pour lesquelles on le fait. Si on veut l'utiliser à d'autres fins, on sort du cadre et on se heurte au principe de finalité qui est restrictif.

Le principe de proportionnalité est simple à concevoir, difficile à mettre en œuvre et à définir de manière rigoureuse. C'est un peu le lien entre la taille de la mouche et l'ampleur du marteau qu'on utilise pour l'écraser. On voit très bien comment les choses doivent être ajustées.

Il existe d'autres principes : l'information de la personne concernée, le droit d'accès, le consentement (est-il obligatoire ou non de se soumettre à la technique biométrique ?), les principes de sécurité (une fois constituée une base de données biométriques, comment en préserver la sécurité et éviter que les informations circulent là où elles ne le devraient pas ?).

Pour terminer sur ce tableau très général, je dirai que ces principes que je viens d'énoncer ne sont pas des principes de la CNIL, mais sont également dégagés au niveau européen. Je les retrouve dans un document qui émane du groupe de l'article 29, c'est-à-dire les 15 « CNIL » européennes dans des formes diverses qui ont adopté un document retraçant ces principes.

Il existe quelques divergences sur l'interprétation de ces principes, mais le socle commun est là. Il faut être très attentif au fait que nous sommes dans un cadre européen et non pas strictement national.

Plutôt que de développer dans le détail ces principes, j'ai souhaité vous donner un tableau des principales décisions rendues par la CNIL.

Dans ce tableau figurent des avis, c'est-à-dire une forme d'autorisation rendue dans le secteur public, et, à côté, vous avez des déclarations ordinaires qui émanent du secteur privé. Dans ce domaine, la CNIL se borne à délivrer un récépissé sans pouvoir de blocage.

Cela n'empêche pas qu'il puisse s'établir un dialogue mais la CNIL est informée, elle instruit éventuellement mais son pouvoir est limité. J'y reviendrai quand j'évoquerai l'évolution législative en cours.

J'ai souhaité vous présenter ce tableau parce qu'il donne une grille d'analyse de la manière dont la CNIL procède. Il fait apparaître très clairement les critères qui permettront à la CNIL de juger de la validité juridique d'un système de biométrie, qu'il soit public ou privé, par rapport aux principes que j'ai énoncés.

Il ressort très clairement que cette grille d'analyse utilise comme premier critère la question de savoir quel est le type de biométrie employé : l'empreinte digitale, le contour de la main ?

La distinction fondamentale, c'est entre la technique qui laisse des traces, telle que l'empreinte digitale ou l'ADN, et celle qui n'en laisse pas, comme le contour de la main, l'iris ou la rétine avec, entre les deux, la reconnaissance faciale sur laquelle on peut avoir une hésitation.

Pourquoi ce critère des traces ? Parce que quand il y a des traces, il y a un risque de détournement. Même si la finalité des bases conçues dans le secteur privé ou dans des administrations n'a aucun caractère policier, il y a danger de réutilisation à d'autres fins et un risque de détournement de la finalité.

Nous sommes conscients que les risques de détournement de base de gabarits sont faibles, mais nous sommes très attentifs à cet aspect des choses.

On croisera le critère « type de biométrie » avec un autre critère transversal qui est le « type d'impératif de sécurité mis en œuvre ». D'une manière générale, dans ces décisions, ce n'est pas l'empreinte digitale qui est rejetée, mais son utilisation quand elle paraît excessive.

Pour la Banque de France et les zones hautement sécurisées, il n'y a pas de problème avec l'empreinte digitale. Pour la Cité académique de Lille et l'accès de certains personnels aux locaux dans lesquels on conserve les copies d'examen, il n'y a pas de difficulté non plus compte tenu d'un impératif de sécurité important.

En revanche, pour l'URSSAF de Corse et le contrôle des accès du personnel au motif des risques de terrorisme - qui ne sont pas niés par la CNIL - la décision a été défavorable considérant qu'il y avait un manque de proportionnalité entre la technique retenue et le risque. L'URSSAF de Corse a représenté un dossier avec le contour de la main qui a été avalisé par la CNIL.

C'est un premier élément d'analyse. Le deuxième, ce sont les modalités de stockage des gabarits biométriques avec la question fondamentale de savoir qui conserve les données. Sont-elles conservées de manière individuelle sur une carte à puce, un téléphone portable ou toute autre technologie de ce type ? S'agit-il d'un stockage local ou d'un stockage sur une base de données centralisée avec tous les avantages et les risques que cela peut présenter dans la gestion, l'accès à ces bases et de détournement ? Là encore, l'utilisation de la base de données sera confrontée au critère fondamental de savoir quel est l'impératif de sécurité et s'il justifie la constitution d'une base de données.

Un troisième critère important qui n'apparaît pas tellement dans ce tableau, ce sont les mesures de sécurité prises, notamment s'il y a utilisation d'une base de données, par le gestionnaire du traitement et notamment les mesures de chiffrement. Il existe une gamme de solutions que je serai incapable de vous décrire mais qui vont jusqu'au chiffrement par le gabarit lui-même.

A travers cette suite de décisions qui a une certaine cohérence, on peut dégager une doctrine empirique de la CNIL qui consiste à dire que, s'il n'y a pas de stockage des gabarits dans une base, il n'y a pas de difficulté. Dans la mesure où le gabarit est stocké sur le porteur, il demeure inaccessible à un tiers.

S'il y a une base de données, la première question est de savoir si c'est une biométrie avec trace ou sans trace. Si la biométrie est sans trace, les risques paraissent limités pour la CNIL ; si c'est une biométrie avec trace, c'est le principe de proportionnalité : est-ce que l'impératif de sécurité justifie le degré maximal de biométrie, c'est-à-dire trace plus base de données centralisée ?

Voilà la doctrine telle qu'elle s'est dégagée depuis des années et qu'elle se poursuit.

Pour revenir à mon exemple de la prison, je présume que la CNIL ne verra aucun inconvénient compte tenu de l'impératif de sécurité et du fait qu'il s'agit du contour de la main.

J'ai parlé des formalités, j'ai indiqué qu'elles consistaient en une demande d'avis avec la possibilité de passer outre un avis défavorable mais, généralement, on trouve un terrain d'entente avec les administrations et les ministères qui nous consultent. Pour le secteur privé, c'est un système de déclaration.

Dans ce tableau apparaît une série d'expérimentations, la CNIL est favorable à toutes les formes d'expérimentation. La dernière qu'elle a autorisée était, en décembre dernier, l'expérimentation par Air France, dans le cadre des vols vers Tel Aviv, du stockage de l'empreinte digitale des passagers. Au moment où ils retirent leur carte d'embarquement, ils font enregistrer leur empreinte digitale sur la carte d'accès à bord, on peut vérifier au moment où le passager se présente au comptoir d'embarquement que c'est bien le même passager que celui qui a retiré la carte une demi-heure plus tôt.

C'est une expérimentation d'Air France pour laquelle la CNIL a donné un avis favorable. Elle la suit et attend avec intérêt les résultats. C'est le type de démarche que la CNIL met en œuvre.

Voilà pour l'état actuel des formalités mises en œuvre. Vers quoi nous dirigeons-nous ? Il suffit de regarder le texte voté par l'Assemblée nationale en janvier dernier et par le Sénat le 1er avril dernier. Sur ce point les deux chambres n'ont pas eu de divergence. Alors que les formalités seront assouplies et que nous passerons dans des régimes de simple déclaration, notamment pour le secteur public, parmi les quelques cas pour lesquels l'autorisation de la CNIL sera nécessaire figurent les traitements automatisés comportant des données biométriques

nécessaires au contrôle de l'identité des personnes. C'est l'article 25, huitièmement, du texte législatif en cours de discussion.

Cela signifie d'une certaine manière que la CNIL verra ses pouvoirs renforcés à l'égard des applications biométriques du secteur privé. Cela correspond à l'idée qu'il s'agit d'un enjeu majeur pour les libertés individuelles et la vie privée.

M. LE PRESIDENT. - Merci pour cette présentation.

Si le texte est confirmé définitivement et la loi publiée, quels sont les risques éventuels d'encombrement et de durée des procédures ?

Quand on voit aux Etats-Unis l'utilisation très largement répandue du contour de la main pour assurer le pointage des salariés, l'utilisation aussi très large de la biométrie non pas sur le plan de la sécurité mais pour les prestations sociales, quelles qu'elles soient, comment la CNIL va-t-elle pouvoir faire face à des milliers -pour ne pas dire des dizaines de milliers- de demandes qui émergeront inévitablement dans un horizon assez proche ?

Notamment si les industriels ont des outils très performants et très efficaces, beaucoup d'entreprises du secteur privé demanderont à utiliser ces systèmes quels qu'ils soient. N'y a-t-il pas une difficulté matérielle toute simple de prise en compte par votre structure de ce flux de demandes et de leur suivi ?

M. PALLEZ. - Je ne suis pas très inquiet sur ce plan dans la mesure où nous avons l'habitude de ce genre de question. Par exemple, nous recevons des centaines de demandes d'avis émanant des communes pour l'instauration de systèmes d'information géographique. Quand on a vu une ou deux fois un système, quand on connaît le logiciel et la société qui le fait, cela devient très répétitif. Il y a une décision de principe à prendre au départ, puis cela a un caractère automatique.

Si on sortait quelque chose de nouveau, de différent, cela demanderait un certain temps de réflexion, mais tout ce qui est répétitif se fait très rapidement. On ne sait pas encore comment cela fonctionnera, mais beaucoup d'autorisations seront faites très rapidement sans débat.

M. LE PRESIDENT. - Vous avez vous-mêmes une procédure automatisée si j'ose dire.

M. PALLEZ. – Nous avons des formes de procédures standardisées.

Nous ne sommes peut-être pas prêts à aller jusqu'à la définition de normes simplifiées, ce n'est pas prévu par la loi, mais nous aboutirons probablement à des systèmes comparables. Cela ne devrait pas, sur le plan strictement bureaucratique, être une cause d'embouteillage.

Cela dit, est-ce que le simple accès des salariés ou le contrôle des horaires par les empreintes digitales sont légitimes ? Je ne veux pas trancher mais vous voyez dans le tableau qui vous a été remis que la mairie de Goussainville a

demandé à faire un contrôle des horaires avec l'empreinte digitale et que la CNIL a rendu un avis défavorable.

M. LE PRESIDENT. - En l'occurrence, il s'agit du contour de la main aux Etats-Unis.

M. PALLEZ. – Pour le contour de la main, il n'y aura guère de difficulté. Il a été admis par la CNIL pour l'accès des employés de l'URSSAF de Corse à leurs bureaux. Cela donne une indication assez claire.

UN INTERVENANT. – Comment qualifiez-vous le niveau de sécurité par rapport à ce qui a été énoncé précédemment en termes d'utilisation de la biométrie et de contrôle de cette biométrie aux frontières ?

M. PALLEZ. – Sur le contrôle aux frontières, nous sommes dans des problématiques différentes où interviennent les textes législatifs. La CNIL a donné un avis sur l'avant-projet de loi relatif à la maîtrise de l'immigration et un avis favorable à la création des deux bases de données concernant, d'une part les étrangers en situation irrégulière, d'autre part, les demandeurs de visa, sachant que les deux articles de loi font référence expresse à la loi de 1978.

Nous souhaiterions que ce soit plus détaillé et que les finalités soient mieux précisées. Nous avons quelques réserves, mais qui sont plutôt dans la forme que dans la démarche.

L'appréciation de la sécurité se fait *in situ* sur des systèmes que nous connaissons mal. Je suis embarrassé pour vous donner une appréciation et vous dire que la CNIL valide ou non la sécurité de ces systèmes.

M. DIDIER. – Je pense que nous avons là la démonstration d'une évolution de plus en plus rapide de l'usage de la biométrie. Le fait que la CNIL s'en occupe est un signe de maturité de cette matière.

J'aurai deux niveaux de commentaires à faire, des commentaires sur les principes du premier niveau et un commentaire sur le corps de concepts qui se dégage à l'usage des quelques années de sujets que vous avez eu à traiter.

Vous avez dit qu'il y avait une communauté de vues au niveau de l'Europe, vous avez parlé du groupe de l'article 29 sur les grands principes de finalité, proportionnalité, etc. On est d'accord sur les principes, mais lorsqu'il s'agit de les mettre en œuvre, les appréciations sont de nature différente.

Les principes de proportionnalité et de finalité ne sont pas faciles à mettre en œuvre. Par exemple, sur le droit d'asile, certains pays qui font partie du groupe de l'article 29 sont arrivés à des conclusions différentes. Ce n'est pas choquant, mais cela démontre le clivage possible entre un point de vue apparemment commun et des mises en œuvre différentes.

Par ailleurs, j'ai apprécié à travers les différents rapports annuels que vous avez émis la création de ce corps de concepts qui vous sert de guide pour

mesurer les risques associés à l'usage de la biométrie. Vous avez parlé de technique de trace. J'apprécie la recherche, je ne suis pas d'accord sur les conclusions.

Je prends un exemple. Aujourd'hui, vous venez de laisser quelques dizaines de minutes de traces vocales dans le micro, il existe des fichiers vocaux dans le monde.

Que veut dire trace ? La trace est un concept qui évolue avec l'évolution des technologies. Demain, les centres vocaux deviendront des outils potentiels biométriques.

Il existe d'autres concepts, le caractère participatif ou non. Le fait que l'on puisse reconnaître quelqu'un à son insu avec une caméra à reconnaissance du visage est non participatif. On pourrait discuter sur le caractère intrusif ou non lorsqu'on pose une empreinte qui est un acte volontaire. L'individu qui le fait sait ce qu'il fait, il signe son acte. En revanche, l'individu qui passe dans la rue, qui ne souhaite pas être identifié, l'est de façon non participative. C'est un autre concept.

En matière de proportionnalité et de finalité, vous avez cité quelques exemples sur le contrôle d'accès aux cafétérias dans les universités par exemple. Ce sont des applications qui se développent beaucoup à l'étranger. On se trompe quand on dit que le seul objectif est un objectif de gestion de facturation de l'étudiant à la cafétéria.

En fait, beaucoup de ces applications ont pour objectif de supprimer le badge parce que, d'un côté, il y a des problèmes de gestion, mais aussi parce que le badge est un moyen de « caïdat »: les grands dans les écoles vont menacer les petits pour récupérer le badge et s'acheter un Coca Cola.

Aux Etats-Unis, il existe des expériences de suppression de carte dans les moyens de paiement. Quels sont les segments utilisateurs intéressés par cette approche ? On trouve le segment des « golden boys » qui souhaitent être reconnus. Plus intéressant, on constate que les personnes âgées sont très intéressées par ces systèmes parce qu'elles n'aiment pas se promener la nuit avec des cartes de crédit pour aller acheter une pizza. Il y a le même souci de finalité.

Tout cela pour dire que la finalité est proportionnelle ou que la proportionnalité n'est pas une finalité. Vous êtes sur un sujet extrêmement riche, complexe, et vous aurez probablement à évoluer aussi avec la technique.

De ce point de vue, je me réjouis que vous ayez annoncé le fait que les procédures d'agrément, tout au moins l'avis de la CNIL, allaient être traitées plus rapidement. C'était effectivement un problème. Nous étions dans une période où vous aviez à apprécier. J'espère qu'aujourd'hui les délais ne se mesureront plus en semaines sur ces sujets parce que même sur des applications répétitives, ce sont des délais parfois supérieurs à plusieurs mois qu'actuellement nous constatons.

M. LE PRESIDENT. – La doctrine s'élabore dans un cadre qui est la référence de la CNIL au vu des propositions formulées, des demandes

d'expérimentation, et il est important de connaître les règles du jeu pour que les demandeurs et les entreprises puissent faire des propositions qui d'emblée incorporent ces références de la CNIL.

L'évolution des techniques, nous l'avons constaté aussi, notamment des techniques américaines, risque toujours d'être en amont ou du moins au-delà du cadre doctrinal qui aura été élaboré. C'est aussi à la CNIL de pouvoir suivre de façon précise et régulière l'information nécessaire.

Je crois d'ailleurs que dans une des propositions qui seront formulées, d'une cellule dédiée au niveau interministériel aux questions de biométrie, il y a celle que la CNIL puisse en faire partie puisque là où seront menées des réflexions sur la mise en œuvre et la veille stratégique des différentes techniques de biométrie, il faudra que d'emblée soient associés ceux qui sont habilités à donner les autorisations d'usage.

