N° 938

ASSEMBLÉE NATIONALE

CONSTITUTION DU 4 OCTOBRE 1958

DOUZIÈME LÉGISLATURE

Enregistré à la présidence de l'Assemblée nationale
Le 16 juin 2003

N° 355

SÉNAT

SESSION ORDINAIRE DE 2002 - 2003

Annexe au procès-verbal
de la séance du 12 juin 2003

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

RAPPORT (2ème 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
par M. Claude BIRRAUX,
Président de l'Office

Déposé sur le Bureau du Sénat
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

DEUXIEME PARTIE :

Sortir des atermoiements actuels : la nécessité de définir rapidement un cadre juridique adapté

Les techniques d'identification des personnes à partir des données biométriques offrent d'ores et déjà d'importantes facilités dans le domaine de l'identification judiciaire qui est actuellement le secteur où ces techniques sont le plus largement implantées.

Les progrès qu'elles ne manqueront pas d'enregistrer et qui permettront à la fois de renforcer la fiabilité des outils, de rendre plus aisée leur utilisation, de diminuer les coûts et d'assurer la compatibilité des différents systèmes, comme le souci des pouvoirs publics et des acteurs privés d'accroître l'efficacité et la sécurité des dispositifs qu'ils mettent en œuvre conduiront inévitablement à un développement de ces techniques.

Or, si actuellement les règles juridiques qui encadrent l'utilisation des techniques biométriques apportent de nombreuses garanties, de multiples incertitudes, plus d'ailleurs que les garanties offertes par le cadre juridique en vigueur, constituent un obstacle à leur déploiement.

Les divers acteurs politiques et économiques ne peuvent pourtant se satisfaire d'une gestion au coup par coup qui n'offre aucune « visibilité », ni n'assure le niveau minimum de transparence nécessaire à la définition d'une politique qui soit ouvertement débattue et maîtrisée par les citoyens et décidée par leurs représentants, d'autant que les principales évolutions concernent aujourd'hui des questions qui dépassent largement le cadre strictement national.

Après avoir examiné les garanties et incertitudes juridiques relatives à l'utilisation des systèmes biométriques, il conviendra donc d'analyser les évolutions perceptibles à l'échelle européenne et au niveau international.

I - Garanties et incertitudes juridiques relatives à l'utilisation des systèmes biométriques

L'utilisation des systèmes biométriques soulève au regard des règles de droit applicables deux interrogations fondamentales.

L'une concerne les conditions juridiques dans lesquelles de tels systèmes peuvent être implantés. A quelles conditions peut-on collecter, traiter et échanger des données biométriques ? Sur ce point, un certain consensus s'est dégagé : l'utilisation des systèmes biométriques doit obéir aux règles garantissant la protection des données personnelles et de la vie privée. Mais si un tel principe est communément admis, demeurent diverses incertitudes qu'il convient de recenser et qu'il faudra bien lever.

L'autre interrogation porte sur les conséquences juridiques d'une utilisation des systèmes biométriques. Il s'agit de la question de la valeur probante d'une donnée biométrique à laquelle il est actuellement très difficile de répondre, eu égard à la fois à la complexité des dispositifs juridiques, même si l'on se limite à un cadre national, et aux caractéristiques scientifiques et techniques des systèmes biométriques. Cette question appelle une réflexion qui dépasse le champ des compétences de l'Office parlementaire d'évaluation des choix scientifiques et technologiques, mais mérite cependant d'être abordée, même si aucune solution ne peut être raisonnablement présentée à l'heure actuelle.

1 - Les conditions juridiques d'une utilisation des systèmes biométriques : protection des données personnelles et de la vie privée

Pour aborder correctement cette question, il convient de distinguer trois domaines, même s'ils entretiennent entre eux, sur le plan juridique mais aussi pratique, des rapports plus ou moins étroits.

Le premier recoupe peu ou prou celui de l'identification judiciaire : il s'agit du domaine touchant à la sécurité publique, la défense et la sûreté de l'Etat, selon les termes habituellement employés par les lois régissant la protection des données personnelles qui comportent des dispositions spécifiques applicables à ce domaine particulier. Le second se définit naturellement par rapport au premier et

porte sur les traitements qui ne sont pas mis en œuvre à des fins de sécurité publique, de défense ou de sûreté de l'Etat et le troisième se rapporte aux échanges transfrontières de données.

a) Les dispositifs nationaux utilisés à des fins de sécurité publique, de défense ou de sûreté de l'Etat

La directive européenne 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 a exclu, par son article 3, de son champ d'application les traitements de données à caractère personnel ayant pour objet la sécurité publique, la défense et la sûreté de l'Etat et son seizième considérant précise que les traitements des sons et images par vidéosurveillance n'entrent pas dans le champ d'application de la directive s'ils sont mis en œuvre « à des fins de sécurité publique, de défense, de sûreté de l'Etat ou de droit pénal ».

Les conditions juridiques d'utilisation des dispositifs biométriques nationaux utilisés à ces fins relèvent donc de la compétence de chaque Etat[1].

En France, ces conditions sont définies notamment par la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et par certaines lois particulières dont certaines s'inspirent d'ailleurs largement des principes définis par cette loi et d'autres sont édictées par le code de procédure pénale. Dans d'autres pays tels que les Pays-Bas une législation spécifique a été établie pour définir les conditions d'utilisation des fichiers de police[2].

Comme le Conseil constitutionnel l'a rappelé récemment[3], il appartient au législateur d'assurer la conciliation entre, d'une part, la sauvegarde de l'ordre public, y compris la prévention des atteintes à l'ordre public, et la recherche des auteurs d'infractions, toutes deux nécessaires à la protection de principes et de droits de valeur constitutionnelle et, d'autre part, le respect de la vie privée et des autres droits et libertés constitutionnellement protégés.

La loi de 1978 comporte certaines dérogations en faveur des traitements mis en œuvre à des fins de sécurité.

---

[1] Certains principes ont été définis au niveau du Conseil de l'Europe en 1987 – Recommandation n° R (87) 15 du Comité des Ministres aux Etats membres visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police adoptée le 17 septembre 1987. Les lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel adoptées par l'OCDE le 23 septembre 1980 reconnaissent pour leur part la possibilité de déroger aux principes qu'elles définissent dans les domaines ressortissant de la souveraineté nationale, de la sécurité nationale et de l'ordre public, tout en précisant que ces exceptions devraient être aussi peu nombreuses que possible et portées à la connaissance du public.

[2] Aux Pays Bas la loi du 28 décembre 1988 sur la protection des données a été complétée par une loi du 21 juin 1990 sur les fichiers de police.

[3] Huitième et vingtième considérants de la décision n°2003-467 DC du 13 mars 2003 sur la loi relative à la sécurité intérieure.

D'une part, des dérogations sont prévues au principe de publicité lorsque les traitements concernent *« la sûreté de l'Etat, la défense et la sécurité publique »*. L'article 19 dispose ainsi que dans ces cas, les demandes d'avis adressées à la CNIL peuvent ne pas comporter les mentions obligatoires énumérées par ledit article et qui visent notamment les catégories d'informations nominatives traitées, les conditions de communication et de transferts transfrontières. Par ailleurs l'article 20 permet de déroger au principe de publication des actes réglementaires portant mise en œuvre de tels traitements[4].

D'autre part, des dispositions dérogatoires limitent les droits des personnes dont les données font l'objet de traitements liés à la sécurité. L'article 26 qui pose le principe que toute personne a le droit de s'opposer pour des raisons légitimes à la collecte de données la concernant exclut certains traitements limitativement désignés. De même, l'article 26 qui définit le droit pour les personnes concernées à être informées précise que ses dispositions ne s'appliquent pas à la collecte des « informations nécessaires à la constatation des infractions ». Enfin, l'article 39 définit une procédure particulière d'accès indirect et de rectification pour les traitements relatifs à « la sûreté de l'Etat, la défense et la sécurité publique », cet article ayant été modifié par la récente loi sur la sécurité intérieure afin notamment de résoudre les difficultés liées à l'application des dispositions initiales[5].

Le projet de loi en cours de discussion visant à modifier la loi n°78-17, qui soumet à des régimes d'autorisation les traitements qui intéressent « la sûreté de l'Etat, la défense ou la sécurité publique ou qui ont pour objet la prévention, la recherche, la constatation ou la poursuite des infractions pénales, ou l'exécution des condamnations pénales ou des mesures de sûreté »[6] prévoit également une dispense de la publication de l'acte réglementaire portant autorisation de ces catégories de traitements (article 26). Il déroge également au principe d'information de la personne concernée en faveur des traitements *« ayant pour objet la prévention, la recherche, la constatation ou la poursuite d'infractions pénales »* ainsi que des traitements mis en œuvre pour le compte de l'Etat et intéressant *« la sûreté de l'Etat, la défense, la sécurité publique ou ayant pour objet l'exécution de condamnations pénales ou de mesures de sûreté, dans la mesure où une telle limitation est nécessaire au respect des fins poursuivies par le*

---

[4] Une telle dérogation n'a été utilisée que pour les « services secrets ». Le décret du 7 mars 1986 dispose que « ne seront pas publiés les actes réglementaires relatifs aux fichiers gérés par la direction de la surveillance du territoire, la direction générale de la sécurité extérieure, et par la direction de la protection et de la sécurité de la défense ». David Martin « Les fichiers de police » - PUF - Collection Que sais-je – Juin 1999.

[5] Conseil d'Etat 6 novembre 2002 à propos du droit d'accès aux informations contenues dans le système d'information Schengen et sur les modalités du contrôle du Conseil d'Etat sur l'exercice par la CNIL de sa mission.

[6] Sont également soumis à un régime d'autorisation les traitements automatisés « ayant pour objet l'interconnexion de fichiers relevant d'une ou plusieurs personnes morales gérant un service public et dont les finalités correspondent à des intérêts publics différents » et « l'interconnexion de fichiers relevant d'autres personnes et dont les finalités principales sont différentes ».

traitement » (article 32) et aménage les conditions d'exercice du droit d'accès (article 41), pour les traitements intéressant la sûreté de l'Etat, la défense ou la sécurité publique, en reprenant la rédaction retenue lors de l'adoption de la loi sur la sécurité intérieure.

Le second socle légal sur lequel reposent les traitements liés à la sécurité est constitué par diverses dispositions du code de procédure pénale.