Il me paraît fondamental que vous soyez en amont des processus, avant les expérimentations, associés à la connaissance des outils qui s'élaborent et des technologies qui évoluent à la vitesse que l'on sait.

Il n'est pas invraisemblable de penser que si la biométrie actuelle se limite aux images de surface, nous disposerons de techniques biométriques, à une échéance rapide, utilisant l'ADN. Il n'est pas exclu que l'on puisse avoir instantanément l'ADN d'un individu et qu'au-delà des procédures actuelles sur les fichiers, cette technique puisse être utilisée en biométrie courante.

Par conséquent, il faut que les chercheurs, les industriels, les utilisateurs et ceux qui assurent le cadre de contrôle, sous quelque forme que ce soit, soient associés en amont pour que les expérimentations soient mises en œuvre dans de bonnes conditions et que les utilisateurs ne soient pas confrontés, lorsqu'ils ont décidé de mettre en œuvre un système, à une impossibilité administrative ou une tutelle quelconque.

Ce sera une des propositions de ce rapport, à l'image de ce qui se fait aux Etats-Unis et au Japon et qui s'avère efficace.

Pr CABANIS. - Je voudrais remercier et saluer comme d'autres l'ont fait avant moi la clarté du document de Monsieur PALLEZ et son exposé.

Je voudrais vous poser deux questions.

La première concerne la hiérarchisation qui semble apparaître dans les textes émanant de la CNIL, notamment pour le musée du Louvre, avis favorable de la commission *« reléguant l'utilisation des empreintes digitales à des cas très spécifiques de sécurité »*.

De la même manière, vis-à-vis des Aéroports de Paris, vous semblez évoquer une hiérarchisation des techniques, ce contour de la main vous apparaissant comme le plus simple. Je m'aperçois que cette notion de trace évoquée précédemment peut être une approche.

Comme vient de le souligner notre président, les techniques évoluent très vite, nous savons que certains systèmes d'infrarouge ou d'échographie reviennent exactement à la même application de l'individu. Il faut avancer la main quelque part, c'est tout, on sait ou on ne sait pas ce qu'il y a en dessous de la main.

Dans cette évolution qui a été appelée de leurs vœux par d'autres que moi auparavant, la CNIL se place-t-elle sur l'outil en général ou simplement du côté de l'individu ressentant une agression ou une nocivité quelconque ? Quelle est la chose la plus importante ?

Ma deuxième question est d'ordre plus technique. De quelle main s'agit-il ? Dans la notion de contour de la main naît ce point essentiel qu'est la variabilité corporelle de symétrie. Nous sommes un corps symétrique, latéralisé selon notre organisation de mammifère, nous avons la même chose à droite et à gauche, mais cela signifie un coefficient de corrélation droite/gauche, et nous savons qu'un coefficient de corrélation, par exemple de longueur du membre supérieur droit par rapport au membre supérieur gauche, ne dépasse pas 60 %. Nous ne sommes pas symétriques, notamment sur les longueurs des membres.

Par ailleurs, nous sommes parfaitement symétriques quand nous voyons bien parce que nous avons deux yeux. En revanche, la vision binoculaire et stéréoscopique chez le sujet normal que nous sommes, c'est-à-dire voyant parfaitement, a un degré de corrélation entre le côté droit et le côté gauche atteignant pratiquement 90 % parce que c'est la condition pour avoir une vision en relief.

Bref, cette technique infiniment simple d'un contour d'une extrémité d'un membre cumulant un certain nombre de variabilités jusqu'à l'extrémité, donc normalement le plus variable de tous nos éléments symétriques pris pour l'un d'entre eux, a-t-elle un degré d'évaluation qui vous a été quantifié dans sa validité ? Avez-vous eu à raisonner devant des résultats de corrélation de validité d'une main par rapport à des techniques comme celles de l'iris ? Si j'ai bien compris, elle se situe tout en bas, est-elle beaucoup plus variante ?

M. PALLEZ. – S'agissant de la hiérarchisation, vous avez fait intervenir le critère de l'intrusion et du désagrément qu'un individu peut subir dans le contrôle. C'est un critère que nous connaissons, que nous regardons. Nous sommes conscients que l'iris est une technique intrusive, mais ce n'est pas un critère que nous allons faire intervenir directement parce qu'il ne se raccorde pas tellement aux principes que nous avons à mettre en œuvre.

Ce qui a été dit tout à l'heure sur les aspects culturels de telle ou telle technique montre que c'est variable selon les pays. Nous ne nous intéressons pas à l'individu dans son rapport physique à la technique.

Je prends un autre exemple, dans la loi sur le fichier national des empreintes génétiques, il y a toute la problématique du prélèvement obligatoire ; la CNIL ne s'est pas vraiment intéressée à cette question. Je reviens sur les commentaires de tout à l'heure sur l'idée de consentement, d'image prise à l'insu de l'individu, c'est un point important.

Sur l'aspect physique du contact avec l'outil de mesure, nous avons ce critère en tête mais nous ne le faisons pas intervenir de façon importante dans nos décisions.

Par ailleurs, sur le contour de la main, j'ai beaucoup appris en vous écoutant. Je suis juriste, je n'ai donc pas de compétence très poussée dans ce domaine. Je dirai simplement que la CNIL s'efforce d'avoir une expertise sur la fiabilité mais, là encore, la fiabilité d'un système, c'est le souci premier de celui qui met en œuvre le traitement.

C'est aussi le souci de la CNIL dans la mesure où un traitement doit être fiable. S'il aboutit à une identification fausse, il pose un problème au regard de nos principes.

Néanmoins, nous n'avons pas poussé l'expertise assez loin pour que je puisse faire un commentaire, et lorsque nous examinons les dossiers, il faut reconnaître que nous n'allons pas aussi loin que les perspectives que vous avez ouvertes. Cela me conduit à dire que nous avons besoin de participer à des groupes, des cercles, des centres dans lesquels nous puissions bénéficier de ce type d'expertise. Même si nous-mêmes développons une expertise puisque la CNIL a une direction de l'expertise et essaie de développer son expertise autonome, nous avons besoin du concours des scientifiques pour nous éclairer sur des aspects que nous n'avons pas totalement en vue.

Sur chaque dossier examiné sur le plan juridique, il y a un regard d'experts essentiellement informatiques qui donnent une appréciation, qui font des notes techniques et également beaucoup de veille technologique. Sur la biométrie, nous en faisons énormément pour rester au niveau.

Mme HEROLD. – Je n'entends pas beaucoup parler depuis ce matin de la durée de conservation. Cela me paraît un élément à envisager.

Par ailleurs, le contour de la main varie dans le temps. En d'autres termes, serons-nous amenés à des prises d'empreintes régulières de telle sorte que le fichier sera toujours valable ? C'est une autre façon de poser le problème de la durée de conservation et cette durée me paraît d'autant plus importante qu'il s'agirait de système de reconnaissance du visage couplé avec de la vidéosurveillance.

La vidéosurveillance (c'est une banalité de le dire) peut déjà limiter ma liberté de circuler, d'aller et de venir de façon anonyme ; si elle est couplée à un système de reconnaissance des visages, cela devient dramatique, et je ne voudrais pas parler des manifestations d'hier.

Voilà quelques questions qu'il faudrait essayer d'envisager.

M. PALLEZ. – Vous avez raison d'évoquer la durée de conservation, j'aurais peut-être dû en parler. Ce n'est pas un critère pour la CNIL d'acceptation ou non d'un système de biométrie, c'est un critère qui découle de la finalité que nous mettons en œuvre classiquement.

Si la base a été conçue pour permettre l'accès à la cantine scolaire, la durée de conservation est de l'année scolaire ou des quelques années de scolarité.

Cela m'amène à parler du problème de la variabilité du contour de la main. Nous avons été confrontés à cette question pour les cantines scolaires. Pour le collège de Carqueiranne pour lequel nous avons donné une autorisation pour un système de contrôle de la main, on nous a indiqué que les adolescents voyaient leur main évoluer mais qu'au cours de l'année cela ne posait pas de difficultés. Pour nous, c'était plutôt une sorte de garantie que le contour de la main d'un adolescent ne serait guère utilisable cinq ans après. Tout cela est assez lié et il est vrai que la question de la conservation est très importante.

M. DIDIER. – Le contour de la main est une technique née à l'université de Standford pour le contrôle d'entrée aux examens. Par la suite, une société s'est créée, Identimat. C'est une technologie qui n'est pas d'un niveau de sécurité comparable à celui évoqué tout à l'heure ; en matière de sécurité des Etats, c'est une technologie qui n'est pas envisagée.

Vous parliez tout à l'heure de la main gauche et de la main droite, cette technique ne peut traiter que des mains droites, des plots vous imposent de placer la main droite, ce qui veut dire que les gauchers doivent prendre l'habitude de donner leur main droite.

C'est une technique, comme toutes les techniques biométriques, soumise à quelques difficultés. Par exemple, les personnes âgées qui ont des rhumatismes ne peuvent plus se faire reconnaître.

En matière de durée de conservation et d'évolutivité, en l'état actuel de la technique, étant donné l'implémentation retenue par l'industriel, on est protégé, mais rien n'empêche d'avoir des algorithmes qui recherchent des invariants en fonction du temps.

Là encore, il faut faire très attention, la technique évolue, et ce que l'on dit aujourd'hui sera peut-être faux demain.

M. LE PRESIDENT. - Je crois que se pose aussi la question de la durée de conservation dans les maisons d'arrêt.

Je vous propose une pause avant de reprendre la suite.

(la séance, interrompue à 11h00, est reprise à 11h15)

M. LE PRESIDENT. - Je vous propose de passer à l'approche industrielle. Nous avons la chance dans notre pays de disposer d'au moins deux grandes entreprises ayant une couverture mondiale dans ce domaine. Comme je l'ai indiqué, la biométrie a des implications qui ne doivent pas nous échapper sur le plan économique, et, des choix qui seront ou qui sont en train d'être opérés, découlera un certain nombre de conséquences économiques que nous ne pouvons pas évacuer de nos réflexions.

Je sais que par le passé notre pays n'a pas toujours été aussi vigilant sur ces paramètres et a laissé échapper beaucoup de choses. Depuis quelques années maintenant, l'intégration « à l'américaine » de toutes les conséquences des décisions politiques ou administratives doit être prise en compte. Cela n'échappe pas à nos amis d'outre-atlantique ou japonais.

A ce stade de la présentation, je serais heureux que SAGEM et Thalès puissent donner leur vision de la biométrie, les perspectives qu'elle ouvre dans les applications en termes de difficulté administrative en France et aussi au plan international.

Il faut aussi évoquer les incidences économiques, étant entendu que dans les instances internationales, il existe une tradition de lobbying de plusieurs pays étrangers, notamment auprès des instances européennes. Je ne parle pas des instances américaines, ce n'est plus une tradition, c'est un fait bien acquis. On ne sait pas où se situe la réflexion, en tout cas la décision.

Au plan européen, beaucoup d'entreprises européennes ont compris et mesuré l'enjeu qu'il y avait à participer au processus décisionnel au niveau bruxellois, notamment dans les structures dites de « comitologie » ou ailleurs. Nous avons une vieille pudeur, je n'en connais pas toutes les raisons, certaines sont malencontreuses qui font que les industriels sont insuffisamment associés au processus d'information la plus complète possible.

Dans ces conditions, je serais heureux que nous puissions avoir cet éclairage tout à fait indispensable et permettant d'avoir une approche suffisamment solide des choses pour qu'ensuite les décisions soient prises de la façon la plus efficace possible.

M. Bernard DIDIER, Directeur du développement des activités sécurité de la Sagem – Monsieur le Président, mesdames, messieurs,

Je suis directeur du développement des activités sécurité de la SAGEM. Ce que je vais vous dire aujourd'hui repose sur plus de vingt ans de pratique et de recherche en matière d'usage de la biométrie.

En 1982, la Caisse des Dépôts m'avait demandé de créer une société qui s'appelait Morphosystème et qui est devenue très rapidement le leader mondial du traitement automatique des empreintes digitales.

En 1993, cette société a été rachetée par SAGEM. Aujourd'hui, en matière de grands systèmes d'identification biométrique, la SAGEM détient 50 % des parts de marché mondiales, le numéro deux en détenant un peu moins de 20 %.

Je reprendrai la suggestion de Monsieur le Président, j'articulerai ma présentation en trois volets.

Quelles sont les possibilités actuelles de la biométrie ?

Quels développements peut-on en attendre ?

Quelles sont les suggestions et recommandations en matière de développement de la biométrie en France et dans le monde ?

L'exposé sera court. Chacun de mes propos est un point d'entrée thématique qui mériterait quelques heures de développement. J'essaierai d'être concis.

Quelles sont les possibilités de la biométrie ?

Premier constat : la biométrie, par reconnaissance d'empreintes digitales, est d'un usage courant et connaît un développement significatif.

Le caractère exploratoire de la réflexion officielle conduite en France ne doit pas cacher une évidence : aujourd'hui, dans beaucoup de pays dans le monde, on utilise quotidiennement la biométrie des empreintes digitales pour identifier ou authentifier des personnes.

Si j'avais à dégager une grande ligne sur ces vingt dernières années, je dirais que l'élément majeur n'est pas l'usage des techniques biométriques en matière d'identification criminelle. Sur ces vingt dernières années, c'était annoncé. Ce n'est pas non plus l'usage de la biométrie au quotidien. Vous en avez très peu vu. Là encore, ce secteur d'activité attend en vain depuis des années un démarrage toujours annoncé.

L'élément le plus significatif, le plus exceptionnel pour moi est l'usage depuis ces dix dernières années de la biométrie par des gouvernements à des fins non policières. Les discussions que nous avons aujourd'hui ne sont pas les conséquences de ce qui s'est passé en 2001, mais l'évolution logique d'une tendance mondiale sur la réflexion autour de la biométrie.

Quelques faits pour illustrer ces propos.

Sur plus de 50 Etats que nous avons équipés durant ces vingt dernières années, 19 gouvernements utilisent la biométrie à des fins non policières. C'est, par exemple, l'Etat de New York pour la gestion de son assistance sociale, la délivrance des passeports en Argentine, etc.

L'ensemble des systèmes mis en place gère une population de plus de 180 millions d'habitants adultes. La capacité globale de ces systèmes installés dans le monde est de 100 millions de comparaisons d'empreintes digitales à la seconde.

Un autre élément significatif en termes de puissance de calculs : le plus gros système non policier biométrique a une capacité de recherche comparable à celui du FBI.

Deuxième constat : depuis peu, certains des grands systèmes ont pu couper leur dépendance avec des architectures de machines spécifiques. Il n'existe que deux ou trois sociétés dans le monde qui maîtrisent la mise en place de très grands systèmes biométriques capables de gérer des dizaines de millions de personnes et de faire des dizaines de milliers de recherches par jour.

Quelle est la limite aujourd'hui de la technologie en matière d'identification ? Je l'estime à entre 100 et 200 millions de comparaisons par seconde pour un système. C'est ce que nous sommes capables de montrer et de démontrer.

A partir du moment où cette limite ne dépend plus d'architectures de machines spécifiques, elle va pouvoir profiter des évolutions régulières de l'augmentation de la puissance des calculateurs. Cette limite sera repoussée tous les ans.

En matière de complexité des systèmes aussi, il est intéressant de constater que les flux sont plus difficiles à gérer que les grandes populations. A un moment, il faut en tenir compte puisque la problématique aujourd'hui est en train de se transformer en problématique à la fois de base mais aussi de flux extrêmement importants. Des limites architecturales sont à considérer.

Les chiffres que je vous ai donnés permettent de répondre à des questions qui se posent aussi bien en Europe qu'aux Etats-Unis.

Troisième constat : la technologie empreintes digitales est certainement plus mâture et a donc anticipé un usage futur et diversifié.

On m'a demandé d'apporter quelques éléments pour illustrer mes propos. Ceci est un boîtier biométrique, vous avez un lecteur d'empreinte, vous pouvez mettre une carte à puce pour contrôler l'identité du doigt de la personne avec le gabarit contenu dans la carte à puce. Ce boîtier permet aussi de stocker 50 000 personnes et de les rechercher en moins de dix secondes. Il est totalement autonome, on peut le munir d'une batterie. Ce boîtier a été vendu à plus de 70 000 exemplaires.

Deuxième élément, un système de contrôle d'accès biométrique. Ceci s'adresse au marché de l'industrie.

Troisième élément plus amusant, un téléphone sécurisé par empreinte digitale. Cela s'adresse aux consommateurs.

Vous avez ici un lecteur d'empreinte, une unité de calcul qui traite l'empreinte et une batterie. La totalité de la fonction biométrique tient dans la main et a la taille d'un porte-clés. Cela vous laisse envisager les usages futurs grand public de la biométrie.

Quatrième constat : en matière de performance, il n'existe pas de technologie absolue. Ceci a été évoqué tout à l'heure. Chacune des technologies majeures connaît des difficultés à enregistrer une frange spécifique de population. Chacune de ces technologies est soumise à des erreurs, c'est-à-dire ne reconnaît pas une personne autorisée, surtout quand on demande un niveau de sécurité élevé.

Ce n'est pas propre à la biométrie. Tout système de sécurité est soumis à des erreurs quand on fait des analyses systémiques.

Regardons plus précisément les trois technologies majeures. L'empreinte a de bonnes performances, elle est d'un usage démontré. L'iris a un potentiel de performance comparable à celui de l'empreinte digitale, mais c'est une technologie jeune qui n'a pas fait ses preuves dans la mise en place de grands systèmes. Le visage a des performances moyennes et médiocres lorsqu'on parle d'identification.

Cinquième constat : en matière de choix d'usage de techniques biométriques, les critères de performance ne sont pas les seuls pris en compte. Nous avons évoqué tout à l'heure l'existence de fichiers, le caractère participatif, le contact. Par exemple, il est connu qu'en Asie la technologie biométrique à contact ne sera peu utilisée pour des raisons d'hygiène. On peut se poser la question dans les prisons du caractère hygiénique des techniques par reconnaissance de la main.

Selon le problème que vous avez à résoudre, si vous voulez identifier des individus dangereux, l'existence de fichiers criminogènes va vous intéresser et vous mettrez en avant l'empreinte et le visage malgré les performances du visage. En revanche, si vous voulez faire une veille non participative, vous allez utiliser la reconnaissance du visage à distance. Si vous tenez compte des libertés individuelles, de l'hygiène, vous prendrez l'iris.

Il est aussi possible d'utiliser plusieurs techniques biométriques. Vous pouvez identifier une personne à partir d'une empreinte digitale et contrôler son authenticité à travers l'iris.

Si la performance est un objectif fondamental, alors vous pouvez combiner deux techniques pour essayer de profiter des points forts de l'une pour compenser les points faibles de l'autre.

En conséquence, il est fondamental sur ces problèmes de biométrie d'avoir une expression précise des besoins et c'est l'une des difficultés.

Sixième constat : en matière de protection des libertés individuelles, il existe des solutions qui rendent difficile l'usage non autorisé de la fonction biométrique - des techniques de cryptage que vous avez évoquées tout à l'heure - mais il existe aussi des techniques de dissociation des informations biométriques.

Quels développements peut-on en attendre ?

1. Les Etats utiliseront de plus en plus les systèmes biométriques pour contrôler la délivrance des droits.

Quand on regarde dans le passé, on a fait porter l'emphase sur le contrôle de l'usage d'un droit (on contrôle l'identité, le passage aux frontières) ; en revanche, l'effort n'a pas porté sur le contrôle de l'unicité de la délivrance du droit.

Nous le voyons au travers des exemples que je vous ai cités, de plus en plus, les Etats réfléchissent à la vérification de demandes multiples ; plus grave encore, le problème d'usurpation d'identité qui amène les Etats à réfléchir à cette approche.

Cette tendance du contrôle de la délivrance se retrouve outre-atlantique sur des sujets de plus en plus civils, notamment pour contrôler des demandes d'emploi par rapport à des fichiers d'interdits, par exemple les employés aéroportuaires ou de distributions de fonds.

2. Par ailleurs, l'usage de la biométrie dans les visas et les passeports devrait se généraliser, mais faire naître quelques problèmes en Europe.

La volonté américaine d'utiliser la biométrie à très court terme est structurante pour les Etats majeurs. La refonte des passeports prendra du temps, en revanche les visas seront des sujets plus rapidement adressés parce qu'il n'y aura pas les mêmes contraintes et cela concernera les citoyens qui ne font pas partie du pays.

De ce fait, la contrainte de sécurité se déplacera des frontières d'un Etat au lieu de délivrance des visas et c'est un élément majeur. La sécurité ne commencera plus aux frontières des Etats.

L'Europe, pour sa part, est hétérogène en matière juridique et il existe des divergences d'analyse en matière d'usage de la biométrie. Si vous ajoutez la dimension Schengen, l'ensemble des acteurs aura probablement beaucoup de difficultés à se mettre d'accord, cela leur prendra plus de temps que pour les Etats-Unis.

3. Nous avons parlé tout à l'heure d'interopérabilité, les standards et l'interopérabilité seront probablement à l'avenir un ferment de nouvelle compétitivité industrielle. On pensait qu'il suffisait de choisir une technique, le problème ne se résume pas à cela, encore faut-il que dans un même corps de techniques les empreintes digitales soient décrites de la même façon.

En matière d'empreintes digitales, je pense qu'il existe aujourd'hui un consensus sur l'usage des points caractéristiques. Sur l'iris, le problème est d'une autre nature, l'ensemble des techniques commercialisées repose sur les mêmes racines technologiques et l'interopérabilité devrait être préservée. Sur le visage, ce sera plus dur, l'une des solutions est de stocker l'image du visage plutôt que la description du visage. Voyez d'ailleurs l'orientation de l'OACI, c'était une réponse à la question.

Autre point important, les approches gouvernementales de critères communs en biométrie. C'est une réflexion conduite aujourd'hui par les USA, la Grande-Bretagne, l'Allemagne, le Canada, l'Italie, la Hollande, dont la France est quasi absente. Cela représente un risque certain de constitution d'une barrière technologique préjudiciable à l'industrie française et à l'image de crédibilité des titres émis par l'Etat français.

Il est important de souligner que le développement de l'industrie française de la carte à puce s'est appuyé sur une politique de certification reconnue et exigeante. Il serait souhaitable d'en tirer des enseignements aussi pour la biométrie.

4. L'usage intelligent de plusieurs biométries utilisées l'une après l'autre ou en combinaison va se développer. Plusieurs facteurs joueront. Aux Etats-Unis, de multiples acteurs ont des points de vue différents, certains sont pour le visage (Département d'Etat) et d'autres (Département Justice) n'envisagent pas d'utiliser autre chose que l'empreinte digitale et c'est non négociable. On peut penser que cette différence d'analyse se reproduira entre les Etats et chacun aura son point de vue.

Il est probable qu'on va se rendre compte que l'usage du visage est limité en termes de performances. Le visage pour sa part essaiera dans l'avenir de chercher une solution en termes d'efficacité à travers une gestion tridimensionnelle.

Dans le même temps, la crédibilité de l'iris devrait prendre corps. Cette technologie est jeune, mais crédible.

Il est tout aussi probable que ces deux dernières technologies, le visage et l'iris, essaieront d'entrer dans le marché du consommateur en profitant de l'essor des GSM et des PDA disposant déjà de caméras.

Sur un autre plan, les contraintes d'exploitation de vitesse, de taux de rejet, etc. militeront en faveur de l'usage en combinaison de la biométrie.

Pour ces raisons d'interopérabilité, de performance, il sera retenu plusieurs biométries au niveau mondial. La globalisation de l'usage devrait aussi se traduire par des exigences en matière d'architecture qui seront accessibles à très peu d'acteurs et seulement ceux qui maîtrisent totalement la chaîne biométrique.

5. Le concept d'identité régalienne devrait prendre corps, c'est le problème du titre fondateur. La valeur de l'identité sera reconnue au fil du temps. Etre identifié, c'est aussi être reconnu en tant que citoyen d'un Etat avec tout ce que cela comporte. C'est aussi poser la question de savoir qui protège et qui est responsable de son identité. En tant que citoyen, je pose la question.

Le schéma régalien de l'identité assuré par l'Etat pourrait devenir un socle fondateur et une identité gérée correctement une première fois pourrait éviter l'usage de questions multiples et variées des différentes administrations de l'Etat pour tâcher de retrouver une identité douteuse parce que le titre d'identité ne s'appuie pas sur des techniques efficaces.

6. En matière de liberté individuelle, le concept de biométrie à trace se diluera face aux évolutions technologiques ou aux usages. Il est probable que le corps de doctrines qui régit l'analyse de la CNIL aujourd'hui sera remis en cause avec les évolutions technologiques.

Il faut quand même retenir qu'avant 1900 il n'existait dans le monde pratiquement que des fichiers anthropométriques, le siècle dernier nous a apporté des fichiers d'empreintes, d'ADN, vocaux, de photos.

Je ne pense pas que cette évolution s'arrête. Il ne faut pas oublier que tous les fichiers ne sont pas seulement constitués à des fins de lutte contre la criminalité, ils servent également à identifier des victimes au cours d'attentats, des

amnésiques. Nous avons aidé la police de New York à identifier un nombre significatif de victimes du World Trade Center avec nos technologies.

Enfin, j'aurai quatre suggestions.

1. Il serait souhaitable que le gouvernement se dote des moyens permettant la mise en place d'une politique de certification biométrique et se coordonne rapidement avec les Etats européens qui ont engagé cette démarche.

2. Il serait judicieux que les acteurs en charge de la réflexion sur la biométrie soient clairement définis (je ne développe pas mais c'est très important) et engagent des discussions concrètes avec des industriels. Je fais écho à vos propos Monsieur le Président.

Il n'est pas trop tard pour conduire des expérimentations pilotes, notamment sur la délivrance des visas, afin de conforter l'analyse et de construire une expérience que d'autres Etats européens ont déjà engagée.

Nous sommes aujourd'hui avec deux Etats européens en opération pilote sur le contrôle des visas. Nous avons un poste de contrôle de visas multibiométrique au Ghana et un deuxième en cours d'installation au Sri Lanka pour deux pays européens.

3. Un projet d'extension à la biométrie du système d'information Schengen est un bon point de départ à un projet multi-Etats. Il doit être rapidement envisagé. Les instances multilatérales ont besoin d'un appui technique fort des différents pays et notamment de la France pour mener à terme de tels projets.

4. Face aux évolutions rapides de l'usage de la biométrie, l'analyse au cas par cas de la CNIL risque très rapidement de montrer ses faiblesses. Des textes régissant les conditions légales d'usage des informations biométriques seraient un bon garde-fou. Qui a le droit d'utiliser les informations biométriques qui ont été mises dans un boîtier biométrique pour un contrôle d'accès ? La police y a-t-elle accès et sous quelles conditions ?

En conclusion, les techniques biométriques existent, elles savent répondre aujourd'hui très rapidement à certaines classes de problèmes. Le véritable enjeu aujourd'hui est d'avoir une expression précise des besoins, mais ce n'est pas le cas. Il faut envisager les aspects légaux et les choix de société.

La biométrie, à bien des égards, est un outil stratégique de souveraineté. Il existe beaucoup d'analogies à ce titre avec la cryptographie. Aux Etats-Unis, ce sont les mêmes organisations gouvernementales qui influencent les orientations industrielles.

Alors que la France et donc l'Europe a su prendre une position de leader mondial dans ce domaine, sommes-nous prêts à assurer les risques éventuellement critiques d'une non-décision ou d'un non-usage alors que nous savons pertinemment que nous possédons les moyens de limiter de tels risques ?

M. LE PRESIDENT. - Merci de cette présentation qui a permis de situer l'état de l'art et un certain nombre d'interrogations pour lesquelles des éléments de réponse ont été apportés dans le cours de la discussion. La vigilance des autorités françaises est très vive sur ces différents points, je crois qu'on en a fait la démonstration.

Quand vous faisiez allusion à l'absence de représentants français, je pense qu'il s'agissait du *working group* britannique ?

M. DIDIER. – Je peux développer sans être trop technique ce que l'on appelle des critères communs. En fait, on s'intéresse, quand on regarde une fonction sécuritaire, à sa qualité, à la façon dont elle va se comporter. On regarde la boîte sécuritaire.

Prenons l'exemple de la carte à puce, c'est une fonction sécuritaire. On regardera quelles sont ses performances, si elle remplit bien sa fonction sécuritaire et la difficulté à la casser. On définira des profils, des niveaux de sécurité, on regardera si pour casser une carte à puce il suffit d'un tournevis ou s'il faut utiliser une machine dont la construction demandera six mois.

C'est une méthodologie qui définira un niveau de sécurité et qui deviendra un standard *de facto*. Par exemple, les cartes à puce bancaires sont déclarées de niveau EAL 4+.

C'est cette même démarche qui est en train d'être conduite par ces gouvernements qui vont définir des niveaux de sécurité qui feront que quand un Etat choisira, il saura quel est le niveau de sécurité mis en place.

Si n'importe qui peut lire vos passeports, si n'importe qui peut acheter un lecteur et s'arranger pour le faire passer pour un lecteur gouvernemental, il pourra lire des informations sensibles. Comment fera-t-on pour protéger le système de sécurité globalement ? Tous les Etats que je vous ai cités ont un groupe de travail qui définit ces standards de protection qui seront imposés ultérieurement.

M. LE PRESIDENT. - D'où la nécessité d'y être présent, comme les processus de certification sur lesquels travaillent de façon très acharnée les Américains.

Thalès va peut-être compléter ou apporter d'autres éléments d'information à ce qui vient d'être dit par Monsieur DIDIER…

M. Philippe KARNAUCH, Président Directeur Général de Thalès-Identification - Beaucoup de choses ont été dites, je vais plutôt procéder par complément, je suis d'accord sur beaucoup de points avec Monsieur DIDIER.

Je dirige Thalès Identification qui est une filiale à 100 % du groupe Thalès, spécialisée dans les systèmes d'émission de titres identitaires (permis de conduire, carte d'identité, passeport, visa, certaines cartes de sécurité sociale, etc.).

Je ne parlerai que du domaine biométrique dans le contexte des systèmes identitaires, des titres identitaires réglementaires.

L'authentification, qu'on appelle également le un contre un dans notre jargon, consiste à vérifier que je suis bien la personne que je prétends être. On va comparer l'élément biométrique que j'ai sur moi (mon empreinte, mon visage, mon iris) à un gabarit qui sera stocké quelque part : on m'authentifiera.

Avec l'identification, que l'on l'appelle « un contre N » dans notre jargon, *a priori* on ne sait pas qui je suis, je ne décline pas mon identité et on doit m'identifier. On prend un élément biométrique, l'empreinte par exemple, on va chercher dans la base les empreintes qui ressemblent au plus près à la mienne pour essayer de trouver qui je suis.

Sur des documents qui sont du plus grand intérêt à court terme, on parle dans le cas du passeport d'authentification du porteur à l'entrée ou à la sortie d'une frontière. Pour le visa, c'est la même chose.

Enfin, d'autres types de documents peuvent être une carte d'identité, un permis de conduire, une carte de sécurité sociale ou de prestations sociales. On peut citer l'exemple de l'Espagne avec sa carte TASS de prestations sociales qui est une carte à puce sécurisée physiquement avec une biométrie empreinte. Le but est d'authentifier les porteurs de carte donc les porteurs de droits car des enjeux financiers sont mis en œuvre.

Nous avons parlé d'authentification, c'est-à-dire entre le titre et son porteur, nous avons assez peu parlé de la procédure en amont qui permettra d'émettre le titre.

Dans la procédure d'émission, lors d'une première demande de titre, on doit venir avec des documents justificatifs qui seront et resteront indispensables. Si l'on doit mettre une biométrie dans le titre, il peut paraître souhaitable, dès l'étape de la demande de titre, afin d'éviter les usurpations d'identité qui sont une atteinte à la liberté de l'individu que je peux être, de faire une identification donc une recherche un contre N pour vérifier que le demandeur du titre n'a pas déjà un tel titre sous une autre identité.

Une fois ce processus franchi, on passe à l'autorisation de production du titre, à la production puis à la procédure de délivrance. Lors de cette procédure, lorsque le demandeur en personne viendra demander son titre, le titre sur lequel son gabarit biométrique aura été stocké, il devra là encore présenter son empreinte, son visage ou son iris pour faire un contrôle, pour s'assurer qu'on remet le titre au demandeur et non à une tierce personne.

Dans ce cas, on sécurise totalement la chaîne, on n'oublie pas un élément fondamental de sécurité qui est la fraude documentaire.

Ensuite, lorsqu'on a stocké les gabarits dans une base de données, en cas de renouvellement, la procédure pour le citoyen peut être accélérée puisqu'il suffit qu'il s'authentifie. Cela peut lui simplifier la vie.