Jusqu'à l'intervention de la loi sur la sécurité intérieure, seuls l'article 78-3 du code de procédure pénale et les articles consacrés au fichier national des empreintes génétiques faisaient clairement allusion au « prélèvement » de données biométriques sur les personnes[7].

L'article 78-3 relatif aux contrôles, vérifications et relevés d'identité dispose ainsi que *« si la personne interpellée maintient son refus de justifier de son identité ou fournit des éléments d'identité manifestement inexacts, les opérations de vérification peuvent donner lieu, après autorisation du procureur de la République ou du juge d'instruction, à la prise d'empreintes digitales ou de photographies lorsque celle-ci constitue l'unique moyen d'établir l'identité de l'intéressé »* et précise que *« la prise d'empreintes ou de photographies doit être mentionné et spécialement motivée dans le procès verbal »*[8], l'article 78-5 édictant une peine à l'encontre des personnes refusant de se prêter aux prises d'empreintes digitales ou de photographies autorisées par le procureur de la République ou le juge d'instruction.

S'agissant des empreintes génétiques, jusqu'à l'intervention de la loi n°2001-1062 du 15 novembre 2001 qui a défini une peine à l'encontre des personnes définitivement condamnées pour une des infractions visées qui refuseraient de se soumettre à un prélèvement biologique destiné à permettre l'analyse d'identification de leur empreinte génétique, un doute planait quant à la possibilité de procéder à un tel prélèvement sans le consentement de la personne, la CNIL ayant exposé les termes du problème dans son rapport d'activité de 1999.

La loi du 18 mars 2003 relative à la sécurité intérieure apporte sur ces questions une clarification importante en autorisant, dans le cadre des enquêtes de flagrance, des enquêtes préliminaires et au cours de l'information judiciaire les

---

[7] Quelques dispositions réglementaires évoquent cependant le principe de « signalisation » de manière implicite : article 3 alinéa 2 du décret n°87-249 relatif au FAED, article D287 du code de procédure pénale (décret n°98-1099 du 8 décembre 1998) portant sur les entrées et sorties des détenus et qui dispose que « les services de l'identité judiciaire du ministère de l'intérieur informent l'établissement pénitentiaire des opérations anthropométriques » ou encore article D249-3 du même code qui permet au chef d'établissement pénitentiaire de sanctionner disciplinairement le détenu refusant de se plier aux opérations de signalisation.

[8] L'article 78-3 du code de procédure pénale dispose par ailleurs que « si elle n'est suivie à l'égard de la personne qui a été retenue d'aucune procédure d'enquête ou d'exécution adressée à l'autorité judiciaire, la vérification d'identité ne peut donner lieu à une mise en mémoire sur fichiers et le procès verbal ainsi que toutes les pièces se rapportant à la vérification sont détruits dans un délai de six mois sous le contrôle du Procureur de la République ».

« opérations de prélèvements externes nécessaires à la réalisation d'examens techniques et scientifiques de comparaison avec les traces et indices prélevés pour les nécessités de l'enquête » ainsi que *« les opérations de signalisation nécessaires à l'alimentation et à la consultation des fichiers de police selon les règles propres à chacun de ces fichiers »*, le refus de se soumettre aux opérations de prélèvement étant puni d'un an d'emprisonnement et de 15 000 euros d'amende. S'agissant des personnes concernées, la loi vise celles susceptibles de fournir des renseignements sur les faits en cause, c'est-à-dire les témoins, ainsi que celles à l'encontre desquelles il existe une ou plusieurs raisons plausibles de soupçonner qu'elles ont commis ou tenté de commettre l'infraction.

Comme l'a souligné le gouvernement dans ses observations sur les recours dirigés contre ladite loi devant le Conseil constitutionnel, les prélèvements externes peuvent être définis comme des *« opérations de prélèvement indolores réalisées de manière non invasive*[9] *- c'est-à-dire ne créant aucune lésion – et qui ne sont susceptibles de mettre en cause ni l'intégrité physique ni la dignité de la personne humaine »,* tels que les prélèvements de salive, aux fins d'une expertise par empreinte génétique, d'empreintes digitales, de photographies, voire de prélèvements de spécimens d'écriture[10].

Les dispositions législatives ou réglementaires afférentes aux fichiers particuliers définissent elles-mêmes des règles relatives notamment aux finalités et aux conditions d'accès de certaines personnes habilitées et des personnes concernées. Les finalités sont nécessairement déterminées de façon assez large. Ainsi, le fichier d'empreintes digitales a été constitué *« en vue de faciliter la recherche et l'identification, par les services de la police nationale et de la gendarmerie nationale, des auteurs de crimes et de délits et de faciliter la poursuite, l'instruction et le jugement des affaires dont l'autorité judiciaire est saisie »*[11]. Le fichier d'empreintes génétiques est ainsi *« destiné à centraliser les empreintes génétiques issues des traces biologiques ainsi que les empreintes génétiques des personnes condamnées pour l'une des infractions mentionnées à l'article 706-55 (du code de procédure pénale) en vue de faciliter l'identification et la recherche des auteurs de ces infractions ».* Ces dispositions peuvent ainsi comporter des règles spécifiques. Ainsi par exemple, le décret du 8 avril 1987

---

[9] A noter que dans son rapport d'activité de 1999, la CNIL considérait qu'un « prélèvement qui suppose un acte « invasif » sur le corps humain, tel qu'une prise de sang, un prélèvement capillaire ou un prélèvement buccal ne peut être effectué de force sur la personne », la Chancellerie estimant, selon le même rapport, qu'en matière pénale le principe de l'inviolabilité du corps humain restait de portée générale en l'absence de disposition législative expresse autorisant, dans certains cas, un prélèvement forcé.

[10] L'étude d'impact émanant du ministère de l'intérieur et publiée en annexe du rapport parlementaire sénatorial sur le projet de loi relative à la sécurité intérieure mentionne également les empreintes vocales, l'odeur corporelle ainsi que les opérations anthropométriques constitutives de la signalisation. Elle précise que « le fondement traditionnel de la signalisation tiré de la nécessité d'établir précisément l'identité d'une personne mise en cause dans une procédure judiciaire est explicitement complété par la notion de prélèvement effectué aux fins de comparaison technique avec un indice relevé dans une affaire délictuelle ou criminelle ».

[11] Décret n°87-249 du 8 avril 1987.

relatif au fichier d'empreintes digitales énonce le principe selon lequel *« aucune interconnexion, rapprochement ou aucune forme de mise en relation avec un autre traitement automatisé d'informations nominatives »* n'est autorisé.

b) Le droit commun applicable aux systèmes biométriques

Dans son dernier rapport d'activité (n°22 – 2001), la CNIL a esquissé une doctrine destinée à encadrer les conditions d'utilisation des systèmes biométriques:

-« Les technologies de reconnaissance biométrique ne reposant pas sur le ***stockage*** *des gabarits dans une base de données ne soulèvent pas de difficulté particulière en termes « informatique et libertés », dès lors que* ***le gabarit est conservé sur soi (une carte à puce) ou sur un appareil dont on a l'usage exclusif (un téléphone portable, un ordinateur…) et nulle part ailleurs.***

-« En revanche, lorsqu'une ***base de données*** *est constituée dans le cadre d'un dispositif biométrique, l'élément biométrique retenu peut avoir une incidence sur nos libertés et notre vie privée ; tel est le cas lorsque l'élément biométrique retenu « laisse des* ***traces*** *» dans notre vie quotidienne (ADN, empreinte digitale). Dans un tel cas, le contrôle de finalité et de proportionnalité peut conduire à accepter la mise en œuvre de telles bases de données lorsqu'un* ***impératif particulier de sécurité*** *le justifie.*

-« A défaut d'une telle justification particulière, et lorsqu'une ***base de données*** *de gabarits est constituée, le choix d'un* ***élément biométrique « ne laissant pas de trace »,*** *tel que le contour de la main, la rétine, la reconnaissance vocale… devrait être préféré à la prolifération des fichiers d'ADN ou d'empreintes digitales ».*

Elle a, par ailleurs, rappelé que l'utilisation des traitements informatiques associés à un système de vidéosurveillance, lequel relève de dispositions spécifiques[12] doit être soumise aux dispositions de la loi de 1978 et donc à son contrôle.

[12] Dans sa délibération n°94-056 du 21 juin 1994 portant adoption d'une recommandation sur les dispositifs de vidéosurveillance mis en œuvre dans les lieux publics et les lieux recevant le public, la CNIL avait considéré que « lorsqu'elles sont captées par la caméra (…) les images des personnes doivent être regardées comme des informations nominatives permettant (…) l'identification de ces personnes » et que « l'enregistrement et le stockage des images collectées par la caméra de vidéosurveillance permettent de constituer un fichier des personnes ainsi filmées et que cette opération sera encore plus aisée à effectuer lorsque les images seront numérisées ». La loi n°95-73 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité a défini un régime juridique spécifique, l'article 10 disposant que « les enregistrements visuels de vidéosurveillance ne sont considérés comme des informations nominatives, au sens de la loi n°78-17 du 6 janvier 1978 (…) que s'ils sont utilisés pour la constitution d'un fichier nominatif ». Le Conseil constitutionnel, dans sa décision n°94-352 DC du 18 janvier 1995, a jugé les garanties

Cet effort de normalisation doit être salué, mais il ne permet pas de lever les multiples incertitudes qui demeurent sur les conditions d'application des règles relatives à la protection des données personnelles aux dispositifs biométriques susceptibles d'être mis en œuvre.

La frontière entre, d'une part ce qui relève du domaine de la sécurité publique, de la sûreté de l'Etat et des activités de l'Etat dans le domaine pénal et, d'autre part, ce qui n'en relève pas n'est pas établie clairement. Au demeurant, la directive de 1995 qui, dans son article 3 exclut de son champ d'application les traitements ayant pour objet *« la sécurité publique, la défense, la sûreté de l'Etat et les activités de l'Etat relatives à des domaines du droit pénal »*, dispose aussi dans son article 13 que *« le Etats membres peuvent prendre des mesures législatives visant à limiter la portée »* de diverses obligations et droits prévus par la directive, en particulier ceux afférents à la qualité des données (principe de loyauté, de finalité, de pertinence, d'exactitude, de durée limitée de conservation), à l'information de la personne concernée, au droit d'accès et à la publicité des traitements, *« lorsqu'une telle limitation constitue une mesure nécessaire pour sauvegarder a) la sûreté de l'Etat, b) la défense, c) la sécurité publique, d) la prévention, la recherche, la détection et la poursuite d'infractions pénales ou de manquements à la déontologie dans le cas des professions réglementées, e) un intérêt économique ou financier important d'un Etat membre ou de l'Union européenne, y compris dans les domaines monétaire, budgétaire et fiscal, f) une mission de contrôle, d'inspection ou de réglementation relevant, même à titre occasionnel, de l'exercice de l'autorité publique dans les cas visés aux points c), d) et e), g) la protection de la personne concernée ou des droits et libertés d'autrui »*.