Une fois le titre remis au porteur, il est en circulation, la chaîne se boucle en situation opérationnelle par les contrôles aux frontières, c'est de l'authentification ; cela peut être aussi de l'identification en un contre n, c'est-à-dire une petite base de données qui est celle des personnes recherchées aux frontières (terroristes, criminels, etc.).

Il n'en reste pas moins que même si ces techniques biométriques sont mises en œuvre - ce qui a mon sens est le seul véritable moyen de sécuriser totalement la chaîne - il conviendra de toujours garder à l'esprit que les pièces justificatives et la procédure associée devront rester sécurisées, et que cette sécurité devra continuer à être renforcée au fil des évolutions technologies disponibles sur le marché.

Ce genre de système totalement bouclé n'est pas un rêve. Je vais vous citer l'exemple de la Namibie où nous avons installé un système de permis de conduire, de taille relativement modeste. Ce système est appliqué de bout en bout. Il est intéressant de voir des pays lointains et « exotiques » se doter de ce genre de système complet.

Sur les techniques biométriques elles-mêmes, l'essentiel a été dit. Le visage est la plus ancienne biométrie du marché, le cerveau humain étant le plus bel ordinateur d'exécution d'algorithme biométrique, c'est utilisable partout. L'OACI nous amène vers cette voie de stocker l'image -et non pas un gabarit- dans une puce, de manière sécurisée. C'est bien un policier aux frontières qui va faire la reconnaissance.

Ceci dit, cela nécessitera une sécurité physique forte et même de plus en plus forte du document. La sécurité logique pourra être apportée par la puce ou par un code barre de décrypté mais la sécurité physique du document doit rester forte. Il ne faut pas oublier les contraintes opérationnelles. Tous les Etats ne vont pas se doter dans les deux ans à venir de lecteurs automatiques, de dispositifs de visualisation d'un passeport qui contient une puce, cela se fera à l'échelle planétaire mais cela demandera du temps pour des raisons budgétaires.

Cette sécurité physique de premier niveau doit être renforcée. Plus on donne de droits à un titre, quel qu'il soit, plus il faut le sécuriser physiquement car plus cela tentera les fraudeurs.

Les empreintes digitales sont aujourd'hui une technique éprouvée. Les outils automatiques sont très performants. C'est le meilleur rapport performance/coût sur le marché et c'est opérationnel immédiatement.

La contrainte d'opérationnalité à court terme telle qu'évoquée aussi bien par les Américains que les Français que lors de la réunion des ministres de l'Intérieur et de la Justice des membres du G8 laisse relativement peu de choix sur la technique

biométrique à utiliser en complément de la reconnaissance faciale. Là aussi, il faudra utiliser deux types de biométrie pour avoir un système efficacement bouclé. De plus, aujourd'hui, c'est la biométrie qui se prête le mieux à l'interopérabilité, les travaux avancent très vite en la matière.

Quant à l'iris, il n'y a pas de déploiement à grande échelle. C'est une technique *a priori* très prometteuse, mais avec des techniques d'enregistrement des données biométriques assez contraignantes et d'un coût très élevé.

Sur le plan réglementaire, finalement, nous avons un curseur à régler : quel degré de protection veut-on donner au citoyen et aux Etats démocratiques ?

Je pars du un contre un, l'authentification de la personne à une frontière. Si je monte un peu dans le niveau de base de données, lorsque j'ai une base de données dans laquelle je n'autorise que des contrôles d'authentification pour le renouvellement des titres, j'avance d'un cran. Ensuite, en montant un peu plus, j'ai du un contre une identification sur des petites bases pour la lutte contre la criminalité et le terrorisme, mais également pour identifier des personnes décédées. Au bout, j'ai le un contre l'ensemble de la population pour lutter efficacement contre l'usurpation d'identité.

C'est la finalité souhaitée qu'il faut déterminer, c'est un choix de sécurité politique, législatif ; cette finalité doit être déterminée et la proportionnalité s'appliquera en fonction de cette finalité.

L'authentification, c'est-à-dire le un contre un entre moi-même et le titre que je porte, est une tendance irréversible pour les documents de voyage, on ne reviendra pas en arrière, c'est parti. Ensuite, en fonction du degré de protection souhaité, de la taille des bases de données et des restrictions d'interconnexion, on aura probablement des restrictions d'accès et d'utilisation croissantes.

Ces contraintes réglementaires devront être adaptées en fonction de ce principe de proportionnalité, mais c'est d'abord la finalité qui doit être figée.

En la matière, la coopération entre les instances étatiques françaises gouvernementales, tous les services techniques des ministères concernés et les industriels doit être renforcée. C'est un point général et de culture française, il y a une sorte de tabou dans la discussion, dans l'échange d'informations entre instances gouvernementales françaises et industriels là où nos amis et néanmoins concurrents allemands ont des liens beaucoup plus resserrés.

Là aussi, j'appelle de mes vœux à une concertation plus étroite entre industriels et instances gouvernementales.

M. LE PRESIDENT. - Merci pour ces informations complémentaires.

M. PALLEZ. - Je voudrais réagir aux propos de Monsieur DIDIER sur la CNIL. Je trouve assez paradoxal de dire que face à une technique qui évolue sans arrêt, une loi serait mieux adaptée qu'une réponse au cas par cas d'une autorité

administrative à l'écoute des réalités. Franchement, je ne comprends pas très bien ce qui pourrait être l'objet d'une loi qui en quelque sorte interviendrait dans ce domaine si ce n'est pour dire que tout est permis.

Je serais intéressé de connaître le contenu de cette loi. Je trouve qu'il faut faire attention parce que si on se réfère à l'expérience de la signature électronique dans laquelle on s'est lancé dans une batterie de textes législatifs et réglementaires dans l'idée que cela allait libérer le marché, le résultat n'est pas très probant.

Bien que par culture je sois plutôt tourné vers le législatif, je serais quand même tenté de dire : « Soyons prudents avant de considérer qu'il faut une initiative législative pour débloquer les choses ! »

M. DIDIER. – Il faudrait réfléchir. En fait, il y a deux usages. Le risque, ce ne sont pas les sujets sur lesquels nous débattons, sur lesquels nous aboutirons forcément à un consensus, mais de retrouver de la biométrie à tout bout de champ dans les entreprises, chez les particuliers, etc.

Il y aurait peut-être à réfléchir à un garde-fou qui consisterait à dire que lorsqu'il y a un usage non souverain, l'information biométrique ne peut pas être utilisée -par la police par exemple.

C'est peut-être une approche angélique, mais il est clair qu'on trouvera de plus en plus de biométrie. On laisse des traces partout, mettre un garde-fou définitif au mauvais usage de cette information demande réflexion. Je ne sais pas si c'est faisable.

M. LE PRESIDENT. – Cela paraît difficile, c'est en marchant qu'on pourra apprécier davantage.

Je voulais poser une question sur la capacité de réaction, de réponse des procédures et de la doctrine. S'il s'avère dans deux ou trois ans que les procédures mises en œuvre sont de nature à freiner l'évolution du système ou à le rendre trop contre-productif ou trop laxiste, on pourra faire une appréciation assez rapide de la situation. Nous ne disposons pas actuellement du recul nécessaire.

Pour revenir aux aspects industriels, avez-vous d'autres questions à poser aux industriels ?

Pr. Franck LE PREVOST, Université Joseph Fourier, Grenoble – Je suis professeur à l'Université Joseph FOURIER, je m'intéresse aux questions de cryptographie, de signature électronique, etc…

J'ai une question concernant l'évaluation des technologies qui seront proposées. Vous avez parlé tout à l'heure de cryptologie, les techniques crypto ont été évaluées sur un plan très ouvert, c'est-à-dire des choses comme la signature électronique, les algorithmes de cryptage, etc. Les différents acteurs ont très librement ouvert et présenté les technologies.

On a pu juger sur pièce et la communauté internationale peut juger sur pièce. Qu'envisagez-vous sur le plan de la biométrie ?

A contrario, je citerai un autre exemple de technologie qui a été plutôt standardisée sur un plan fermé, par exemple les techniques de protection des disques compacts, notamment le Secur Digitel Music Initiative qui avait proposé un standard et un challenge dans des conditions assez rocambolesques, mais qui avait été cassé quand même.

Un autre exemple dernièrement, sur la protection contre la copie de compact discs, Jenifer LOPEZ, musique vendue à dix millions d'exemplaires par Sony, une protection contre la copie, il suffisait de passer un stylo feutre autour du compact disc pour lever cette protection.

Ce sont des exemples assez extrêmes mais avérés et qui ont été supportés par les industries très puissantes. Vous avez parlé de politique de certification, je comprends cette démarche, mais voyez-vous une évaluation ouverte des technologies ? Comment pourra-t-on dire que telle technique est mûre ou pas ? Comptez-vous associer des acteurs indépendants universitaires ?

M. DIDIER. – J'ai une réponse fermée et une réponse ouverte.

Depuis plusieurs années, nous évaluons toutes ces techniques, nous avons mis au point des méthodologies très efficaces, qui nous permettent de savoir quel est le niveau de performance des différents concurrents sur le marché et c'est intéressant, nos concurrents biométriques viennent se faire évaluer. Nous savons exactement quels progrès ont été faits en reconnaissance faciale et de l'iris.

Avant-hier nous avons annoncé un accord stratégique avec le leader mondial de la technologie de reconnaissance faciale. Voilà pour la réponse fermée.

Pour la réponse ouverte, il existe dans la communauté autour de la biométrie des « challenges » réguliers beaucoup plus difficiles que pour la cryptographie. Le matériau sur lequel nous travaillons est plus physique que mathématique.

Je veux dire que l'évaluation peut consister à évaluer des algorithmes, mais également un système en fonctionnement, c'est-à-dire que, dans la dernière étape, on va évaluer la difficulté à se servir du système et une erreur générée par un mauvais usage sera une erreur alors que dans la partie algorithmique où l'on aura des jeux d'essai, cette dimension n'apparaîtra pas.

Il existe des compétitions régulières où les différents compétiteurs présentent leurs algorithmes. C'est discutable parce qu'il faut faire attention à la définition des jeux d'essai, mais cela donne une bonne idée. Il existe un centre d'évaluation fédéral américain à San José.

Une tentative a été faite en France de mettre en place des centres d'évaluation biométrique par la communauté européenne et cela a échoué. A travers les critères communs, j'espère voir une récupération gouvernementale de la

méthodologie d'évaluation parce que les taux de performance y sont précisés, et je suppose que viendront des jeux d'essai qui iront avec.

M. KARNAUCH. - Dans toutes les méthodologies d'essais, il ne faut jamais oublier que la qualité de la prise de la donnée biométrique, ce que l'on appelle l'enregistrement, est un critère essentiel.

On peut avoir un algorithme fantastique, si la qualité de l'enregistrement est mauvaise, vous aurez un mauvais résultat. C'est un point essentiel qui doit être pris en compte dans les évaluations.

Pr Bernadette DORIZZI, Institut national des Télécommunications - Je suis professeur à l'Institut national des télécommunications qui fait partie du groupe des écoles des télécommunications qui regroupe la majorité des écoles françaises d'ingénieur et de management dans le domaine des télécommunications. Nous avons dans nos équipes plusieurs laboratoires spécialisés dans différentes techniques biométriques, aussi bien le visage que les empreintes, les signatures dynamiques, les formes de la main. Nous avons depuis plusieurs années une solide expérience dans ce domaine de la biométrie.

Il me semble que ce problème de l'évaluation est assez important au niveau de l'évaluation comparative. Il me semble fondamental qu'il puisse y avoir des campagnes conduites par des organismes tiers non impliqués de manière économique et industrielle, faites dans des conditions d'utilisation de type laboratoire où l'on testera des algorithmes ou des adéquations algorithmes/capteurs puisque ce domaine est particulier par rapport à la cryptographie, par rapport à cette difficulté de devoir adapter des capteurs et des algorithmes.

Bien sûr, il existe de telles compétitions, une a lieu en Italie sur les empreintes digitales. Il me semble qu'un travail dans ce sens sera nécessaire qui, à mon avis, devra se faire au niveau européen voire international.

On a pas mal parlé de multimodalité qui est un mot clef de la recherche en biométrie pour l'avenir. On a bien vu qu'aucune n'était satisfaisante. On se rend compte que les situations d'usage amènent à profiter de cette panoplie de modalités et les situations de performance aussi puisqu'il a été mentionné à juste titre qu'aucune modalité ne pourrait satisfaire toute une population sans amener des problèmes particuliers.

Par rapport à ces évaluations multimodalités, il n'existe rien à l'heure actuelle qui soit fait d'une manière transparente et centralisée.

M. LE PRESIDENT. – C'est bien un des problèmes que je soulèverai dans ce rapport. Au niveau des autorités, on parle de groupe d'experts, mais on ne sait pas dans quel cadre cela s'inscrit, sous quelle forme, sous quelle modalité et quels sont leurs référents.

D'où la nécessité d'avoir une structure au plan national qui puisse assurer la mise en commun des connaissances, faisant appel au milieu scientifique, à des

chercheurs et universitaires, ou à des écoles spécialisées pouvant apporter les éléments fondamentaux de recherche, les éléments d'évaluation, les préconisations et, en liaison étroite, avec les industriels.

Je ne demande pas la création d'un institut de la biométrie en France, mais une amorce de quelque chose. Il y a là une nécessité de plus en plus impérative compte tenu des décisions qui seront prises à très court terme et qui engageront ensuite, peut-être pas de manière irréversible bien que quand les systèmes seront arrêtés, quand les outils seront mis en œuvre, il y aura un caractère presque irréversible, d'où l'urgence à agir.

M. DIDIER. – Pour donner une importance de l'effort que cela peut représenter, quand le FBI a décidé de s'équiper d'un système de gestion d'empreintes digitales, cela portait à l'époque sur 35 millions de personnes (aujourd'hui 70 millions), ils voulaient s'assurer qu'ils retenaient la meilleure technologie. Ils ont donné 30 millions de dollars à trois groupes industriels pour mettre en place un système permettant au gouvernement d'évaluer la technologie.

Cela représente des efforts énormes et on aurait intérêt à les capitaliser au niveau de l'Europe, sinon tous les Etats se reposeront ces questions.

M. LE PRESIDENT. – J'espère que le rapport y contribuera assez largement et aura un effet incitateur.

M. ROBIN. - Pour rebondir sur la remarque de Philippe KARNAUCH et de Monsieur DIDIER, effectivement, on a besoin de contrôler les performances. Par rapport à la crypto, ce n'est pas tant la performance de l'algorithme qui est importante dans un système biométrique, mais la performance de toute la chaîne complète.

Même l'empreinte est très bien. S'il y a sur le marché vingt types de capteurs, un système peut être complètement mis à mal parce qu'on a utilisé le mauvais capteur à 200 F. Chaque brique dans le système est extrêmement importante.

Je suis d'accord également sur le fait qu'il faut évaluer, mais ces évaluations coûteront cher car elles demandent d'évaluer tout le système et pas seulement un algorithme sur un PC.

Il faut avoir des instances pour évaluer mais ne pas se tromper. Cela nécessitera des budgets. Quand j'entends que la DARPA et la SARPA commencent aux Etats-Unis à rentrer dans le jeu pour financer l'industrie américaine comme c'est fait au niveau militaire, il faut que la France et l'Europe se mettent en ordre de bataille.

M. LE PRESIDENT. – Nous participons à votre analyse, mais sur toute une série de questions stratégiques, nous observons depuis quelques mois ou quelques années une évolution très forte des Etats-Unis pour pousser à des sauts technologiques. Cela comporte tous les éléments de la chaîne, y compris les maillons faibles.

Dans le domaine de l'espace, on constate depuis deux ans que les crédits budgétaires de recherche pour l'espace militaire aux Etats-Unis sont passés d'un facteur 3 par rapport à l'ensemble des crédits européens à un facteur 30.

Cela apportera rapidement ses fruits. C'est le cas dans une série de domaines, c'est le concept de dominance totale qui est en route. Si nous ne sommes pas capables de réagir en bonne intelligence avec nos capacités intellectuelles, nos capacités industrielles et les décisions gouvernementales que nous avons à prendre, nous serons totalement laminés.

Peut-être pouvons-nous maintenant demander à Monsieur REGNIER de nous apporter la vue du ministère des Affaires étrangères.