En outre, la position de la CNIL qui retient la notion de « trace » pour opérer une distinction entre les techniques biométriques selon leur degré de « dangerosité » semble se référer essentiellement aux dispositifs actuellement mis en œuvre de manière opérationnelle dans le cadre de l'identification judiciaire, la « menace » n'étant pas intrinsèquement liée à l'installation ou à l'utilisation dans le domaine « civil », privé ou public, de dispositifs biométriques dès lors que ceux-ci répondent aux prescriptions définies par les textes garantissant la protection des données personnelles, mais provenant plutôt des possibilités données aux autorités judiciaires ou policières d'accéder aux fichiers ainsi constitués et pour lesquels les données ont été collectées à des fins déterminées, non directement liées à la recherche d'auteurs d'infractions[13].

---

définies par ladite loi suffisantes à l'exception d'une disposition prévoyant que l'autorisation est réputée acquise à défaut de réponse dans un délai de quatre mois. Les conditions d'application du dispositif législatif ont été précisées par les décrets du 17 octobre 1996 et du 15 janvier 1997 ainsi que par une circulaire du 22 octobre 1996. Le *Parliamentary Office of Science and Technology* britannique a rendu, pour sa part, un rapport sur l'utilisation des caméras de vidéosurveillance – *Postnote* n° 175 – Avril 2002.

[13] A cet égard, il convient en effet de rappeler que dans son rapport d'activité 2000, la CNIL soulignait que « le ministre de l'intérieur n'a pas donné suite au projet de numérisation

La constitution de fichiers biométriques utilisant des données de même nature que celles enregistrées dans les fichiers de police (empreintes digitales, ADN aujourd'hui, photographies ou voix demain) pose le problème de l'accès à ceux-là des gestionnaires de ceux-ci à des fins de recoupement, ou de policiers agissant dans le cadre d'une commission rogatoire.

En dehors de ces questions de souveraineté liées à l'étendue des moyens dont disposent les services d'identification judiciaire et au degré de protection des données biométriques, comme d'autres données personnelles, vis-à-vis de l'Etat, la doctrine définie par la CNIL laisse les autres acteurs, en particulier ceux du secteur privé, dans l'expectative.

Les entreprises qui souhaitent renforcer par des procédés biométriques la sécurité physique de leurs locaux ou la sécurité logique de leurs réseaux ou des données nominatives qu'elles utilisent sont confrontées à de multiples incertitudes juridiques concernant la procédure à suivre et la responsabilité qu'elles sont susceptibles d'encourir. L'utilisation d'une technique biométrique implique-t-elle une autorisation ou une simple déclaration ? La sécurisation des locaux et des échanges de données est-elle susceptible de justifier le recours à des procédés biométriques ? Quel est le degré de sécurité ou de confidentialité exigé pour pouvoir utiliser telle technique particulière ? Les investissements effectués, même limités au stade de l'étude d'un projet d'implantation, ne risquent-ils pas d'être perdus ? Afin de limiter le risque juridique et économique, l'entreprise ne sera-t-elle pas incitée à choisir une technique biométrique moins performante ou moins adaptée à ses besoins réels ? Ne sera-t-elle pas finalement encouragée à renoncer à utiliser un dispositif biométrique ?

Il ne s'agit pas uniquement d'une question de procédure. Les entreprises qui gèrent un service public et les administrations sont confrontées à un même dilemme et ces incertitudes se répercutent nécessairement sur les acteurs économiques intervenant dans le domaine de la production ou de l'implantation des systèmes biométriques.

Aussi semble-t-il nécessaire d'examiner plus avant les conditions dans lesquelles le fonctionnement des systèmes biométriques est susceptible d'être appréhendé au travers des concepts juridiques employés.

---

d'empreintes digitales (…) afin de ne pas donner l'impression que pourrait se constituer, à l'occasion d'une démarche administrative, un outil de police judiciaire ».
Ainsi, si le décret relatif la carte nationale d'identité dispose que l'empreinte digitale prélevée lors de l'établissement de celle-ci peut être utilisée « en vue de l'identification certaine dans le cadre d'une procédure judiciaire », le décret n°82-103 du 22 janvier 1982 relatif au répertoire national d'identification des personnes physiques dispose quant à lui qu'en dehors des cas expressément prévus par la loi, le répertoire ne peut servir à des fins de recherche des personnes.

Données biométriques et données personnelles :

Actuellement un consensus existe sur le fait d'assimiler une donnée biométrique à une donnée personnelle. C'est ainsi la position adoptée par la CNIL, la commission d'accès à l'information du Québec[14] ou l'Office parlementaire britannique.

La directive de 1995 s'applique ainsi, aux termes de son article 3, *« au traitement de données à caractère personnel, automatisé en tout ou partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier* », mais elle ne s'applique toutefois pas au traitement de données à caractère personnel *« effectué par une personne physique pour l'exercice d'activités exclusivement personnelles ou domestiques »*.

Une donnée à caractère personnel y est définie comme « toute information concernant une personne physique identifiée ou identifiable ». Est réputée identifiable, selon la directive, *« une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification, ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale »*.

Le quatorzième considérant de la directive précise que *« compte tenu de l'importance du développement en cours, dans le cadre de la société de l'information, des techniques pour capter, transmettre, manipuler, enregistrer, conserver ou communiquer des données constituées par des sons et des images, relatives aux personnes physiques, la présente directive est appelée à s'appliquer aux traitements portant sur ces données »*.

En revanche, le onzième considérant dispose que le principe de protection ne s'applique pas aux *« données rendues anonymes d'une manière telle que la personne concernée n'est plus identifiable* » en renvoyant aux *« codes de conduite »* pour déterminer les moyens par lesquels les données peuvent être rendues anonymes et conservées sous une forme ne permettant plus l'identification de la personne concernée.

A l'égard du traitement - à savoir *« toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification par transmission, diffusion ou toute forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction »* - des

[14] Au Québec une loi concernant le cadre juridique des technologies de l'information et réglementant l'usage de la biométrie a été adoptée en 2001 et la commission d'accès à l'information a défini en 2002 une série de principes d'application extrêmement stricts (annexe 5). Ce guide de « bonnes pratiques » énumère les différentes questions qui se posent lors de l'implantation d'un système biométrique et auxquelles des solutions doivent être trouvées afin de garantir l'intégrité et la confidentialité des données traitées.

données à caractère personnel, les Etats membres doivent en vertu de l'article premier de la directive assurer, conformément à celle-ci, la protection des libertés et droits fondamentaux des personnes physiques, notamment leur vie privée.

Cette protection comporte plusieurs volets dont le plus important définit les conditions générales de licéité des traitements de données à caractère personnel, la responsabilité de « la personne responsable du traitement » étant susceptible d'être engagée pour réparer le préjudice subi du fait d'un traitement illicite mais aussi le cas échéant sur le plan pénal[15].

La licéité des traitements est tout d'abord subordonnée à la qualité des données, lesquelles doivent être traitées loyalement et licitement, collectées pour des finalités déterminées, adéquates et non excessives au regard des finalités pour lesquelles elles ont été collectées, exactes et si nécessaire mises à jour, conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités.

La licéité des traitements dépend aussi du respect des droits de la personne concernée. La directive énonce, d'une part, les conditions dans lesquelles la légitimité d'un traitement est reconnue et qui est fondée sur le consentement direct ou indirect (exécution d'un contrat) de la personne concernée, son intérêt « vital » ou sur les obligations incombant au responsable du traitement (obligations légales, exécution d'une mission d'intérêt public dont le responsable du traitement ou dont le tiers auquel les données sont communiquées est investi). Elle définit, d'autre part, les conditions dans lesquelles la personne concernée doit être informée et peut exercer son droit d'accès et son droit d'opposition lorsque des *« raisons prépondérantes et légitimes tenant à sa situation particulière »* le justifient et lorsque le traitement n'est pas fondé sur son consentement direct ou indirect, ni sur une obligation légale à laquelle le responsable du traitement est soumis.

La confidentialité et la sécurité des traitements doivent également être assurées, des mesures techniques et d'organisation devant garantir un niveau de sécurité approprié au regard des risques présentés par le traitement et la nature des données à protéger, compte tenu de l'état de l'art et des coûts liés à leur mise en œuvre.

---

[15] En vertu de l'article 6 de la directive, il incombe au responsable du traitement d'assurer le respect de ces prescriptions ; l'article 23 dispose que les Etats membres prévoient que toute personne ayant subi un dommage du fait d'un traitement illicite ou de toute action incompatible avec les dispositions nationales prises en application de la directive a le droit d'obtenir du responsable du traitement réparation du préjudice subi, le responsable du traitement pouvant être exonéré partiellement ou totalement s'il prouve que le fait qui a provoqué le dommage ne lui est pas imputable ; l'article 24 dispose pour sa part que les Etats membres prennent les mesures appropriées pour assurer la pleine application des dispositions de la directive et déterminent notamment les sanctions à appliquer en cas de violation des dispositions prises pour l'application de la directive.

Enfin, la directive définit des procédures de contrôle.

Le projet de loi en cours de discussion relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n°78-17 définit une donnée à caractère personnel comme *« toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres »*, le Sénat ayant précisé que *« pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens susceptibles d'être raisonnablement mis en œuvre, soit par le responsable du traitement, soit par une autre personne »*.

S'agissant des conditions de licéité des traitements, le projet de loi s'aligne également sur les dispositions définies par la directive. Ainsi, par exemple, le principe du consentement y est affirmé, tout en autorisant les traitements n'ayant pas reçu le consentement direct des personnes mais satisfaisant à certaines « conditions » (respect d'une obligation légale incombant au responsable du traitement, sauvegarde de la vie de la personne concernée, exécution d'une mission de service public dont est investi le responsable ou le destinataire du traitement, exécution d'un contrat auquel la personne concernée est partie ou de mesures précontractuelles prises à sa demande, réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou le destinataire).

A cet égard, les données biométriques présentées comme des signes objectifs et inaltérables ne présentent aucune particularité par rapport aux autres données personnelles afférentes à l'identité d'un individu (nom, prénom, date et lieu de naissance) et doivent bénéficier d'un niveau de protection équivalent.

Données biométriques, traitements présentant des risques particuliers et données sensibles :

Deux niveaux de protection renforcée sont définis par la directive de 1995.

Le premier niveau est de nature procédurale. En vertu de l'article 20 de la directive, les Etats membres précisent les traitements susceptibles de présenter des risques particuliers au regard des droits et libertés des personnes concernées et veillent à ce que ces traitements soient examinés avant leur mise en œuvre, un simple contrôle *a posteriori* étant requis pour les autres traitements. Les considérants de la directive précisent que le principe d'un contrôle *a posteriori* par l'autorité de contrôle devrait en général être considéré comme suffisant et que le nombre de traitements susceptibles de présenter des risques particuliers *« du fait de leur nature, de leur portée ou de leurs finalités telles que celle d'exclure des personnes du bénéfice d'un droit, d'une prestation ou d'un contrat, ou du fait de l'usage particulier d'une technologie nouvelle »*, devrait être très restreint.

Le second niveau vise des traitements effectués sur des catégories particulières de données que l'article 8 de la directive énumère et qui bénéficient d'une protection renforcée au regard des principes communs de licéité.

Il s'agit des données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que les données relatives à la santé et à la vie sexuelle.

Il s'agit aussi des données relatives aux infractions, aux condamnations pénales ou aux mesures de sûreté.

Il s'agit enfin des numéros nationaux d'identification ou de tout autre identifiant de portée générale, mais sur ce point la directive ne définit aucune interdiction ou garantie particulière ; elle se contente d'énoncer que les Etats membres déterminent les conditions dans lesquelles ces « données » peuvent faire l'objet d'un traitement.

Au regard du premier principe, un nombre très limité de techniques biométriques sont susceptibles de poser un problème. La plupart des données biométriques ne permettent pas *a priori* de révéler une race ou une ethnie particulière[16], ni l'état de santé[17] de la personne concernée. Le deuxième principe ne concerne nullement les données biométriques. Reste le troisième principe qui semble opérer une assimilation entre les numéros d'identification « signifiants » tels que le numéro français de sécurité sociale et « tout autre identifiant de portée générale » sans qu'une définition précise ne soit donnée à cette expression.

La question des identifiants, qu'ils soient de nature biométrique ou pas, est doublement délicate. Déjà en 1980 le Conseil de l'Europe, à l'occasion de l'adoption des lignes directrices régissant la protection de la vie privée et les flux transfrontières de données à caractère personnel, avait pu mesurer cette ambiguïté. Ainsi d'une part, dans son exposé des motifs, le groupe de travail relevait que « dans certains pays, les identificateurs individuels universels pourront être considérés comme inoffensifs et utiles alors que, dans un autre pays, ils pourront être considérés comme éminemment délicats et leur utilisation pourra être limitée

[16] En 1991, la CNIL considérait que « les informations relatives au signalement des personnes mises en cause permettant aux enquêteurs de noter l'aspect physique et les signes distinctifs d'une personne (…) sont de nature à faire apparaître les origines raciales ou les convictions religieuses des personnes concernées ». Sur la base de ces principes, le décret du 14 octobre 1991 relatif aux fichiers gérés par les services des renseignements généraux autorise la collecte, la conservation et le traitement d'informations qui font apparaître « les signes physiques particuliers, objectifs et inaltérables », comme éléments de signalement. Cette expression est d'ailleurs reprise par l'arrêté du 6 août 1993 autorisant la création d'une base de données destinée à l'initialisation du système d'information Schengen et dans la Convention Europol.

[17] L'EWA canadien a ainsi évoqué la reconnaissance par l'iris qui permettrait de détecter des maladies de l'œil ou des diabètes ainsi que l'empreinte digitale dont l'examen pourrait révéler des troubles chromosomiques, mais de telles assertions devraient être vérifiées par des experts médicaux.

voire interdite »[18] et, d'autre part, s'agissant des garanties de sécurité nécessaires à la protection des données personnelles, les cartes d'identification sont présentées comme une solution possible dans les commentaires détaillés.

En France, cette question prend une dimension particulière puisque c'est à la suite de l'émotion suscitée par un projet (projet SAFARI de 1974) de généralisation du numéro INSEE à toute l'administration que la loi de 1978 a été adoptée et la CNIL instituée. Aussi, l'utilisation du numéro de sécurité sociale est-elle encadrée (décret en Conseil d'Etat pris après avis de la CNIL), le défaut d'autorisation étant sanctionné pénalement, ce qui d'ailleurs n'a pas empêché une large utilisation de ce numéro. La loi de 1978 repose sur une logique différente de celle sous-tendant la directive puisque, si elle contient également des mesures de protection particulières pour les données médicales, les infractions et les données sensibles faisant apparaître les origines raciales, les opinions politiques ou religieuses, l'appartenance syndicale ou les mœurs des personnes, elle opère une distinction entre le secteur public, soumis à un régime d'autorisation, et le secteur privé, soumis à un régime de déclaration qui n'exonère pas le demandeur de ses responsabilités.

Le projet de loi visant à transposer en droit interne la directive de 1995 tient compte des observations présentées par la CNIL lors de son élaboration : les traitements de données biométriques nécessaires au contrôle de l'identité des personnes[19] sont soumis à un régime d'autorisation, sans plus de précision sur les conditions dans lesquelles ladite autorisation sera accordée ou refusée[20].

Données biométriques, droit d'accès et rectification :

S'il est un domaine où les données biométriques posent des problèmes techniques particuliers au regard de la protection des données personnelles, c'est bien celui des conditions d'exercice du droit d'accès ou de rectification.

L'article 12 de la directive pose le principe de la *« communication, sous forme intelligible, des données faisant l'objet des traitements »*. Il reconnaît à la personne concernée le droit de prendre *« connaissance de la logique qui sous-*

[18] Voir à ce propos « l'interconnexion des fichiers administratifs », Service des affaires européennes du Sénat http://www.senat.fr

[19] Les « données génétiques » sont visées par un autre alinéa ; sont soumis à un régime d'autorisation « les traitements automatisés portant sur des données génétiques, à l'exception de ceux d'entre eux qui sont mis en œuvre par des médecins ou des biologistes et qui sont nécessaires aux fins de la médecine préventive, des diagnostics médicaux ou de l'administration de soins ou de traitements ».

[20] Le projet de loi définit dans deux articles distincts le régime des traitements relatifs à des données faisant apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou qui sont relatives à la santé ou à la vie sexuelle de celles-ci d'une part et, d'autre part ceux concernant les infractions, condamnations et mesure de sûreté.

tend tout traitement automatique des données la concernant », au moins dans le cas où des décisions individuelles automatiques produisant des effets juridiques à son égard ou l'affectant de manière significative, sont prises sur le seul fondement d'un traitement automatisé de données destiné à évaluer certains aspects de sa personnalité, le quarante et unième considérant prenant soin de préciser que ce droit ne doit pas porter atteinte au secret des affaires, ni à la propriété intellectuelle, notamment au droit d'auteur protégeant le logiciel mais que cela ne doit toutefois pas aboutir au refus de toute information de la personne concernée. La directive prévoit également la rectification, le verrouillage et l'effacement des données incomplètes ou inexactes.

La loi de 1978 reconnaît également à *« toute personne justifiant de son identité »*, un droit d'interrogation et de communication *« en langage clair »* et pose le principe de la rectification, de la mise à jour et de l'effacement des informations inexactes, équivoques, périmées.

Le projet de loi de transposition reprend ces principes : communication *« sous une forme accessible »*, information de la personne concernée lui permettant de connaître et de contester la logique qui sous-tend le traitement quand les résultats de celui-ci lui sont opposés, sous réserve du respect du droit d'auteur, rectification à la demande de *« toute personne physique justifiant de son identité »* des données inexactes, incomplètes, équivoques, périmées.

De ce point de vue, les techniques biométriques peuvent susciter quelques difficultés, dans la mesure où la donnée n'est pas nécessairement conservée sous une forme visuellement reconnaissable[21] .

c) Données biométriques et transferts transfrontaliers

C'est probablement à ce niveau que se concentrent les incertitudes les plus inquiétantes.

L'article premier de la directive dispose que *« les Etats membres ne peuvent restreindre ni interdire la libre circulation des données entre Etats membres pour des raisons relatives à la protection des libertés et des droits fondamentaux des personnes physiques, notamment de leur vie privée, à l'égard du traitement des données à caractère personnel »*.

L'ensemble des Etats membres sont ainsi, du fait de l'adoption de la directive, considérés avoir des niveaux de protection équivalents, ce qui ne sera

[21] En 1986, la CNIL avait considéré qu'un droit d'accès direct au fichier des empreintes digitales devait être reconnu aux personnes intéressées en raison notamment du caractère « objectif » des informations recueillies, lesquelles ne concernaient « que l'identité de l'individu » et parce que la présence de l'intéressé avait été jugée « indispensable pour contrôler si les empreintes digitales sont bien les siennes ».

pas forcément le cas, notamment en ce qui concerne les données biométriques. On peut donc estimer qu'à terme, par l'effet de l'intensification des échanges de données, les Etats ayant défini des règles strictes quant au traitement des données biométriques seront conduits à s'aligner sur ceux ayant fait preuve d'une plus grande souplesse, d'autant que, à la différence des numéros d'identification nationaux, les techniques biométriques permettront de fournir des identifiants « universels ».

Les articles 25 et 26 de la directive instituent par ailleurs une procédure complexe pour régler le problème des transferts extra européens.

Tout en posant le principe que le transfert vers des pays tiers est subordonné à l'exigence d'un niveau de protection adéquat, eu égard notamment à la nature des données, la finalité, la durée du traitement et aux règles de droit applicables, elle prévoit un certain nombre de dérogations.

Il appartient à la Commission et aux Etats membres d'apprécier le niveau adéquat ; si la Commission estime que ce niveau n'est pas atteint, le transfert est interdit et la Commission doit remédier à la situation par la négociation et si elle constate que ce niveau est atteint, les Etats membres prennent les mesures nécessaires pour se conformer à sa décision.