M. Jacques REGNIER, Direction des Français à l'étranger et des étrangers en France, Ministère des affaires étrangères – Je suis conseiller technique auprès du Directeur. Je suis aussi conseiller de la délégation française auprès de l'OACI ainsi que chargé de la délégation française au sein du Comité technique Visa dans le cadre européen.

Je suppose que beaucoup de choses ont été dites en mon absence, ce n'est pas la peine de les résumer, je me contenterai de dire que je comprends nos industriels qui souvent reprochent aux représentants officiels de ne pas assez parler de leur savoir-faire. Ne pensez pas cela, il y a ce qui se passe autour des tables, mais beaucoup de choses se passent dans les couloirs. En matière de diplomatie, c'est surtout dans les couloirs qu'on arrive à avoir des décisions. Je ne voudrais pas que vous sortiez de cette salle en pensant que nous ne faisons rien pour vous.

M. REGNIER. –.Je vais vous parler de la façon dont, dans le cadre européen, nous allons aborder le problème du visa du futur. Il est évident que maintenant on ne peut plus parler de visa français mais de visa européen qui est l'autorisation de se présenter aux frontières extérieures de l'espace Schengen, c'est-à-dire des pays qui appliquent la convention de Schengen.

Qu'est-ce qu'un visa ? C'est cette autorisation de se présenter à une frontière qui doit être connue et matérialisée : d'une part, pour les intéressés qui doivent savoir ce à quoi ils ont droit, d'autre part, pour les autorités aux frontières ou la police pour les contrôles internes à l'espace Schengen.

Pour les intéressés, il est évident que la notification de leurs droits ne peut se faire que de façon visuelle, matérielle, lisible, sans accessoire extérieur.

Au niveau des autorités, il en va autrement. Certes, il faut prévoir que cette notification soit visuelle, mais on peut prévoir des systèmes plus sophistiqués et plus techniques, voire carrément virtuels.

Je passerai sur l'historique des visas, quand je suis arrivé dans ce ministère il y a vingt-trois ans, on en était encore au tampon encreur. Comme beaucoup d'Etats, nous sommes passés par l'étape de vignettes nationales autocollantes et nous avons maintenant une vignette Schengen unique pour tous les

pays qui appliquent la convention de Schengen. Ceci fait l'objet d'un cahier des charges unique mais il n'y a pas de fabrication centralisée, chaque vignette peut être fabriquée par chaque pays, et on peut constater certaines variantes au niveau des couleurs qui ne sont pas tout à fait identiques.

Des liens existent entre la personne et son passeport parce qu'il y a au moins dans le passeport un élément très important qui est celui de la photographie. Il est facile de constater que la personne qui présente un passeport est le bon porteur du document du titre de voyage. En revanche, il y avait une lacune en matière de visa, la vignette visa ne comportait comme information d'identification que le nom de la personne et le numéro du passeport sur lequel cette vignette devait être apposée. Il y avait une lacune, il n'y avait plus de rapport direct entre la personne et la vignette visa. Le seul moyen de faire cette jonction, c'était un lien biométrique.

Une première étape est franchie, la décision est prise dans le cadre de l'Union européenne : à partir de cette année, on imprimera la photo sur les vignettes visas.

Ceci n'est pas neutre en matière d'investissement, il faut des imprimantes jets d'encre couleur, des scanners pour prendre des photos. Quand pour le seul Etat français on délivre dans 230 consulats tous les visas à travers le monde, il est évident que l'investissement est conséquent.

Cet investissement est d'autant plus conséquent qu'il n'existe pas de service des visas Schengen à l'étranger et c'est bien dommage ; les Etats européens feraient beaucoup d'économies dans la mesure où nous pourrions mettre nos moyens en commun. Aujourd'hui, entre 2 000 et 3 000 consulats des pays Schengen délivrent des visas à l'étranger, les décisions qui seront prises en matière de biométrie contribueront peut-être à accélérer ce mouvement de regroupement.

La première étape, c'est le côté visible de l'iceberg, c'est-à-dire l'impression de la photo sur la vignette visa. Les Allemands ont déjà commencé dans un consulat. D'ici la fin de l'année, dès que l'Imprimerie nationale sera en mesure de nous livrer les nouvelles vignettes visa, nous pourrons les expérimenter dans les consulats, vraisemblablement à Genève qui a l'avantage d'être notre centre expérimental puisque toutes les nationalités se présentent à Genève. Ceci nous permettra de tester.

J'en reviens à un point développé tout à l'heure sur la qualité de l'élément biométrique. En l'occurrence, il s'agit d'une photo. Nous avons beaucoup de craintes sur la façon dont on va mémoriser et imprimer le visage des demandeurs.

Il est évident qu'on ne pourra pas toujours prendre des photos numériques en direct, on devra travailler sur des photos d'identité. Quand on voit dans certains pays la qualité des photomatons ou des photographes locaux, j'ai de grosses craintes qui sont partagées par l'OACI qui essaie de sortir, comme l'a fait le ministère de l'Intérieur pour les cartes d'identité, une palette de ce qu'il faut faire ou ne pas faire, mais il est évident que nous aurons de mauvaises surprises.

Pour la partie invisible, j'en avais déjà parlé il y a quatre ans lors d'un symposium en Allemagne, il s'agit de la puce à mémoire avec lecture sans contact.

En matière de visa, compte tenu de la décentralisation de sa fabrication et du fait qu'on n'est pas maître du document sur lequel est apposée la vignette visa, on est obligé de prévoir quelque chose de très souple et le plus sécurisé possible. On s'oriente donc sur un élément biométrique, des données classiques relatives au visa et au passeport seront stockées dans une puce à lecture sans contact. Ce sera la principale orientation.

Pour ce qui est de la nature des éléments qui seront pris en compte, nous connaissons l'orientation de l'OACI, je pense que des décisions seront prises le 22 mai lors du prochain conseil pour mettre en place une procédure évitant le vote par pays avec consultation écrite, ce qui nous ferait gagner six mois. Ce serait une bonne chose.

L'orientation de l'OACI est une mémorisation de la photo ainsi que d'un autre élément biométrique, le choix étant ouvert pour les pays entre l'empreinte digitale et l'iris.

J'ajouterai sur l'iris, évoqué au cours de la réunion de la semaine dernière, que c'est un problème de culture : cela a un côté traumatisant pour les gens parce qu'il n'est pas évident de mettre sa tête devant l'appareil. Il est plus simple de mettre le doigt sur un autre appareil qui est beaucoup plus petit, on ne se sent pas agressé. Mais surtout, actuellement, il existe un brevet unique tenu par une seule société. Pour une fois, l'OACI a eu une bonne réaction qui a été de ne pas retenir cette solution. L'iris a été écarté notamment à cause de cet aspect.

Je reviens sur les éléments biométriques qui seront retenus vraisemblablement. Le premier est la photo. Il s'est posé le problème du second élément biométrique. Il est évident que la France a maintenu le choix de l'empreinte digitale, le ministre de l'Intérieur a déjà annoncé la chose.

Ces éléments, images de l'empreinte et de la photo, seront mémorisés à terme dans cette puce. Aucune décision n'a été prise dans le cadre européen, nous en sommes au stade des réflexions. Compte tenu des enjeux économiques qui sont derrière, toute la diplomatie ne pourra jamais remplacer le fait que, malgré tout, chaque pays soutient ses industriels. Il est donc évident qu'il y aura des discussions très serrées.

De toute façon, on s'appuie sur les recommandations de l'OACI : photos, empreintes digitales, mémorisation de puces sans contact. Ce sont les trois grandes décisions prises la semaine dernière. Pour une fois nous étions en avance par rapport à ces décisions.

Nous sommes en train de régler le problème de la vérification de l'authentification, c'est du contrôle de un par un, c'est-à-dire un visa/une personne. De la même façon que l'année dernière avait été prise la décision d'un passeport/une

personne. Cela évitera certaines embrouilles et certains trafics, notamment au niveau des enfants. Les choses seront plus claires.

On parle de l'identification de un à un parce que c'est une décentralisation de la fabrication, de l'identification de cette vignette visa. Il y a un éclatement total au niveau des contrôles à l'entrée du territoire Schengen, il faut donc que le visa soit un élément permettant d'authentifier une personne.

La puce à lecture sans contact permettra, avec le stockage de ces informations biométriques, de faire du contrôle de un à un, un peu n'importe où parce que la police peut avoir un PDA avec lecteur intégré : on pose le passeport dessus, on lit le visa et on voit la tête de la personne interpellée, on peut déjà savoir que c'est bien la bonne personne.

Un deuxième problème a été annoncé au G8, c'est la constitution d'une base de données informatique européenne des visas délivrés et refusés.

En France, depuis une quinzaine d'années, nous avons mis en place le Réseau Mondial Visa qui nous permet d'avoir une centralisation en France de tous les visas délivrés dans tous nos consulats à travers le monde. Nous sommes le seul pays à avoir cette possibilité à l'heure actuelle. Il n'empêche que la décision sera prise, je pense qu'il y aura un problème financier très important à régler dans le cadre de l'Union européenne : comment pourrons-nous financer la Lituanie, l'Estonie sur ce genre de technique ?

D'autres pays qui se disent plus avancés ont beaucoup de carences en la matière, ils devront investir très gros en matière d'informatique et de réseau. Tout cela pour vous dire que nous sommes les précurseurs, au moins en Europe, sinon dans le monde, en matière de Réseau Mondial Visa.

La décision va quasiment être prise de constituer une base de données communautaire qui s'appelle VIS (Visa information system), qui reprendra l'architecture technique du SIS.

Cela veut dire que tous les consulats des pays qui appliquent la convention de Schengen devront alimenter cette base de données de tous les visas. En moyenne, on estime qu'entre 15 et 20 millions de visas par an vont être délivrés à partir du moment où nous serons 27 pays qui appliqueront la convention de Schengen.

Compte tenu du fait qu'un visa de circulation peut durer cinq ans, vous voyez la dimension de cette base de données et tout ceci pour l'instant est fait sans aucun financement. Il est donc évident que ceci mettra un certain temps pour la mise en place d'un tel système.

C'est pourquoi, dans le cadre du Comité technique Visa, je fais tout pour accélérer au moins la première phase qui est celle d'un visa électronique avec mémorisation dans une puce sans contact d'éléments biométriques et de data de façon que certains contrôles puissent être effectués.

M. LE PRESIDENT. - Merci pour cette présentation complémentaire de ce qui a été l'objet d'éléments de discussion avec le représentant du ministère de l'Intérieur. Avec l'élargissement de l'Europe, des problèmes supplémentaires vont se poser par rapport à ceux que nous connaissons déjà, raison de plus pour avoir un système clef en main à leur proposer et qu'ils prennent les systèmes français ou européens.

Pr CABANIS. – Votre exposé, Monsieur REGNIER, était d'une clarté parfaite et je vous en remercie vivement car vous avez soulevé une autre question qui me brûle les lèvres depuis plus d'une heure, qui est celle de passer de la donnée biométrique et son fichier à un ensemble de données, c'est-à-dire à un dossier. C'est la question que je voulais poser à messieurs les industriels, quand passe-t-on de la donnée et d'une structure de fichiers organisée à une base de données d'un paramètre à N paramètres, c'est-à-dire N pour un ?

Par ailleurs, lorsque j'ai entendu de votre bouche dire que le système de vision de l'iris était un système breveté et totalement spécialisé chez un industriel, je voudrais juste corriger cette donnée en disant qu'il y a en France 8 000 ophtalmologistes qui voient des iris et qui les photographient tous les jours.

Ces systèmes sont aujourd'hui des systèmes d'ophtalmoscopie directe que chacun d'entre nous peut observer si nous sommes examinés par un ophtalmologiste, et ces systèmes aujourd'hui sont numérisés. Le scanning laser ophtalmoscope notamment permet d'avoir une extraordinaire approche de l'iris comme du fond d'œil comme de la cornée.

Il y a peut-être une notion de compréhension d'un petit logiciel ajouté à cette numérisation du segment antérieur. A-t-on besoin d'un appareil spécialisé pour photographier le visage des gens ? Cette question est de la même nature. Profondément, je ne le crois pas, je crois que l'essentiel est d'avoir une représentation photographique numérisée du visage et d'avoir une représentation numérisée de l'iris en mydriase ou en myosis simplement avec un système d'agrandissement qui est l'appareil d'examen clinique de tous les ophtalmologistes du monde aujourd'hui.

Je ne saisis pas très bien. Pourquoi ajouter deux ou trois données de référence ou de quantification ? Nous les avons par définition sur les systèmes numériques.

M. LE PRESIDENT. - Je crois que malheureusement un brevet a été pris.

M. DIDIER. – Deux brevets fondamentaux ont été déposés pour la technologie dont nous parlons. Aujourd'hui encore, une quarantaine de brevets sont détenus par cette société qui est le produit de la fusion de sociétés qui travaillaient sur l'iris.

Le brevet israélien qui va tomber dans le domaine public, cette année ou l'année prochaine, dit que l'iris est unique. En fait, il a breveté la notion d'unicité,

c’est-à-dire ce qui permet d’identifier une personne à partir de certaines informations contenues dans l'iris.

Un deuxième brevet porte sur l'usage de certaines transformations algorithmiques, déposé par Daugman qui a breveté une approche efficace.

Autour de ce corps de brevets, il y a des brevets d'application qui vont proposer différentes façons de lire un iris. Aujourd'hui, je ne suis pas inquiet sur les évolutions en matière de confort d’acquisition d’iris, on pourra l’acquérir de façon de plus en plus confortable, ce qui était un des freins à l’usage de cette technologie.

M. LE PRESIDENT. - Je donne la parole à Madame DORIZZI qui va nous faire une petite synthèse de ce débat, étant entendu que les contributions qui n'ont pas été totalement présentées seront utilisées pour le rapport.

Mme DORIZZI. - Cette matinée a été extrêmement riche en contributions diverses qui ont eu aussi pour effet de se renforcer les unes les autres, voire d'augmenter leur impact.

Nous pouvons retenir un certain nombre de points comme ces techniques biométriques qui se trouvent aujourd'hui à une période un peu historique due au contexte politique et sans doute un peu économique, et qui amènent à se poser de manière urgente des questions qui étaient latentes.

C'est tout ce domaine qui a été largement évoqué ce matin de l'utilisation de la biométrie pour des applications de type protection de la société comme on a pu le voir au niveau des visas, des passeports et de la sécurisation au niveau des immigrations, qui correspond à un besoin nouveau auquel on voit apparaître des solutions déjà opérationnelles.

C'est la démonstration que ce secteur a déjà, au niveau de la recherche et des développements menés ces dernières années, puisque ce n'est pas un domaine récent, permis de proposer des solutions à des problèmes concrets qui se posent aujourd’hui de manière urgente.

Il ne faut pas cacher le fait qu'il reste derrière des questions et des recherches à mener pour l'avenir qui, à mon avis, devront être conduites en évitant ce syndrome français de la répartition entre laboratoires, industrie et recherche académique qui se fait dans les laboratoires

On a beaucoup parlé d'algorithmes, derrière les techniques biométriques se trouvent des recherches algorithmiques. On a beaucoup parlé des visages, c’est certainement la modalité dans laquelle on attendait le plus encore des avancées nouvelles en termes de nouveaux algorithmes, de nouveaux apports.

On a parlé du fait qu’on allait stocker l'image du visage et non pas des caractéristiques extraites parce que, pour l’instant, il n’y a pas de consensus autour d'une caractéristique qui représenterait un visage.

Cela traduit bien l'état de la recherche aujourd'hui et le fait qu'il y a du travail derrière pour fiabiliser ces systèmes, pour fiabiliser les systèmes en lien avec des capteurs. C'est une des caractéristiques de ce domaine. On doit fiabiliser aussi une chaîne entière de traitement, on est devant quelque chose qui amène à des questions nouvelles et à une recherche active à mener.

On a aussi beaucoup évoqué les aspects standardisation normative, c'est un challenge très important pour les aspects interopérabilités et développement, en particulier sur des échelles européennes ou internationales. Cela paraît quelque chose d'important où la France a sa place à prendre par rapport à des organismes qui sont en marche.

On l'a vu dans la matinée, ce qui rend si passionnant cette thématique de la biométrie, c'est un travail de recherche et de développement pluridisciplinaire. On touche aussi bien la médecine et le corps humain que les aspects législation. On n'a pas tellement évoqué ce matin les aspects sociologiques et psychologiques qui sont extrêmement importants dans l'essor, en particulier au niveau commercial et du grand public. Je crois que nous sommes dans une discipline qui a cette richesse de toucher toutes les composantes de l'homme, ses capacités de réfléchir, de produire de nouveaux algorithmes, de nouvelles techniques très poussées au niveau scientifique jusqu'à tout ce qui touche au corps humain et à tous les réflexes psychosociologiques, législatifs qui sont derrière.