Néanmoins, sous réserve de dispositions nationales contraires régissant des cas particuliers, les Etats membres doivent prévoir qu'un transfert de données à caractère personnel vers un pays tiers n'assurant pas un niveau de protection adéquat peut être effectué lorsque certaines conditions sont remplies : la personne concernée a indubitablement donné son consentement au transfert envisagé, le transfert est nécessaire à l'exécution d'un contrat entre la personne concernée et le responsable du traitement ou de mesures précontractuelles prises à la demande de la personne concernée, le transfert est nécessaire à la conclusion ou à l'exécution d'un contrat conclu ou à conclure, dans l'intérêt de la personne concernée, entre le responsable du traitement et un tiers, le transfert est nécessaire ou rendu juridiquement obligatoire pour la sauvegarde d'un intérêt public important, ou pour la constatation, l'exercice ou la défense d'un droit en justice, le transfert est nécessaire à la sauvegarde de l'intérêt vital de la personne concernée, ou encore le transfert intervient au départ d'un registre public destiné à l'information du public et ouvert à la consultation du public. En dehors de ces cas, les Etats membres peuvent aussi autoriser un transfert si le responsable du traitement *« offre des garanties suffisantes au regard de la protection de la vie privée et des libertés et droits fondamentaux des personnes, ainsi qu'à l'égard de l'exercice des droits correspondants »*, ces garanties pouvant résulter de clauses contractuelles mais cette autorisation étant soumise à une procédure spécifique.

L'article 19 de la directive dispose par ailleurs que les transferts de données envisagés à destination de pays tiers doivent figurer dans la notification.

S'agissant des domaines ne relevant pas du champ d'application de la directive, il convient de noter que la récente loi relative à la sécurité intérieure comporte un article consacré à ce problème.

Aux termes de la nouvelle loi, les données contenues dans les traitements automatisés de données personnelles gérés par les services de police et de gendarmerie nationales peuvent être transmises à des organismes de coopération internationale en matière de police judiciaire ou à des services de polices étrangers qui présentent, pour la protection des données personnelles, des *« garanties équivalentes »* à celles du droit interne, *« dans le cadre des engagements internationaux régulièrement introduits dans l'ordre juridique interne »*. Parallèlement, les services nationaux de police et de gendarmerie peuvent recevoir des données contenues dans les traitements gérés par les organismes de coopération internationale en matière de police judicaire ou les services de police étrangers dans le cadre des engagements de même nature.

La recommandation R(87) 15 du Comité des Ministres aux Etats membres du Conseil de l'Europe visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police, adoptée le 17 septembre 1987, dispose pour sa part que la communication de données à des autorités étrangères devrait se limiter à des services de police et devrait être permise que s'il existe une disposition légale claire découlant du droit interne ou international ou, si à défaut d'une telle disposition, la communication est nécessaire à la prévention d'un danger grave et imminent ou à la répression d'une infraction pénale grave de droit commun , et dans la mesure où il n'est pas porté atteinte aux réglementations internes relatives à la protection de la personne concernée. Elle précise par ailleurs que les données ainsi communiquées ne devraient pas être utilisées à d'autres fins que celles spécifiées dans la demande de communication, toute utilisation à d'autres fins devant être subordonnée à l'accord de l'organe expéditeur.

S'agissant de l'utilisation des empreintes génétiques, une recommandation du Conseil de l'Europe du 10 février 1992 définit les conditions dans lesquelles les analyses d'ADN peuvent être utilisées dans le cadre du système de justice pénale (consentement sauf décision judiciaire, protection des données, destruction des échantillons, contrôle des laboratoires) et le Conseil de l'Union européenne a adopté, le 9 juin 1997, un texte relatif à l'échange des analyses d'ADN en matière pénale. Au sein d'INTERPOL, un guide sur l'échange de données génétiques et sur les pratiques en matière d'analyse d'ADN est paru en juin 2001 et un formulaire normalisé pour l'échange international de profils d'ADN a été élaboré[22] et, en mai dernier, le G8 a adopté des principes directeurs afin d'améliorer l'échange d'informations sur les empreintes génétiques.

Le règlement 45/01 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données, adopté par le

[22] Rapport d'activité 2001.

Parlement européen et le Conseil, reprend, dans la mesure du possible, les dispositions de la directive 95/46 et institue un Contrôleur européen de la protection des données traitées par les organes communautaires. Mais, selon certains auteurs[23] et comme le suggère l'intitulé du règlement, celui-ci ne concerne que les traitements mis en œuvre par les institutions et organes communautaires relevant en tout ou partie du champ d'application du droit communautaire et non ceux mis en œuvre par ces mêmes instances dans le cadre de la coopération policière et judiciaire en matière pénale, pas plus que les traitements mis en œuvre au sein des systèmes européens d'information dits du troisième pilier (SIS -Système d'information Schengen, SID -Système d'information des douanes, et SIE -Système d'information Europol)[24]. Divers auteurs et le Parlement européen ont dénoncé l'insuffisance du cadre normatif actuel.

Le projet de loi modifiant la loi de 1978 détermine (articles 30, 32 et 38) les conditions dans lesquelles la CNIL, lors des déclarations, des demandes d'autorisation et d'avis, le public, ainsi que les personnes concernées sont informés des possibilités de communication à des tiers ou à des destinataires et de transfert à un Etat non membre de la Communauté. La CNIL doit également publier la liste des Etats dont la Commission des Communautés européennes a établi qu'ils assurent un niveau de protection suffisant à l'égard d'un transfert ou d'une catégorie de transferts de données à caractère personnel (article 30). Le transfert vers des pays ne présentant pas le même niveau de protection est en principe interdit, mais le projet de loi reprend à peu près les mêmes exceptions que celles édictées par la directive. L'article 69 de la loi de 1978 modifiée par le projet de loi permet aussi de déroger à ce principe, lorsque *« le traitement garantit un niveau de protection suffisant de la vie privée ainsi que des libertés et droits fondamentaux des personnes, notamment en raison des clauses contractuelles ou règles internes dont il fait l'objet »*, par simple décision de la CNIL ou, pour les traitements qui intéressent la sûreté de l'Etat, la défense ou la sécurité publique ou

---

[23] Francesco Maiani, *Revue trimestrielle de droit européen* n°2, avril – juin 2002.

[24] Le SIS (Schengen) est un réseau de banques de données, identiques entre elles, mises à la disposition des autorités nationales de police et un réseau de communication entre celles-ci. L'article 117 de la Convention de Schengen impose aux parties contractantes d'assurer que leurs législations nationales respectent la Convention n°108 et la recommandation du Conseil des ministres du Conseil de l'Europe intitulée « Réglementation de l'utilisation de données à caractère personnel dans le secteur de la police ». Les parties contractantes se sont engagées mutuellement à exécuter les décisions définitives des autres parties concernant la rectification, le verrouillage et l'effacement des données. Une Autorité commune de contrôle (ACC), composée de représentants des autorités nationales, est chargée d'étudier les problèmes pouvant se poser lors de l'exercice du contrôle indépendant effectué par les autorités de contrôle nationales des parties contractantes ou à l'occasion de l'exercice du droit d'accès au Système.
Les principes de la Convention 108 sont applicables aux données à caractère personnel collectées, traitées et utilisées par EUROPOL (Convention du 26 juillet 1995 portant création de l'Office européen de police) qui a pour fonction de favoriser l'échange d'informations entre Etats membres, mais aussi d'analyser ces données et de fournir aux autorités de police des Etats membres un service d'intelligence.

qui ont pour objet la prévention, la recherche, la constatation ou la poursuite des infractions pénales, ou l'exécution des condamnations pénales ou des mesures de sûreté, par décret en Conseil d'Etat ; dans ces cas, la CNIL porte à la connaissance de la Commission des Communautés européennes et des autorités de contrôle des autres Etats membres de la Communauté les décisions d'autorisation de transfert qu'elle prend.

2 - Les conséquences juridiques d'une utilisation des systèmes biométriques : la question de la valeur probante d'une donnée biométrique

La preuve se définit comme *« la démonstration de l'existence d'un fait dans les formes admises par la loi »*[25].

En matière pénale, elle revêt une importance toute particulière. *« D'abord, parce qu'elle touche aux garanties des personnes, notamment à la présomption d'innocence à laquelle elle peut porter atteinte, comme elle concerne l'ordre public. Ensuite, parce que toutes les règles de procédure n'ont, en définitive, d'autre finalité que la recherche et l'administration de la preuve »*[26].

Il se trouve par ailleurs que les dispositifs biométriques sont actuellement utilisés très majoritairement dans le domaine de l'identification judiciaire, même si les procédés mis en œuvre ne sont pas tous intégralement automatisés.

Aussi, semble-t-il opportun de rappeler les règles en vigueur dans ce domaine, ne serait-ce que pour souligner que l'utilisation de systèmes biométriques ne paraît pas de nature à occasionner leur remise en cause dans l'immédiat tout au moins.

Plus délicate en revanche est la question de la valeur probante des données biométriques dans les domaines non directement liés à l'identification des auteurs d'infractions pénales.

Ces deux questions seront donc tour à tour examinées, étant précisé qu'en règle générale, dans l'établissement de la preuve, l'identification biométrique ne constituera qu'un moyen parmi plusieurs autres présomptions. La « preuve biométrique » n'a pas en principe vocation à se substituer aux autres moyens de preuve.

---

[25] Vocabulaire juridique – PUF – 1987.
[26] Jacques Buisson « Preuve » Répertoire pénal Dalloz – mars 1999.

a) L'identification des auteurs d'infractions pénales

L'imputation de faits délictueux à une personne déterminée mise en cause ne constitue qu'un élément de la preuve pénale, mais elle est essentielle.

Le principe de la présomption d'innocence implique en effet que l'accusation repose sur des charges suffisantes de la culpabilité de l'auteur apparent et qu'au cours du procès le doute profite à l'accusé.

Dans le cadre de la procédure française de type inquisitoire, la preuve est soumise à un double régime de légalité et de liberté, en amont et au cours du procès pénal.

En amont, le principe de la légalité de l'administration de la preuve, dont la violation est sanctionnée par des nullités, oblige les autorités policières et judiciaires à respecter certains principes, tel que le principe de la loyauté dans la recherche des preuves, le principe de la dignité de la personne humaine, le principe des droits de la défense ou le principe de l'intimité de la vie privée, mais aussi les dispositions légales et réglementaires encadrant certaines procédures.