Je pense que nous vivons une expérience extrêmement passionnante en réunissant dans cette salle des gens d'origines diverses et c'est cette richesse qui va nous conduire à un développement très important de la biométrie dans l'avenir.

Merci encore.

M. LE PRESIDENT. - Merci pour cette synthèse qui est plus un rapport d'étape qu'une conclusion définitive puisque le sujet est encore en devenir et en devenir extrêmement rapide. L'Office assure aussi un suivi des études qui sont faites. Dans mes conclusions et recommandations, vous avez compris implicitement que je proposerai qu'il y ait un espace de rencontre au plan national qui puisse piloter l'ensemble des partenaires y compris au plan européen. Nous avons pu aujourd'hui lister la plupart d'entre eux.

Nous ne pouvions pas aborder les aspects psychologiques et sociologiques, et Dieu sait s'ils sont importants, puisqu'il a été fait mention des Asiatiques et de leur réserve vis-à-vis de telle ou telle technique. J'ai découvert des choses passionnantes à cette occasion.

Nous aurons l'occasion assez rapidement de retrouver la plupart des acteurs ici présents et d'autres pour définir une « organisation » à mettre en place vis-à-vis de cette question, car les incidences sont énormes.

Sans que je sois mobilisé sans arrêt par les questions économiques, on a trop considéré par le passé en France cet aspect des choses avec un certain dédain et comme n'étant pas noble. Je crains malheureusement que d'autres en profitent. Il

convient que nous inversions notre approche de ces questions et que nos préoccupations soient très matérialistes de temps en temps.

Je remercie tous les participants qui ont aujourd'hui contribué à cette audition. J'abrège parce que certains m'ont dit que, compte tenu des difficultés de transport, ils souhaitaient terminer relativement tôt. Je souhaite à tous ceux qui rejoignent d'autres rendez-vous bonne chance dans les transports.

Pr CABANIS. – Partageant l'enthousiasme de Madame DORIZZI, j'aimerais saluer l'Office parlementaire pour cette extraordinaire initiative et profiter pour qualifier notre président d'un mot dans cette transversalité de l'approche scientifique, technique, industrielle et juridique en le remerciant car il s'est comporté en humaniste.

La séance est levée à 12h55.

Annexe 3

Biométrie et médecine légale

Cahiers d'Anthropologie et Biométrie Humaine (Paris)
1995 - XIII, n° 1-2, p. 49-57

BIOMETRIE ET MEDECINE LEGALE

BIOMETRY AND FORENSIC MEDICINE

Y. DELOISON[1], D. LECOMTE, JP. CAMPANA

RESUME

Les techniques anthropométriques sont appliquées en médecine légale à l'identification d'un sujet. Cinq questions principales se posent au médecin légiste ou à l'anthropologue devant des restes osseux plus ou moins complets :
1) S'agit-il de restes humains ou animaux ?

Dans le cas où il y a identification humaine :
2) Quelle est l'origine géographique du ou des sujets ?
3) A quel sexe appartiennent ces éléments ?
4) A quelle dimension peut-on évaluer la stature ?
5) Quel âge pouvait avoir le sujet lors de son décès ?

Un exemple illustre l'application de ces méthodes : il s'agit de la reconnaissance du squelette de DUGUAY-TROUIN par L. DEROBERT et Ch. PIEDELIEVRE effectuée en 1973 lors du tricentenaire de la mort du célèbre corsaire.

SUMMARY

In forensic medicine, the technics of anthropology are applied as help to a subject's identification. Four main questions are put relative to more or less complete human remains :
1) Are they animal or human remains ?
2) What is the geographicorigin of the subject ?
3) What is the sexe of the person ?
4) What is his stature ?
5) How old was he when he is dead ?

An exemple explains these methods : the verification of the Duguay-Trouin's skeleton by L.DEROBERT and Ch.PIEDELIEVRE made in 1973 at that birthday of the death of the famous corsair.

Mots-clés : sexe, âge, stature, crâne, bassin.

Key-words : sex, age, stature, skull, pelvis.

[1] Musée de L'Homme - Laboratoire d'Anthropologie - Paris.

INTRODUCTION

Si la biométrie peut se définir comme l'ensemble des techniques de mesure des êtres vivants et des méthodes statistiques de traitement des mensurations, la médecine légale quant à elle, fut définie en 1830 par ORFILA comme représentant l'ensemble des connaissances médicales propres à éclairer diverses questions de droit, à diriger les législateurs dans la composition des lois.

La médecine légale n'est pas une science exacte, elle est essentiellement empirique et pragmatique. L'autopsie tend à déterminer les causes de la mort ; les techniques biométriques et plus précisément anthropométriques sont utilisées pour identifier des restes plus ou moins complets. (Nous donnons ici un résumé des techniques utilisées, pour plus de détails, voir C.SIMONIN, 1955 ou L. DEROBERT,1974).

DEVELOPPEMENT DU SUJET

Lorsque le médecin légiste est confronté à des restes fragmentaires, il doit s'assurer dans un **premier temps** qu'il s'agit bien de restes humains et non animaux.

En présence d'un os complet, l'ostéologie comparée permettra d'en retrouver l'origine.

Une méthode histologique sera utilisée s'il s'agit de fragments osseux. Elle est fondée sur les différences existant entre les diamètres des canaux de Havers constituant l'architecture des os ; ainsi chez l'Homme, il est admis que le diamètre moyen des canaux de Havers est compris entre 30 et 150 µ alors que chez les animaux, il est inférieur à 100 µ. A la mesure de ce diamètre, on peut ajouter la numération des canaux qui est de 8 par mm^2 chez l'Homme et supérieur à 13 chez les animaux. De plus, l'étude de l'architecture osseuse apporte des renseignements notamment pour déterminer l'âge d'un sujet comme on le verra plus loin.

Enfin, une méthode sérologique peut être appliquée. Elle repose sur la formation d'anti-sérum humain. En mélangeant in vitro du sang ou de l'albumine d'origine humaine au sang d'un lapin préinjecté, l'anti-sérum produit un précipité blanchâtre visible à l'oeil nu.

La **deuxième question** qui se pose porte sur la détermination de l'origine géographique. Une réponse sera recherchée en tenant compte des indices calculés à partir des mesures relevées soit sur la tête entière soit sur le crâne.

Nous noterons ici essentiellement cinq indices :

- l'indice céphalique ou horizontal : $\dfrac{\text{Diamètre transverse maximal}}{\text{Diamètre antéro-postérieur maximal}} \times 100$

- l'indice vertical : $\dfrac{\text{Hauteur du crâne}}{\text{Diamètre antéro-postérieur}} \times 100$

- l'indice de largeur : $\dfrac{\text{Hauteur du crâne}}{\text{Diamètre transverse maximal}} \times 100$

- l'indice facial supérieur : $\frac{\text{Hauteur nasion point alvéolaire}}{\text{Diamètre bizygomatique maximal}} \times 100$

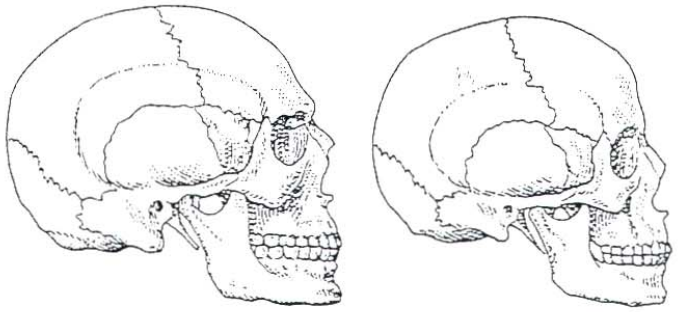
- l'indice nasal : $\frac{\text{Largeur nasale maximale}}{\text{Hauteur nasale}} \times 100$

Enfin, le prognathisme sera évalué selon des angles variés.

Du fait du déplacement de plus en plus grand des populations, la détermination de l'origine géographique est délicate et facilement entachée d'erreur.

La troisième question que se pose le médecin légiste porte sur la détermination du sexe qui se fera à partir de caractères observés à la fois sur le crâne et sur le bassin, s'il a la chance de posséder ces deux pièces.

En effet, d'une façon générale, un crâne masculin présente par rapport à un crâne féminin : un front plus fuyant, des bosses sourcilières et une glabelle plus saillantes par rapport à la racine du nez, une articulation fronto-nasale anguleuse, des rebords orbitaires épais, des apophyses mastoïdes proéminentes (Fig.1), un crâne lourd. Tous ces caractères sont aussi à considérer non pas seuls mais comparés au groupe si le squelette n'est pas isolé.

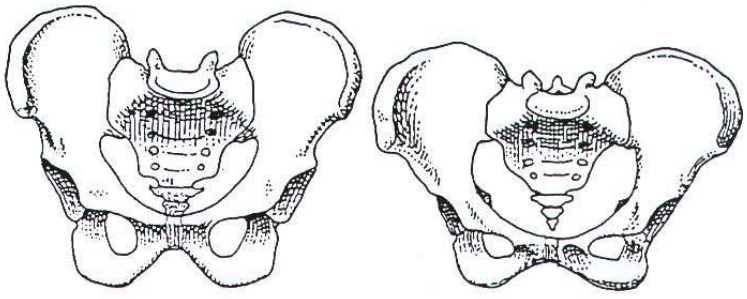


CRANE D'HOMME. CRANE DE FEMME.

Fig. 1 - Différences entre le crâne féminin et le crâne masculin (C. SIMONIN, 1967)

La détermination du sexe sera un peu facilitée si le bassin est présent parmi les restes. D'une façon générale, on observe sur le bassin, la grande échancrure sciatique dont le grand axe est orienté vers le bas chez l'Homme et vers l'horizontale chez la Femme ; l'angle sous pubien aigüe chez l'Homme et large sur le bassin féminin ; la prédominance des valeurs verticales chez l'Homme et des valeurs horizontales chez la Femme ; enfin, les ailes iliaques d'un bassin de Femme sont plus ouvertes et plus minces que chez l'Homme (Fig.2).

Toutefois il faut savoir qu'aucun caractère pris isolément n'a de valeur absolue ; c'est le groupement des signes et leur convergence qui permettent de décider.



BASSIN D'HOMME. BASSIN DE FEMME.

Fig. 2 - Différences entre un bassin féminin et un bassin masculin (C.SIMONIN, 1967)

La **quatrième question** posée concerne la détermination de la stature du sujet.

Si le squelette est complet, il est facile d'en mesurer sa stature en tenant compte du fait qu'un sujet couché, c'est à dire en decubitus dorsal, est plus grand de 16 à 30 mm par rapport à sa taille debout.

Il existe une corrélation entre la longueur des os longs et la stature. Différentes tables ont été établies (C.SIMONIN, 1955). Les tables de ROLLET et MANOUVRIER ont été établies pour des populations européennes ; celles de TROTTER et GLEISER sont surtout utilisées aux Etats Unis.

Si l'on dispose uniquement d'os longs : fémur, tibia, humérus, radius, fibula ou cubitus, les méthodes classiques de corrélation entre la taille et la longueur des os longs peuvent être utilisées.

Si l'on dispose d'un ou plusieurs os longs du membre inférieur : fémur, tibia ou de vertèbres ; les méthodes modernes de FULLY-PINEAU, qui utilisent des coefficients permettent le calcul de la stature avec une exactitude satisfaisante.
Formules de PINEAU et FULLY :
Stature = 2,09 (fémur+5 lombaires) + 42,67 + k 2,35
Stature = 2,32 (tibia+5 lombaires) +48,63 + k 2,54

La **cinquième question** auquelle doit répondre le médecin légiste et qui n'est pas la moins importante est représentée par l'évaluation de l'âge du sujet.

S'il s'agit d'un enfant, donc d'un sujet âgé de moins de vingt ans, ce sont les points d'ossification primitifs ou secondaires qui servent de référence.

Dans le cas d'un sujet adulte, sept caractères principaux peuvent être étudiés :

1) - L'aspect de la facette articulaire ostéo-cartilagineuse des côtes qui a été classée en quatre stades (C.SIMONIN, 1967) :
Stade I à 20 ans, surface plane ondulée.
Stade II à 30 ans, surface concave.
Stade III à 40 ans, surface creuse.
Stade IV à 57 ans, surface résorbée.

2) - L'aspect de la symphyse pubienne, classée en quatre stades selon le plus ou moins grand relief des crêtes osseuses : I, 18 ans ; II, 26 ans ; III, 45 ans ; IV, 50 ans.

3) - En pratique, lorsque cela est possible, l'ossification du sternum est facile à observer (Fig.3) :
Stade I à 23 ans il est formé en quatre pièces.
Stade II à 30 ans il est formé en trois pièces.
Stade III à 49 ans il y a ossification complète en une seule pièce.
Stade IV à 57 ans il y a ossification du cartilage sterno-claviculaire.

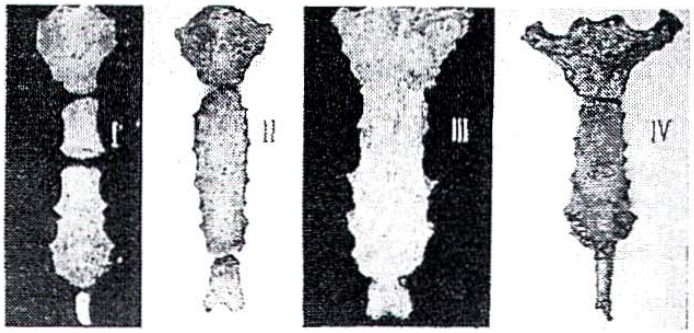


Fig. 3 - Age du sternum (C. SIMONIN, 1967)

4) - L'ossification du sacrum peut être observée mais elle est difficile à évaluée.

5) - Le remaniement de l'achitecture des os au cours de la vie est un bon critère ; elle est classée en quatre stades :
Stade I 20 ans , architecture dense.
Stade II 35 ans, architecture réticulo-spongieuse.
Stade III 46 ans, discontinuité des travées osseuses, progression du canal médullaire vers l'épiphyse.
Stade IV 57 ans, architecture cavitaire ; disparition des travées et envahissement de l'épiphyse par le canal médullaire.

6) - Quand le crâne était présent, il était tenu compte de l'état des synostoses de la voûte cranienne, mais il y a une grande variabilité dans l'âge de la soudure de ces sutures ; en effet, cet âge varie non seulement avec le sexe mais aussi l'alimentation et les conditions de l'environnement. Il ne représente donc pas un bon critère.

7) - Enfin, les dents peuvent servir à déterminer l'âge. Chez un enfant, on tient compte de leur ordre d'apparition. Cette connaissance est utile depuis le 65 ème jour de vie intra-utérine jusqu'à une vingtaine d'années. A l'âge adulte deux méthodes sont connues : celle de GUSTAFSON et celle de LAMENDIN qui tend à remplacer la précédente.