L'utilisation de techniques biométriques d'identification des personnes peut à cet égard soulever certaines difficultés, en raison notamment de l'imprécision des textes actuels, même si la récente loi sur la sécurité intérieure a permis de progresser dans ce domaine. Ces difficultés sont liées principalement aux conditions dans lesquelles sont collectées les données biométriques qui seront ultérieurement comparées.

Il s'agit en premier lieu des conditions de récolement et de conservation des indices.

Sur les lieux de la commission d'une infraction, la prise d'indices, qui permet de déterminer le mode opératoire de l'auteur et de procéder à son identification, n'est pas soumis au principe de la non coercition. Elle peut donc avoir lieu à l'insu des personnes visées et sans leur consentement. Le décret n°87-249 du 8 avril 1987 relatif au fichier automatisé des empreintes digitales mentionne ainsi les *« traces relevées dans le cadre d'une enquête pour crime ou flagrant délit, d'une enquête préliminaire, d'une commission rogatoire ou de l'exécution d'un ordre de recherche délivré par une autorité judiciaire »* et précise que les traces d'empreintes enregistrées sont accompagnées d'informations relatives notamment au lieu sur lequel elles ont été relevées, ainsi qu'à la date du relevé, au service ayant procédé à la signalisation et à la date et au lieu d'établissement de la fiche signalétique. Le support technique sur lequel a été relevée une empreinte digitale est une annexe au procès verbal de constatations des enquêteurs et n'entre dès lors pas dans les prévisions de l'article 56 du code de procédure pénale relatives au placement sous scellés (Cassation, Chambre criminelle 29 septembre 2002). Il en est pratiquement de même des empreintes

génétiques, sous réserve cependant de la conservation sous scellés des échantillons qui font l'objet de dispositions propres.

En matière de perquisitions et de saisies, les procédures sont encadrées par des textes précis, mais ceux-ci ne déterminent pas les conditions particulières dans lesquelles des « empreintes » biométriques pourraient être relevées.

Les prélèvements opérés sur les individus eux-mêmes obéissent à d'autres règles. Le respect des droits de la défense oblige ainsi à reconnaître à la personne soupçonnée *« le droit de ne pas contribuer à sa propre incrimination »* (Cour européenne des droits de l'homme – 8 février 1996 – Murray contre Royaume-Uni). Mais la Cour européenne des droits de l'homme a, s'agissant de la donnée biométrique actuellement considérée comme la plus « sensible », jugé que ce droit *« ne s'étend pas à l'usage de données que l'on peut obtenir de l'accusé en recourant à des pouvoirs coercitifs, mais qui existent indépendamment de la volonté du sujet, par exemple les documents recueillis en vertu d'un mandat, les prélèvements d'haleine, de sang et d'urine, ainsi que de tissus corporels en vue d'une analyse de l'ADN ».* Le respect de l'intimité de la vie privée peut aussi constituer une limite à l'utilisation de « preuves biométriques ». La jurisprudence abondante sur les enregistrements de paroles et de sons en témoigne. La circulaire du 22 octobre 1996 relative à la vidéosurveillance évoque également les risques, appréciés il est vrai en dehors du cadre d'une procédure judiciaire, liés à la prise d'images au regard des dispositions garantissant le respect de la vie privée. Les textes régissant les fichiers d'empreintes digitales et d'empreintes génétiques déterminent les conditions dans lesquelles il est procédé aux relèvements ou aux prélèvements et les personnes à l'égard desquelles ces procédures peuvent être engagées.

S'agissant des conditions dans lesquelles un « rapprochement » peut avoir lieu, des dispositions explicites ont été introduites dans les textes régissant certains fichiers. Le décret précité de 1987 relatif au FAED dispose ainsi que *« les fonctionnaires dûment habilités du service d'identité judiciaire du ministère de l'intérieur et des unités de recherches de la gendarmerie nationale pourront seuls avoir accès aux informations enregistrées et procéder aux opérations d'identification à la demande de l'autorité judiciaire ou des officiers de police judiciaire de la police nationale ou de la gendarmerie nationale »*, en précisant que ledit fichier *« ne peut faire l'objet d'aucune interconnexion, rapprochement ou d'aucune forme de mise en relation avec un autre traitement automatisé d'informations nominatives »*. L'article 706-54 du code de procédure pénale relatif au FNAEG prévoit pour sa part que *« les officiers de police judiciaire peuvent d'office ou à la demande du procureur de la République ou du juge d'instruction, faire procéder à un rapprochement de l'empreinte de toute personne à l'encontre de laquelle il existe une ou plusieurs raisons plausibles de soupçonner qu'elle a commis un crime ou un délit, avec les données incluses au fichier, sans toutefois que cette empreinte puisse être conservée ».* La récente loi sur la sécurité intérieure qui a introduit les nouveaux articles 55-1 (crimes et délits

flagrants), 76-2 (enquête préliminaire) et 154-1 (commissions rogatoires) dans le code de procédure pénale a par ailleurs défini les conditions dans lesquelles il est procédé *« sur toute personne susceptible de fournir des renseignements sur les faits en cause ou sur toute personne à l'encontre de laquelle il existe une ou plusieurs raisons plausibles de soupçonner qu'elle a commis ou tenté de commettre l'infraction »* aux opérations de prélèvements externes *« nécessaires à la réalisation d'examens techniques et scientifiques de comparaison avec les traces et indices prélevés pour les nécessités de l'enquête ».*

Conjointement au principe de la légalité de l'administration de la preuve, a été posé le principe de la liberté d'appréciation par le juge répressif de la valeur des preuves qui lui sont fournies, le système français reposant sur le principe de l'intime conviction du juge.

Cette liberté s'exprime en aval du procès, lors de la mise en accusation[27] et la saisine de la juridiction de jugement, comme au cours du jugement lui-même.

Aussi les résultats d'une identification génétique ne s'imposent-elles pas aux juges et restent soumis à leur appréciation souveraine au même titre que les aveux et les témoignages (Cassation, chambre criminelle 3 juillet 1997 ; 9 janvier 1998).

Les conclusions d'un expert ne lient pas non plus le juge ; elles n'ont la valeur que d'un avis. Le recours à des moyens biométriques d'identification est ainsi susceptible de conduire à la multiplication de contre expertises sur la base de la jurisprudence fondée sur le respect des droits de la défense et établie en matière de témoignage, en vertu de laquelle tout accusé a droit d'interroger ou faire interroger les témoins à charge et obtenir la convocation et l'interrogation des témoins à décharge dans les mêmes conditions que les témoins à charge.

Aux Etats-Unis par exemple, où les experts témoignent systématiquement et où il y a toujours une audience obligatoire sur les protocoles utilisés par tel expert dans une affaire donnée, la défense conteste fréquemment les protocoles utilisés[28] pour l'analyse d'ADN. L'utilisation des empreintes digitales comme élément de preuve a aussi été contestée récemment. En 1999, la

[27] Ainsi à propos du renvoi en cour d'assises pour meurtre d'une personne qui arguait l'absence de présomption grave et précise à son encontre au motif que seulement six points de comparaison identiques à ceux de l'empreinte digitale de son pouce droit avaient été retrouvés dans une tâche de sang se trouvant sur le couteau, alors qu'il était établi que 17 points de comparaison étaient nécessaires pour permettre l'identification formelle d'un individu, la Cour de cassation a rejeté le pourvoi, la chambre d'accusation ayant relevé l'existence de « charges suffisantes » après avoir exposé les faits et répondu comme elle le devait aux articulations essentielles du mémoire dont elle était saisie. Cassation Chambre criminelle 11 octobre 1995.

[28] Aux Etats-Unis, le Procureur n'est pas obligé de recourir au mode de preuve par empreinte génétique. Le FBI a proposé récemment que des crédits soient alloués à tous les Etats fédérés et au niveau fédéral pour procéder à l'analyse d'ADN des condamnés, notamment ceux qui se disent innocents.

défense, dans l'affaire US v. Mitchell, a appelé la communauté scientifique à s'intéresser à la fiabilité des preuves produites et reposant sur des empreintes digitales, notamment en examinant la validité des tests effectués, le taux d'erreur, et les règles de comparaison. En 2002, dans l'affaire US v. Llera Plaza, le juge, après avoir refusé d'autoriser la vérification par un expert de la correspondance entre une trace d'empreinte digitale et l'empreinte « roulée » d'une personne particulière, a admis la production de rapports d'experts en matière d'empreintes digitales[29] .

b) L'identification des titulaires de droits ou d'obligations

Dans quelle mesure les techniques biométriques d'identification (ou d'authentification) sont-elles susceptibles d'agir sur les conditions d'exercice de droits ou d'obligations que la loi ou le contrat reconnaît à telle personne ?

Dans la plupart des cas[30], les résultats issus de l'application de techniques biométriques pour les contrôles d'accès ou la sécurisation des titres ne produiront pas directement d'effets juridiques ; leur portée restera essentiellement pratique. Les modalités de contrôle ou de vérification s'en trouveront facilitées si le dispositif est conçu pour accélérer les procédures de contrôle ou de vérification ou s'alourdiront si elles s'inscrivent dans un domaine jugé très sensible qui exige que le taux de fausses acceptations soit le plus faible possible. Dans ces cas en effet, l'identification biométrique ne constitue pas une condition juridique en elle-même, mais seulement une modalité particulière de contrôle se substituant ou complétant des dispositifs préexistants ou dont la mise en œuvre est envisagée.

L'article 3 de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés énonce à cet égard que *« toute personne a le droit de connaître et de contester les informations et les raisonnements utilisés dans les traitements automatisés dont les résultats lui sont opposés »*, tandis que l'article 29 prescrit à la personne ordonnant ou effectuant le traitement l'obligation, vis-à-vis des personnes concernées, de prendre les mesures nécessaires pour empêcher la déformation ou l'endommagement des informations et que l'article 36 pose les principes de la rectification et de l'effacement des informations inexactes ou équivoques. La directive de 1995 est

[29] GAO – 03 – 174 « *Biometrics for Border Security* » p.141.

[30] L'article 16-11 du code civil détermine les cas dans lesquels l'identification d'une personne par ses empreintes génétiques peut être recherchée.
Article 16-11 : « L'identification d'une personne par ses empreintes génétiques ne peut être recherchée que dans le cadre de mesures d'enquête ou d'instruction diligentées lors d'une procédure judiciaire ou à des fins médicales ou de recherche scientifique.
« En matière civile, cette identification ne peut être recherchée qu'en exécution d'une mesure d'instruction ordonnée par le juge saisi d'une action tendant soit à l'établissement ou la contestation d'un lien de filiation, soit à l'obtention ou la suppression de subsides. Le consentement de l'intéressé doit être préalablement et expressément recueilli.
« Lorsque l'identification est effectuée à des fins médicales ou de recherche scientifique, le consentement de la personne doit être au préalable recueilli ».

moins explicite puisqu'elle n'émet de réserves qu'à l'encontre des traitements automatisés de données destinés à évaluer certains aspects de la personnalité, tels que notamment le rendement professionnel, la fiabilité, le crédit, le comportement de la personne concernée. Le projet de loi en cours de discussion prend en compte cette orientation en limitant la portée juridique de décisions qui seraient prises sur le fondement d'un traitement automatisé de données destiné à évaluer certains aspects de la personnalité ou à définir le profil de l'individu, tout en précisant qu'une décision prise dans le cadre de la conclusion ou de l'exécution d'un contrat et pour laquelle la personne concernée a été mise à même de présenter ses observations n'est pas regardée comme prise sur le seul fondement d'un traitement automatisé.

C'est actuellement dans le domaine des transmissions électroniques que le développement des techniques biométriques pourrait produire des effets juridiques tangibles à terme, en raison de l'importance des problèmes liés à l'identification ou l'authentification des parties à une « transaction » de ce type.

Si l'on s'en tient aux termes de la loi n°2000-230 du 13 mars 2000 relative à la « signature électronique », les techniques biométriques sont appelées à avoir un impact dans ce domaine[31]. L'article 1316 du code civil ne subordonne-t-il pas l'admission en preuve de l'écrit sous forme électronique au même titre que l'écrit sur support papier à la double condition que *« la personne dont il émane puisse être identifiée »* et que l'établissement et la conservation dudit écrit soient de nature à en garantir l'intégrité ? Il est vrai néanmoins que le deuxième alinéa de l'article 1316-4 du même code semble lier intrinsèquement les deux éléments en définissant la « signature électronique » comme *« l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache »*, la fiabilité de ce procédé étant présumée, jusqu'à preuve contraire, lorsque *« la signature électronique est créée, l'identité du signataire assurée et l'intégrité de l'acte garantie, dans des conditions fixées par décret en Conseil d'Etat*[32] *»*.

---

[31] Les Chinois, il y a plus de 1000 ans, utilisaient l'empreinte digitale à des fins de signature de documents.

[32] Au sens du décret n°2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 une signature électronique est dite « sécurisée » si elle satisfait à trois exigences : être propre au signataire, être créée par des moyens que le signataire puisse garder sous son contrôle exclusif et garantir avec l'acte auquel elle s'attache un lien tel que toute modification ultérieure de l'acte soit détectable. L'article 3 du décret exige d'un dispositif sécurisé de création de signature électronique notamment qu'il garantisse par des moyens techniques et des procédures appropriés que les données de création de signature électronique a) ne peuvent être établies plus d'une fois et que leur confidentialité est assurée b) ne peuvent être trouvées par déduction et que la signature électronique est protégée contre toute falsification c) peuvent être protégées de manière satisfaisante par le signataire contre toute utilisation par des tiers.
A la suite de la directive sur le commerce électronique du 8 juin 2000 (2000/31/CE) qui notamment prescrit aux Etats de veiller à ce que leur système juridique rende possible la conclusion des contrats par voie électronique et à ce que le régime juridique applicable au processus contractuel ne fasse pas obstacle à l'utilisation de contrats électroniques ni ne conduise à priver d'effet et de validité juridiques de tels contrats pour le motif qu'ils sont passés par voie électronique, le projet de loi, en cours de discussion, pour la confiance dans l'économie

Les techniques biométriques d'identification sont capables de fournir des indices susceptibles d'être pris en compte dans le cadre du règlement d'un litige portant sur un fait matériel voire même sur un acte juridique. Le fait d'avoir apposé sa main ou son doigt peut ainsi par exemple attester des horaires de travail, de la demande du bénéfice d'une prestation, de la présence dans un lieu ou de l'accès à un service d'un individu. Il est actuellement difficile d'apprécier les effets, sur le plan contentieux, de leur utilisation : leurs résultats seront-ils contestés ou seront-ils considérés comme un moyen de preuve suffisant susceptible de dissuader le plaideur de contester le fait lui-même ? Mais en se projetant dans le futur, on peut essayer de déterminer les évolutions qu'un déploiement des techniques biométriques peut susciter.

De même que le progrès scientifique conduit le législateur à définir des présomptions[33], notamment, du moins dans un premier temps, des présomptions simples, compte tenu du degré de fiabilité des techniques mises en œuvre, le développement des techniques biométriques renforcera vraisemblablement cette tendance, avec le risque de voir se multiplier les mesures d'expertise[34], la présomption facilitant par ailleurs l'administration de la preuve par le plaideur qui en bénéficie.

La « preuve biométrique » ne sera donc pas forcément une preuve automatique restreignant la liberté d'appréciation du juge. Au niveau de l'admissibilité des preuves, d'autres moyens seront susceptibles d'être produits et sur le plan de la valeur probante, il appartiendra au juge de décider du crédit qui pourra être accordé à cet indice de nature technique.

On peut enfin évoquer la question de la validité des conventions qui subordonneraient l'attribution ou la perte d'un droit à un mode particulier de preuve ou limiteraient la responsabilité d'une des parties.

---

numérique, introduit dans le titre III du code civil relatif aux contrats et obligations conventionnelles, un nouvel article 1108-1 qui comporte deux alinéas. Le premier renvoie aux dispositions du code civil sur la « signature électronique », en particulier à l'article 1316-4, l'établissement et la conservation sous forme électronique d'un écrit exigé pour la validité d'un acte juridique pouvant répondre aux conditions fixées par ces dispositions. Le deuxième alinéa précise que la mention manuscrite de la main même de celui qui s'oblige peut être apposée sous forme électronique « si les conditions de cette apposition sont de nature à garantir que la mention ne peut émaner que de lui-même ».

[33] Les présomptions sont définies par l'article 1349 du code civil comme « des conséquences que la loi ou le magistrat tire d'un fait connu à un fait inconnu ». « Ces faits connus sont des indices d'où il résulte une **probabilité** plus ou moins grande de l'existence du fait qu'il s'agit de prouver » Répertoire Dalloz – Procédure civile – Preuve n°25.

[34] En vertu de l'article 6 du nouveau code de procédure civile, les parties ont la charge d'alléguer les faits propres à fonder leurs prétentions et les mesures d'instruction sont précisément destinées à apporter la preuve des faits dont dépend la solution du litige ; l'article 232 du même code donne au juge le pouvoir de commettre toute personne de son choix pour l'éclairer sur une question de fait qui requiert les lumières d'un technicien.

II - Les évolutions perceptibles à l'échelle européenne et internationale

Plusieurs évolutions sont perceptibles au niveau international, liées essentiellement aux initiatives prises par certains Etats.

Dans les deux domaines de l'identification judiciaire et de la sécurisation des titres, des travaux ont été engagés depuis plusieurs années par les Etats et une coopération a été recherchée.

Or, les avantages liés à l'utilisation des techniques biométriques, qui depuis de nombreuses années ont été reconnus dans le domaine de l'identification judiciaire, apparaissent encore plus évidents dans un contexte où la collaboration s'avère désormais indispensable entre plusieurs Etats pour combattre la criminalité organisée.

De même, la sécurisation des titres délivrés par la puissance publique qui constitue un sujet de préoccupation pour les gouvernements peut également s'appuyer sur des techniques biométriques tandis que l'intensification des flux transfrontaliers des personnes rend nécessaire une harmonisation des normes techniques permettant d'assurer un niveau de sécurité reconnu par tous et d'accélérer les opérations de vérification.

Les acteurs économiques se trouvent nécessairement impliqués par les décisions prises par les Etats, même si l'identification judiciaire ou la délivrance de titres ne constitue qu'une partie de la demande à laquelle ils sont susceptibles de répondre.

1 - Le contexte politique international : biométrie et circulation transfrontalière des personnes

Plusieurs Etats mènent actuellement des réflexions sur l'utilisation des techniques biométriques.

Mais c'est dans le domaine du contrôle de la circulation transfrontalière des personnes que des décisions importantes ont été prises et que les échéances semblent les plus rapprochées.

Après avoir présenté la politique des Etats Unis dans ce domaine et avoir retracé les travaux menés au sein de l'Organisation de l'Aviation Civile Internationale (OACI), les orientations européennes seront examinées, étant rappelé qu'en mai dernier, lors de la réunion du G8, a été décidée la création d'un groupe de travail d'experts pour déterminer les techniques biométriques les plus aptes à permettre un meilleur contrôle des individus lors du passage des frontières.

a) La politique des Etats-Unis

Aux Etats-Unis, à la suite des attentats terroristes qui ont été perpétrés sur le territoire américain, diverses initiatives ont été prises au niveau fédéral pour renforcer la sécurité du pays.

Au cours des deux dernières années, deux lois importantes ont été adoptées, *the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act* de 2001, couramment nommé le « USA PATRIOT Act », et *the Enhanced Border Security and Visa Entry Reform Act* de 2002.

Ces nouvelles dispositions s'insèrent dans une série de textes qui ont été adoptés depuis 1996, en particulier *the Illegal Immigration Reform and Immigrant Responsability Act* de 1996 et *the INS Data Management Improvement Act* de 2000. C'est ainsi que pour passer les frontières terrestres, depuis 1998, les cartes délivrées contiennent déjà un identifiant biométrique et sont lisibles par machine (« *laser visas* ») : les utilisateurs mexicains sont photographiés et l'empreinte des deux index est prise, mais le *General Accounting Office* a observé que si 5 millions de cartes ont bien été délivrées, le service d'immigration ne dispose pas encore de lecteurs appropriés et que les contrôles sont effectués manuellement à l'entrée du territoire[35]. En outre, comme l'indiquait ce même organisme, pour l'obtention et la vérification des documents de voyage, le Département d'Etat, depuis plusieurs années, conduit des projets pilotes utilisant la reconnaissance faciale dans vingt-trois postes consulaires outre-atlantique.