La méthode de GUSTAFSON détermine six caractères ; pour les connaître elle nécessite de détruire une dent alors que celle de LAMENDIN (Fig.4), plus simple, ne recherche que deux caractères : la translucidité et le degré de parodontose, c'est à dire le déchaussement. Elle permet de déterminer l'âge du sujet avec un risque d'erreur de trois ans environ, ce qui représente une bonne

précision. Elle présente aussi l'avantage d'être d'application rapide. En voici ses principales formules :

$$\text{Translucidité } T = \frac{\text{Hauteur de translucidité}}{\text{Hauteur de la racine}} \times 100$$

$$\text{Parodontose } P = \frac{\text{Hauteur de parodontose}}{\text{Hauteur de la racine}} \times 100$$

Age estimé en années $A = (0{,}18 \times P) - (0{,}42 \times T) + 25{,}53$

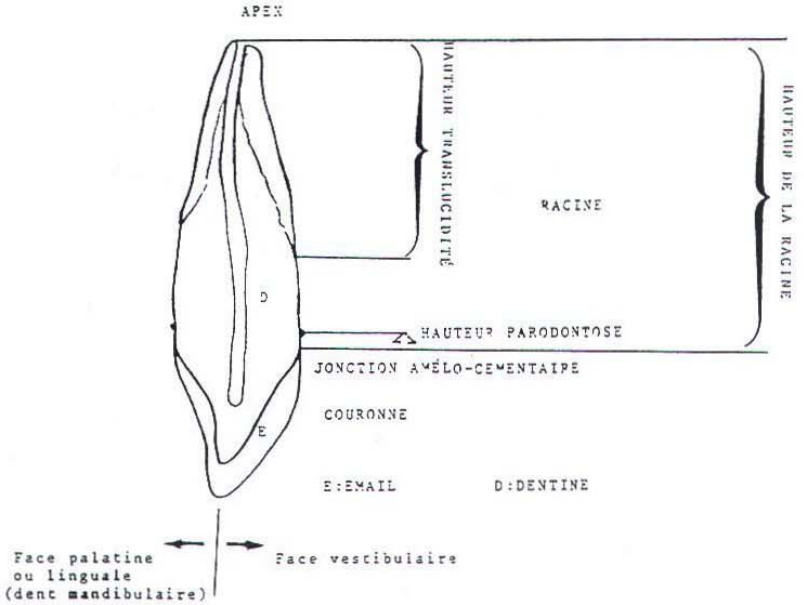


Fig. 4 - Méthode de LAMENDIN

UN EXEMPLE D'APPLICATION DE CES TECHNIQUES

En 1973, le Professeur L.DEROBERT et le Docteur Ch.PIEDELIEVRE furent chargés par le Comité du Tricentenaire de DUGUAY-TROUIN d'identifier et d'individualiser le squelette du corsaire au milieu d'autres squelettes mis au jour dans la crypte de la chapelle de la Vierge en l'église Saint Roch à Paris.

DUGUAY-TROUIN est né à Saint Malo le 10 juin 1673 et mort à Paris le 28 septembre 1736. Un acte légal authentifiait son inhumation dans la crypte de l'église Saint Roch.

Des fouilles furent alors entreprises pour dégager l'ensemble des squelettes de cette crypte, celle-ci ayant servi d'ossuaire. Ayant atteint le niveau où l'on pensait que devait se situer le squelette du célèbre marin, trois squelettes furent trouvés d'un côté et six d'un autre. Ces squelettes furent numérotés de 1 à 9. Parmi ces restes, cinq squelettes, les numéros 4, 5, 6, 7 et 8, furent attribués à des sujets féminins et donc écartés de la recherche. Les squelettes restants, 1, 2, 3 et 9 furent étudiés plus en détail.

Le crâne et le bassin du sujet n°1 furent effectivement attribués à un homme. Sa stature évaluée à environ 1 mètre 70. L'état de son crâne qui présentait de nombreuses synostoses associé à l'état de ses os lui firent attribuer un âge de soixante plus ou moins trois ans.Une particularité de ce crâne est constituée par une nette asymétrie au niveau de l'arcade zygomatique gauche qui lui donne une pommette gauche plus renflée que la droite (Fig.5).

Le crâne et le bassin du sujet n°2 furent aussi attribués à un sujet de sexe masculin, sa stature évaluée à 1 mètre 72 et son âge à cinquante quatre ans environ. Ce squelette présentait moins d'ostéoporose que les sujets n°1 et 9.

Pour le sujet n°3, le crâne était absent mais l'anatomie de son bassin permit de l'attribuer à un sujet masculin. Sa stature fut évaluée à 1 mètre 68 et son âge estimé à environ cinquante ans.

Quant au sujet n°9, il fut reconnu masculin par l'étude de son crâne et de son os iliaque ; sa stature estimée à 1 mètre 70 plus ou moins deux centimètres. Une nette ostéoporose de senescence le faisant apparaître plus âgé que le sujet n°1, il lui fut attribué un âge de soixante cinq ans plus ou moins trois ans.

Les sujets 2 et 3 furent éliminés à cause de leur âge considéré comme un peu trop jeune par rapport à soixante trois ans, âge de la mort de DUGUAY-TROUIN.

Il restait à choisir entre les sujets 1 et 9. On s'intéressa, alors, à la disymétrie faciale du sujet n°1. Des portraits de DUGUAY-TROUIN furent recherchés et réunis ; parmi ceux-ci, une gravure exécutée d'après nature par OZANNE fut retenue. En effet, sur ce dessin la joue gauche apparaît plus gonflée que la joue droite (Fig.6). Des photos furent prisent des deux crânes n°1 (Fig.7) et n°9 suivant le même angle et la même dimension que la gravure puis chacune des photographies fut superposée avec la gravure. Des similitudes apparurent entre le crâne 1 (Fig.8) et la gravure mais aucune entre le crâne 9 et le portait fait par OZANNE. Les deux médecins légistes conclurent : "Bien qu'aucune preuve médico-légale ne puisse être établie, il existe un ensemble de probabilités et de similitudes qui font penser raisonnablement que le squelette étendu le long du mur nord-ouest de la crypte, la tête orientée vers l'est (squelette n°1) est celui de DUGUAY-TROUIN." (L.DEROBERT et Ch.PIEDELIEVRE, 1973).

Cette réponse ne donna pas satisfaction complète à ceux qui avaient demandé cette recherche ; ils désiraient une affirmation sans réserves, ce qui eut pour conséquence la poursuite in situ des recherches. Et c'est ainsi, que fut découverte devant les os des pieds du squelette n°1 à quelques centimètres de profondeur une plaque en cuivre gravée au nom de : DUGUAY-TROUIN.

La preuve était donc apportée que le squelette n°1 était bien celui de : DUGUAY-TROUIN.

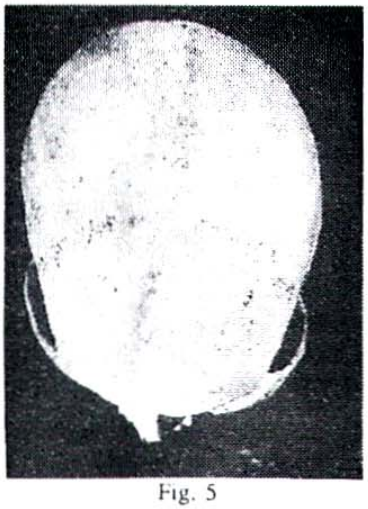


Fig. 5

Fig. 6

Fig. 5 - Vue supérieure du crâne n°1 montrant la projection en avant des régions orbitraire et zygo-manddibulaire gauches.

Fig. 6 - Gravure d'OZANNE ayant servi à l'étude des similitudes avec le crâne n°1

Fig. 7

Fig. 8

Fig. 7 - Crâne du squelette n°1 placé en léger oblique antérieur droit comme le visage de la gravure d'OZANNE

Fig. 8 - Superposition photographique, harmonieuse, du crâne n°1 et du portrait gravé par OZANNE, ramenés à la même echelle

BIBLIOGRAPHIE

DEROBERT, L., 1974, Médecine légale, Flammarion Médecine-Sciences, 1198 pages.

DEROBERT, L. et PIEDELIEVRE, Ch., 1973, Identification du squelette de René DUGUAY-TROUIN, Rapport Médico-Légal .

DEROBERT, L. et PIEDELIEVRE, Ch., 1974, Etude et identification du squelette de René DUGUAY-TROUIN, Lecture faite à l'Académie Nationale de Médecine, le 12 novembre 1974.

SIMONIN, C., 1955 et 1967, Médecine Légale Judiciaire, Librairie MALOINE, Paris, 1054 pages.

Nous tenons à remercier le Dr C.PIEDELIEVRE, M.J.J.DELEMARLE, M. LAMENDIN et le service photographique du Musée de la Marine pour le pret de leurs documents qui nous ont permis de réaliser cet article.

Ce travail a été effectué avec les crédits du CNRS.

Annexe 4

Avis rendus par la CNIL sur le recours aux techniques biométriques

AVIS RENDUS PAR LA CNIL SUR LE RECOURS AUX TECHNIQUES BIOMETRIQUES

Type de Biométrie	Déclarant	Finalité	Nature de l'impératif de sécurité justifiant, selon la CNIL, le recours aux biométries	Position CNIL	Matériel et prestataire technique	Modalités de stockage des gabarits biométriques	Observations particulières de la CNIL
EMPREINTE DIGITALE	Banque de France	Contrôle d'accès des agents	Zones hautement sécurisées (Sécurisation des comptoirs)	Avis favorable n° 97-044 du 10 juin 1997	Sas à unicité de passage équipé d'un appareil « fingerscan » (IDENTIX)	Base de données centralisée	
	Collège Jean Rostand de Nice	Contrôle des accès à la cantine scolaire, gestion des comptes et facturation	Néant	Avis défavorable n°00-015 du 21 mars 2000	Technologie SAGE (boîtiers « morphotouch » de la SAGEM), installée par la société PROFABEL	Base de données centralisée	La constitution d'une base de données biométriques est apparue à la Commission excessive au regard de la finalité poursuivie
	Cité académique de Lille	Contrôle d'accès de certains personnels de l'Education Nationale à certains locaux	Confidentialité des sujets d'examens et concours notamment	Avis favorable n° 00-056 du 16 novembre 2000 DA 709756	Technologie SAGE - BIOTIME (boîtiers « morphotouch »de la SAGEM), installée par la société PROFABEL SEMLEX	Base de données centralisée	
	Préfecture de l'Hérault	Contrôle des temps de travail des agents de la préfecture	Néant	Avis défavorable n° 00-057 des 26 octobre et 16 novembre 2000	Lecteurs badge + biométrie Société Advanced cards systems HORO-QUARTZ	Base de données centralisée	La constitution d'une base de données d'empreintes digitales n'est apparue à la Commission ni adaptée ni proportionnée à l'objectif poursuivi

Type de Biométrie	Déclarant	Finalité	Nature de l'impératif de sécurité justifiant, selon la CNIL, le recours aux biométries	Position CNIL	Matériel et prestataire technique	Modalités de stockage des gabarits biométriques	Observations particulières de la CNIL.
EMPREINTE DIGITALE	COGEMA La Hague	Contrôle d'accès	Zones sensibles (bâtiments de stockage du plutonium)	Examen en séance plénière des 26 .10 et 16.11.2000 Récépissé du 17 novembre 2000 (DO n°624427)	Sas avec lecteur biométrique et PC pour saisie du n° du badge personnel Société GET	Base de données centralisée	
	United Airlines	Gestion des horaires des salariés	Néant	Examen en séance plénière des 26.10 et 16.11.2000 (DO 719326)	Traitement BIOTIME (*cf. supra* cité académique de Lille), installée par la société SEMLEX	*Cf. supra* cité académique de Lille	- projet considéré par la Commission comme excessif et disproportionné au regard des finalités poursuivies - abandonné en nov. 2000 (opposition du personnel)
	Groupement Carte Bleue	Contrôle d'accès	Sécurisation de l'accès aux zones de fabrication	récépissé du 25 avril 2001 (DO 728996)	Fingerscan V20 de IDENTIX	Base de données centralisée Carte à puce envisagée à terme	
	SAGEM	Contrôle d'accès	Sécurisation de l'accès aux zones de fabrication de cartes à puce	récépissé du 25 avril 2001 (DO 746724)	SAGEM	Base de données centralisée	
	Mairie de Mérignac	vote électronique à partir de cartes à microprocesseurs comportant les empreintes digitales des électeurs	Sincérité du scrutin	Avis favorable n°02-015 du 14 mars 2002	Aquitaine Europe Communication et France Telecom	Enregistrement des gabarits uniquement sur les cartes à puce détenues par les seuls électeurs (pas de base de données centralisée)	Expérimentation à l'occasion des élections présidentielles et législatives de 2002

Type de Biométrie	Déclarant	Finalité	Nature de l'impératif de sécurité justifiant, selon la CNIL, le recours aux biométries	Position CNIL	Matériel et prestataire technique	Modalités de stockage des gabarits biométriques	Observations particulières de la CNIL
EMPREINTE DIGITALE	Mairie de Goussainville (DA 798267)	Contrôle des horaires	Néant	Avis défavorable (02-033 du 23 avril 2002)	ZALIX 10 Finger pass Société MBB GELMA	Base de données centralisée	Saisine syndicat CFTC à l'origine de la déclaration
	Aéroports de Paris (DA 799468)	Contrôle des accès des personnels d'ADP et des services publics ou des entreprises intervenant en zones réservées sûreté	Sécurisation des « zones réservées sûreté » (ZRS) des aéroports de Roissy et d'Orly	Avis favorable (02-034 du 23 avril 2002)	SAGEM Morphoaccess ou Morphotouch pour l'empreinte digitale	Durant l'expérimentation : stockage sur une base de données centralisée A terme : stockage sur carte à puce	Utilisation à titre expérimental (six mois) et sur la base du volontariat Bilan demandé à l'issue de l'expérimentation
	SAGEM SA (DO 769366)	Contrôle des accès / Vitrine commerciale	Activités classées « secret défense » et « secret OTAN »	Récépissé du 13 mai 2002	Morphoaccess MA 300 et Morphoaccess MA 200 / Installateur CEGELEC	Base de données centralisée	Utilisation sur la base du volontariat s'agissant de l'accès au bâtiment et obligatoire s'agissant de l'accès aux trois étages sensibles
	URSSAF de la Corse (DA 797265)	Contrôle des accès	Actes de terrorisme récemment commis	Avis défavorable (02-045 du 18 juin 2002)	Fingerscan V20 UA de la société IDENTIX	Base de données centralisée	L'accès biométrique est couplé à l'accès par badge existant Suite à AD, dossier présenté avec biométrie contour de la main (avis tacite du 5 octobre 2002, DA 815421)

Type de Biométrie	Déclarant	Finalité	Nature de l'impératif de sécurité justifiant, selon la CNIL, le recours aux biométries	Position CNIL	Matériel et prestataire technique	Observations particulières de la CNIL
CONTOUR DE LA MAIN	Musée du Louvre	Contrôle des accès et des horaires de certains personnels	Protection des œuvres d'art	Avis favorable n°01-006 du 25 janvier 2001	RECOGNITION SYSTEM (image de la main en 3D)	Rapport BOUCHET du 25 janvier 2001 : « l'avis favorable de la Commission à la mise en œuvre d'un système de contrôle d'accès utilisant le contour de la main aurait l'avantage de fixer un début de doctrine de la CNIL sur le sujet, en acceptant la technique biométrique recourant au contour de la main et en reléguant l'utilisation des empreintes digitales à des cas très spécifiques de sécurité »
	Société DEVINLEC	Contrôle d'accès	Bijouterie	DO n°730005 récépissé du 12 février 2001	RECOGNITION SYSTEM (image de la main en 3D)	Soumis à l'appréciation de la Commission le 25 janvier2001
	Association Ajaccienne d'Aide aux Handicapés	Contrôle des horaires	Néant	DO n°727691 récépissé du 12 février 2001	Contour de la main capté par une caméra	Soumis à l'appréciation de la Commission le 25 janvier 2001
	Aéroports de Paris (DA 799468)	Contrôle des accès des personnels d'ADP et des services publics ou des entreprises intervenant en zones réservées sûreté	Sécurisation des « zones réservées sûreté » (ZRS) des aéroports de Roissy et d'Orly	Avis favorable (02-034 du 23 avril 2002)	Durant l'expérimentation : stockage sur une base de données centralisée A terme : stockage sur carte à puce	Utilisation à titre expérimental (six mois) et sur la base du volontariat Bilan demandé à l'issue de l'expérimentation

Type de Biométrie	Déclarant	Finalité	Nature de l'impératif de sécurité justifiant, selon la CNIL, le recours aux biométries	Position CNIL	Matériel et prestataire technique	Observations particulières de la CNIL
CONTOUR DE LA MAIN	Espace Expansion - Centre commercial Les Quatre Temps (DO 784379)	Contrôle des horaires des salariés des sociétés prestataires de services	Néant	Récépissé délivré le 13 mai 2002	ZALIX 50 Handkey II RECOGNITION SYSTEM IncGabarits stockés sur les trois lecteurs installés Procédé choisi en raison de son moindre coût par rapport aux empreintes digitales / couplage avec la composition d'un code sur le clavier de l'appareil	Soumis à l'appréciation de la Commission le 23 avril 2002
	Collège Joliot-Curie de Carqueiranne (DA 814268)	Contrôle des accès au restaurant scolaire	Néant	Avis favorable (02-070 du 15 octobre 2002)		La Commission a pris acte qu'un système alternatif de carte à code-barre est mis en œuvre pour les personnes ne souhaitant pas utiliser la technique biométrique

Type de Biométrie	Déclarant	Finalité	Nature de l'impératif de sécurité justifiant, selon la CNIL, le recours aux biométries	Position CNIL	Matériel et prestataire technique	Observations particulières de la CNIL
IRIS	Aéroports de Paris (DA 799468)	Contrôle des accès des personnels d'ADP et des services publics ou des entreprises intervenant en zones réservées sûreté	Sécurisation des « zones réservées sûreté » (ZRS) des aéroports de Roissy et d'Orly	Avis favorable (02-034 du 23 avril 2002)	Durant l'expérimentation : stockage sur une base de données centralisée A terme : stockage sur carte à puce	Utilisation à titre expérimental (six mois) et sur la base du volontariat Bilan demandé à l'issue de l'expérimentation

AUTRES DOCUMENTS CNIL CONCERNANT LA BIOMETRIE :

1986 Rapport CANONGE
« DIX ANS D'INFORMATIQUE ET LIBERTES »
Délibération FNAED
Délibération OFPRA 1987
Rapport Banque de France
Rapport CNIL « Voix, image et protection des données personnelles »
Rapport annuel d'activité 2000 : « Les contrôles d'accès par biométrie »
Etude Interne CNIL du 14 décembre 2001: Les techniques Biométriques. (Direction expertise et contrôles)
Communication sur les Biométries - décembre 2001 - (Support Powerpoint – YLH)
Rapport d'ensemble SN
Rapport d'activité 2001
Communication en séance plénière du 10 décembre 2002 concernant l'expérimentation d'Air France dans le cadre des vols vers Tel Aviv (DO 829550) : le gabarit de l'empreinte digitale du passager est stocké sur la piste magnétique de la carte d'accès à bord

Annexe 5

La biométrie au Québec

Les principes d'application pour un choix éclairé

Commission d'accès à l'information
Juillet 2002

Présentation

L'actuel document présente, à titre indicatif, des principes d'application en matière de biométrie au Québec. Les principes découlent d'un premier examen des effets combinés de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (L.R.Q., c. A-2.1) (Loi sur l'accès), de la *Loi sur la protection des renseignements personnels dans le secteur privé* (L.R.Q., c. P-39.1) (Loi sur le secteur privé) et de la *Loi concernant le cadre juridique des technologies de l'information* (L.Q. 2001, c. 32) (Loi sur les technologies de l'information).

Ni limitatifs ni exhaustifs, les principes d'application sont émis dans le seul but de vous informer pour un choix éclairé.

Vous envisagez d'utiliser la biométrie au sein de votre organisation. Voici donc une série de questions qui vous guidera pour évaluer si votre projet se conforme aux lois.

❑ Principes d'application

Principe 1
Les alternatives à la biométrie

La Loi sur les technologies de l'information prévoit que nul ne peut exiger la vérification ou la confirmation de l'identité d'une personne au moyen de la biométrie, sauf par un consentement explicite obtenu de la personne concernée.

Avez-vous envisagé une alternative à la biométrie ?

Quel mode alternatif à la biométrie est offert aux personnes qui ne veulent pas utiliser ce type de technologie ?

De quelle façon prévoyez-vous l'exercice du libre choix par une personne de ne pas utiliser la biométrie en milieu de travail ?

Principe 2
Le caractère indispensable des renseignements recueillis

Tout organisme public qui désire utiliser la biométrie doit s'assurer que les données biométriques personnelles et autres renseignements personnels recueillis sont nécessaires à ses attributions ou à la mise en œuvre d'un programme dont il a la gestion. Dans le secteur privé, les renseignements recueillis doivent être nécessaires à l'objet du dossier constitué.

La nécessité signifie que les renseignements recueillis sont indispensables. L'obtention d'un consentement à la collecte est subordonnée à cette exigence de nécessité.

En plus de la nécessité, la Loi sur les technologies de l'information exige qu'on limite la collecte de données biométriques au minimum de caractéristiques ou de mesures permettant de relier une personne à l'action qu'elle pose.

Le caractère indispensable de la collecte de données que vous projetez peut-il être démontré ? Comment ?

Les fins visées par la collecte peuvent-elles être atteintes sans l'obtention de ces renseignements ?

Comment vous assurer de réduire au minimum la quantité d'informations biométriques à recueillir ?

Avez-vous réalisé une analyse rigoureuse des risques inhérents à la technologie que vous projetez utiliser et des risques associés à l'utilisation que vous désirez faire de cette technologie? Pour l'entreprise ou l'organisme qui veut installer la technologie? Pour les futurs utilisateurs de cette même technologie ? Par exemple, si vous décidez de recourir à l'utilisation de mesures d'empreintes digitales; avez-vous pris en compte les risques particuliers que présente cette technologie au regard de la vie privée?

Quelles raisons justifient la collecte de renseignements personnels ?

D'autres renseignements personnels sont-ils recueillis afin d'atteindre la finalité recherchée ?

Principe 3
La collecte auprès de la personne concernée

La Loi sur les technologies de l'information exige que les caractéristiques ou mesures biométriques ne puissent être saisies sans que la personne concernée n'en ait connaissance. Des données biométriques ne peuvent donc être recueillies à l'insu de cette personne.

Comment vous assurer que les données sont recueillies auprès de la personne concernée ?

Comment valider l'identité de la personne au moment de la cueillette de données biométriques ?

Comment vous assurer que la personne concernée a pleinement connaissance que des données biométriques sont mesurées sur sa personne et quelles sont ces données lors de la vérification d'identité (enrôlement) ? ... ultérieurement lors de la confirmation de son identité ?

Principe 4
Le consentement à l'utilisation de la biométrie

La Loi sur les technologies de l'information exige le consentement explicite de la personne, afin que la vérification ou la confirmation de son identité soit faite au moyen d'un procédé permettant de saisir des caractéristiques ou des mesures biométriques. Le consentement explicite doit porter uniquement sur la collecte de données biométriques et doit être écrit, libre, éclairé, spécifique et limité dans le temps.

Considérant les risques reliés à l'utilisation de la biométrie (par exemple : de vol permanent d'identité, de sécurité reliée à la centralisation des bases de données, de sécurité des réseaux, de discrimination des personnes, de piratage des technologies, des limites de la technologie utilisée, etc), quelle forme donnerez-vous au consentement à requérir des personnes concernées ?

Validez-vous l'identité de la personne auprès de qui vous sollicitez un consentement? Comment ?

Vous assurez-vous que le consentement envisagé répond aux qualités décrites plus haut ? Comment ?

Informez-vous la personne concernée de l'ensemble des risques connus associés ou inhérents au système et à la technologie biométriques utilisés afin que son consentement soit éclairé ? Comment ?

Quel mécanisme avez-vous envisagé afin que les personnes refusant l'utilisation de la biométrie ne subissent aucune pression et aucun inconvénient ?

Informez-vous la personne de la durée de conservation et du moment de destruction des caractéristiques ou mesures biométriques qui font l'objet de la cueillette ? Comment ?

Décrivez-vous à la personne concernée l'ensemble des mesures et des caractéristiques saisies de même que tout autre renseignement qui pourrait être découvert à partir de celles-ci ? Comment ?

Principe 5
La conservation et la sécurité des données biométriques

La collecte des données biométriques doit être entourée de multiples précautions compte tenu des risques qu'elle induit. Des modalités particulières s'imposent lors de l'entreposage de ce type de renseignement sensible qui exige une attention particulière et des mesures de sécurité adaptées. La Commission considère que toutes les données biométriques et celles y étant associées doivent être chiffrées.

Toute banque de données de mesures ou de caractéristiques biométriques constituée en vertu de la Loi sur les technologies de l'information et, le cas échéant, de la Loi sur l'accès doit être préalablement divulguée à la Commission d'accès à l'information.

Avez-vous privilégié les solutions où l'utilisateur détient ses mesures biométriques sur un support portable (chiffré et sécurisé) sous son contrôle ?

Si vous désirez créer une banque de données biométriques, avez-vous divulgué préalablement votre intention à la Commission d'accès à l'information ? Avez-vous aussi divulgué l'existence d'une telle banque, qu'elle soit en service ou non ?

Lorsqu'une banque de données biométriques est constituée, avez-vous prévu recourir au chiffrement de toutes les données contenues ou en lien avec cette banque durant sa conservation? Lors de la prise de copies de sauvegarde et pour les besoins de relève? Lorsque ces données circulent ou transitent sur tout réseau (ou sur plusieurs réseaux), que ce réseau soit public ou privé et interne ou externe ?

Quelles sont les autres mesures de sécurité qui protégeront les données biométriques et assureront la sécurité et la confidentialité de ces données ?

Le degré de sécurité offert par l'utilisation de la biométrie est-il proportionnel à ce qu'exigent les fins recherchées ?

Vous assurez-vous que les caractéristiques ou mesures biométriques contenues dans une banque de données ne peuvent être accédées que par le biais d'une application contenue dans un système ? Comment ?

Avez-vous prévu de journaliser tout les accès aux données biométriques ? Même pour le personnel informatique ?

Principe 6
L'utilisation des données biométriques

La Loi sur les technologies de l'information précise que tout autre renseignement concernant une personne qui pourrait être découvert à partir des caractéristiques ou mesures biométriques saisies ne peut servir à fonder une décision à son égard ni être utilisé à quelque autre fin que ce soit.

Vous assurez-vous que l'utilisation de la biométrie ne peut permettre de révéler des caractéristiques sur la santé, l'état mental et l'état physique et tout autre renseignement sur une personne ? Comment ?

Vous assurez-vous que les renseignements découverts à partir de données biométriques ne peuvent servir à fonder une décision à l'égard de la personne concernée ni être utilisés à une autre fin ? Comment ?

Principe 7
La communication de données biométriques

Une donnée biométrique demeure confidentielle tant que la personne concernée n'a pas consenti à sa divulgation. Ainsi, la communication de données biométriques exige le consentement écrit de la personne concernée.

La Loi sur les technologies de l'information prévoit une particularité en regard des renseignements découverts à partir des données biométriques. Ces renseignements ne peuvent être communiqués qu'à la personne concernée et seulement à sa demande.

Quelles sont les communications de données biométriques prévues ?

Vous assurez-vous que toutes les communications seront autorisées par un consentement écrit de la personne concernée ? Comment ?

Quelle sera la forme du consentement ?

Vous assurez-vous que le receveur répond aux exigences de nécessité lorsque lui sont transmises (avec consentement) des données biométriques ? Comment ?

Principe 8
La destruction de données biométriques

La Loi sur les technologies de l'information prévoit que les données biométriques de même que toutes les notes les concernant doivent être détruites lorsque l'objet qui fonde la vérification ou la confirmation d'identité est accompli ou que le motif qui la justifie n'existe plus. Cette obligation rend impérative la destruction d'une donnée biométrique lorsque ces conditions sont satisfaites. La conservation de ce type de données pour une plus longue période est donc illégale.

Quels mécanismes vous permettent de savoir que l'objet de la vérification ou la confirmation d'identité sont accomplis ou que le motif qui la justifie n'existe plus ?

Vous assurez-vous que les données biométriques sont immédiatement détruites dans ces conditions ? Comment ?

Quels mécanismes utilisez-vous pour détruire de façon irréversible toutes les copies existantes de données biométriques ?

Principe 9
Les droits d'accès et de rectification

Le droit d'accès et de rectification par la personne concernée prévu dans les Loi sur l'accès et Loi sur le secteur privé est maintenu à l'égard des renseignements personnels et des données biométriques. Les données biométriques détenues doivent donc pouvoir être communiquées de façon intelligible pour quiconque souhaite exercer son droit d'accès et de rectification.

Une personne peut-elle accéder à ses données biométriques ? Comment ?

Une personne peut-elle accéder aux données découvertes à partir de ses données biométriques ? Comment ?

Les données peuvent-elles lui être communiquées de façon intelligible ? Si oui, par quel mécanisme ?

Une personne peut-elle exercer son droit à la rectification ? Comment ?

Annexe 6

Conseil JAI du 27 février 2003 Déclaration commune franco-allemande sur l'utilisation de la biométrie

Les Etats membres de l'Union européenne ont déjà manifesté leur intérêt pour l'utilisation des techniques biométriques en vue d'améliorer les normes de sécurité concernant les documents de voyage. Celles-ci permettent de lutter efficacement contre la fraude documentaire et contre l'utilisation de ces documents à des fins d'immigration irrégulière mais aussi à des fins criminelles et terroristes. Compte tenu de l'ampleur de ces menaces, il faut mettre à profit les progrès technologiques dans ce domaine pour améliorer l'authentification des documents de voyage (passeports, visas et titres de séjour) et pour organiser des contrôles fiables et rapides aux frontières extérieures et à l'intérieur du pays. C'est là un enjeu essentiel pour l'ensemble des Etats membres, dans un espace commun de justice, de sécurité et de liberté.

Depuis les attentats du 11 septembre 2001, la possibilité d'introduire des données biométriques dans les documents d'identité et de voyage a été discutée dans plusieurs instances internationales, et notamment l'Organisation de l'aviation civile internationale (OACI), le G8, et les groupes de travail de la Communauté Européenne. Il est nécessaire d'introduire des normes d'utilisation de la biométrie reconnues au niveau international. Il est d'abord indispensable que les Etats membres de l'Union européenne parviennent à harmoniser entre eux les modes d'utilisation de ces données biométriques pour les documents de voyage, les titres de séjour et les visas.

A cette fin, la France et l'Allemagne demandent que le Conseil confie à la Commission le soin de préparer l'adaptation des instruments juridiques qui s'y rapportent et sont actuellement en vigueur, à savoir :

- pour les visas de courte durée, le règlement du 29 mars 1995 N° 1683/95, relatif à l'élaboration uniforme de visas,
- pour le modèle uniforme de titre de séjour, le règlement du 13 juin 2002 N° 1030/2002, relatif à l'élaboration uniforme d'un titre de séjour pour les ressortissants de pays tiers

Concernant la sécurisation des passeports et des autres documents de voyage, les Etats membres examineront les conditions de modification de la résolution du Conseil du 17 octobre 2000 (2000/C 310/01), en vue de parvenir à une harmonisation des nonnes ainsi que des techniques de production et de sécurisation des données. Ces règles pourraient également s'appliquer aux cartes d'identité qui peuvent être utilisées comme documents de voyage par les ressortissants communautaires ou en fonction d'accords particuliers par des ressortissants d'Etats tiers.

Les modifications des textes visés définiront à terme la ou les données biométriques retenues en complément de la photo d'identité, parmi les techniques déjà identifiées par l'OACI la reconnaissance faciale, l'iris de l'œil et les empreintes digitales et le cas échéant la géométrie palmaire ou d'autres techniques qui feraient leurs preuves.

Elles définiront les conditions générales d'utilisation de stockage, d'accès aux données intégrées dans les documents, par les services de contrôles aux frontières et les services de police des Etats membres.

Une phase transitoire pour la mise en œuvre de ces dispositions sera prévue par les textes visés.

Le cadre juridique commun ainsi créé permettra aux Etats membres d'intégrer les données biométriques à introduire dans les titres qu'ils délivrent, en tenant compte de principes qui auront été ainsi posés. Chaque Etat membre devra ainsi effectuer le choix des données biométriques, du moyen de stockage et du système de lecture de ces données en fonction des positions communes définies au niveau communautaire, afin que ces techniques soient parfaitement interopérables dans tous les Etats membres. Seule une harmonisation des procédés devrait garantir l'utilisation effective et efficace des données biométriques des Etats membres.

Ces fondements juridiques communs pour l'utilisation de la biométrie devront être conformes aux règles relatives à la protection des données personnelles et plus précisément à la Charte des Droits de l'Homme ainsi qu'à la directive européenne du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation des données.

Sur la base de ces normes définies au niveau communautaire, les Etats membres devront, au sein des instances internationales dont les recommandations valables au niveau mondial sont en cours d'élaboration, adopter une position commune solide et être capables de s'opposer à la fixation unilatérale de normes biométriques par d'autres pays.

Dans le même temps, il est nécessaire que les Etats membres mettent en place à court terme une coopération technique renforcée, afin d'évaluer de manière utile leurs connaissances sur l'utilisation et l'évolution des différents procédés biométriques et de disposer d'une expertise commune indépendante et de qualité. A ces fins, ils pourront échanger les résultats des tests déjà réalisés par certains d'entre eux afin que l'exploitation des résultats obtenus soit la plus large et la plus enrichissante possible. Pour ce faire, tous les Etats membres devraient participer de façon intensive au forum européen sur les documents de voyage mis en place l'année dernière. Dans le cadre de cette coopération technique, des expérimentations à grande échelle pourraient par ailleurs être réalisées grâce à un financement communautaire.