Les textes adoptés en 2001 et 2002 posent le principe d'une utilisation des techniques biométriques pour assurer le contrôle des frontières. Dans le cadre d'un nouveau système d'informations rassemblant les données détenues par les différentes agences fédérales sur les étrangers cherchant à entrer ou rester aux Etats-Unis, l'identification biométrique, associée à la lecture automatique des visas et des passeports, est envisagée. Le programme ainsi défini confie au *National Institute of Standards and Technology* (NIST) la mission d'établir des normes pour le contrôle des visas américains et fixe au 26 octobre 2004 la date limite à partir de laquelle les visas délivrés doivent être sécurisés et permettre une lecture automatique et les autres documents d'entrée doivent comporter des identifiants biométriques, l'installation des équipements nécessaires pour

[35] GAO-03-174, novembre 2002.

authentifier par la biométrie les visas et les passeports à tous les ports d'entrée étant prévue pour cette date.

Dans le cadre du programme de lutte contre le terrorisme, l'administration fédérale a été profondément réorganisée. Le Département de la sécurité intérieure (*Department of Homeland Security – DHS*) a été mis en place et compte le contrôle des frontières et, en particulier, le contrôle des voyageurs à l'entrée et à la sortie du territoire parmi ses missions. En son sein, un nouveau Bureau (*of Customs and Border Protection*), regroupant les douanes et le service national d'immigration (INS), a été créé en mars 2003.

L'année dernière, le NSEERS (*National Security Entry-Exit Registration System*) intégrant la base IDENT qui contient 9 millions d'empreintes digitales et est gérée par le service d'immigration, a été implanté. Il contient les empreintes digitales des criminels et terroristes étrangers.

En janvier 2003, conformément aux textes adoptés en 2001 et 2002, un rapport[36] conjoint du NIST, du Département de la Justice et du Département d'Etat a été remis au Congrès. Ce rapport préconise l'empreinte digitale et la reconnaissance faciale[37] (photographie), pour lesquelles des bases suffisamment vastes sont disponibles et recommande, pour la sécurisation des titres c'est-à-dire l'authentification de l'origine du document, une PKI (*Public Key Infrastructure*). Le coût du dispositif (installation et maintenance sur six années) est estimé à 3,8 milliards de dollars. Il propose également que le délai d'octobre 2004 soit repoussé d'une année afin de garantir une meilleure performance. Parallèlement et également en janvier 2003, l'*International Biometric Group*, une société de conseil et d'intégration, a remis à l'*Office of Science and Technology* de la Maison Blanche, un rapport sur l'utilisation de la biométrie pour la sécurité des frontières et basé sur l'évaluation des techniques réellement opérationnelles.

Les administrations fédérales se préparent activement.

Le service de l'immigration - (anciennement INS) qui gère d'ores et déjà plusieurs systèmes biométriques (le programme facultatif INSPASS utilisant l'empreinte de la main et qui est ancien, la base IDENT qui doit devenir compatible avec la base du FBI et qui utilise les empreintes digitales et les cartes de franchissement qui comportent une photographie avec hologramme et au dos, sur une bande magnétique, l'empreinte digitale) - est chargé d'installer à chaque point d'inspection les terminaux de lecture permettant de comparer (1/1) les visas. Des sites expérimentaux seront progressivement mis en place puis généralisés.

---

[36] "*Use of Technology Standards and Interoperable Databases with Machine-Readable*".

[37] Dans ses conclusions, le NIST s'est appuyé sur les résultats d'une évaluation reposant sur la comparaison de 121 589 images de 37 437 individus (le Face Recognition Vendor Test 2002 – FRVT 2002). Elle révèle que les taux d'erreurs dans le domaine de la reconnaissance faciale ont diminué de 50 % en deux ans et qu'en matière d'identification, les systèmes de reconnaissance faciale les plus performants atteignent un niveau équivalent à celui établi pour les empreintes digitales en 1998.

Trois problèmes semblent néanmoins préoccuper cette administration : le respect de la date cible, les implications pratiques des taux d'erreurs sur la sécurité et la rapidité des procédures de contrôle, et l'attitude des autres pays qui pourraient aussi exiger pour les visas des citoyens américains l'introduction de données biométriques.

La TSA (*Transportation Security Administration*), qui relève du DHS et est chargée de la sécurité de l'ensemble des moyens de transports, a mené une enquête sur l'évaluation des produits disponibles et défini trois applications spécifiques, le contrôle d'accès des aéroports et des gares, la surveillance/détection des voyageurs susceptibles de menacer la sécurité et l'identification des passagers.

S'agissant du contrôle d'accès des personnels et notamment des pilotes aux zones protégées et aux postes de pilotage, l'iris et l'empreinte digitale paraissent les techniques les mieux appropriées car les plus fiables actuellement, la reconnaissance faciale utilisant des images 3D semblant aussi très prometteuse. Une vingtaine de sites pilotes vont être implantés pour tester les résultats techniques et les incidences pratiques de cinq technologies (iris, géométrie de la main, empreinte digitale, face et voix), avec, comme perspective, la mise en place d'une carte à puce uniforme comportant une donnée biométrique commune et une donnée biométrique à usage local. La donnée biométrique de référence sera probablement l'empreinte digitale qui permet la comparaison 1/*n* à partir d'un fichier centralisé, la donnée opérationnelle étant laissée à l'appréciation de chaque aéroport et permettant le stockage d'informations sur la carte elle-même.

Dans le domaine de la surveillance/détection opérée à partir d'une liste « d'indésirables » (« *watch list* »), la reconnaissance faciale semble préférable. Des tests opérationnels ont été réalisés dans certains aéroports, tels que ceux de Boston et Palm Beach. La technique doit encore être améliorée, mais elle donne déjà des résultats satisfaisants lorsqu'elle est employée à des goulets d'étranglement où les passagers restent relativement statiques.

Pour l'identification des passagers, les objectifs de rapidité, de facilité d'utilisation et d'absence de contact conduisent à privilégier l'iris, la face et la voix, alors que l'OACI a retenu la face, puis l'iris et l'empreinte digitale et que le NIST préconise l'empreinte digitale et la face. La TSA travaille sur le concept de voyageurs inscrits (« *Registered Travelers* ») qui vise à accélérer les procédures de passage en réservant les opérations de contrôle aux personnes les moins connues et suggère l'idée d'une « carte d'identité ». La difficulté essentielle réside dans les problèmes d'échelle qui rendent critiques les questions de performance tant en ce qui concerne le réseau informatique que le système de comparaison.

Dans le domaine de la recherche et du développement, la TSA a défini plusieurs priorités, les crédits disponibles pour la seule biométrie restant limités. Ces priorités concernent la constitution de bases permettant de tester l'iris, la face et la voix ainsi que la combinaison de ces trois techniques, l'amélioration de la

résistance des techniques aux problèmes liés au vieillissement des sujets (permanence), l'image 3D pour la reconnaissance faciale qui permet de réduire les erreurs provoquées par les différences de luminosité, la reconnaissance à distance par l'iris, le contrôle des foules en mouvement et la technique de fusion pour la biométrie multimodale.

Le NIST (*National Institute of Standards and Technology*) travaille depuis près de deux années en étroite collaboration avec les autres agences fédérales et les industriels pour définir des normes nationales et internationales destinées à promouvoir le développement des techniques biométriques dans un climat consensuel. Déjà le NIST avait participé à la définition du standard BioAPI (*Application Programming Interface)*[38] et, en collaboration avec l'agence fédérale de la sécurité nationale (*National Security Agency – NSA*), au développement d'un standard pour les échanges (*Common Biometric Exchange File Format – CBEFF*). Depuis les évènements du 11 septembre, le NIST s'est fortement impliqué dans les travaux de normalisation au niveau international. En juin 2002, a été constituée une sous-commission « biométrie » (SC 37) au sein de la commission ISO/IEC (JTC1) sur les technologies de l'information et la présidence de cette sous-commission a été confiée en décembre 2002 au NIST pour les trois prochaines années. Cet organisme est ainsi appelé à coordonner les travaux de normalisation conduits au niveau national au sein de l'*InterNational Committee for Information Technology Standards* – INCITS et au niveau international avec l'objectif d'accélérer les procédures nécessaires pour aboutir à la définition de normes de compatibilité et d'évaluation des performances.

Certaines réserves ont cependant été exprimées. Ainsi le *General Accounting Office*, qui en novembre 2002 avait remis un rapport d'évaluation relativement critique sur les orientations du programme[39], a formulé[40] devant le Sénat, le 12 mars 2003, des doutes sur la « faisabilité » du projet dans les délais impartis, en s'appuyant sur le rapport du NIST.

Après avoir insisté sur les enjeux du programme (440,4 millions de contrôles aux frontières par an, 7 millions de passeports et 8,4 millions de visas délivrés annuellement) et reconnu que les techniques biométriques pouvaient contribuer à l'amélioration de la sécurité, il a mis en évidence les bouleversements introduits dans les procédures de contrôle, proposant que, pendant dix années, les visas actuels coexistent avec des « visas biométriques », souligné les failles d'un système insuffisamment préparé, tant en ce qui concerne les règles de gestion d'une liste de contrôle que la sécurité du document lui-même, s'est interrogé sur la portée juridique du dispositif envisagé au regard du *Privacy Act* de 1974 et a enfin rappelé le principe de réciprocité applicable en matière de visas et de

[38] ANSI INCITS 358 – 2000, BioAPI v 1.1.

[39] « *Technology Assessment : Using Biometrics for Border Security*" GAO-03-174.

[40] Audition devant la sous-commission sur le terrorisme, la technologie et la sécurité intérieure, la sous-commission sur la sécurité des frontières, l'immigration et la citoyenneté et la commission de la Justice du Sénat – « *Border Security Challenges in implementing Border Technology »* - GAO-03-546T

passeports et la nécessité d'unifier les données biométriques susceptibles d'être retenues par d'autres pays pour leurs passeports.

Selon Katie CORRIGAN, *Legislative Counsel* pour l'ACLU (*American Civil Liberties Union*), le Congrès, qui a pris de nombreuses dispositions depuis le 11 septembre sans prendre le temps d'en débattre vraiment, engage maintenant des réflexions pour évaluer les effets des dispositifs sur la vie privée, leurs incidences économiques et leur efficacité. Un mouvement, transcendant les clivages partisans, se forme actuellement pour corriger l'orientation sécuritaire précédemment définie et défendre les libertés individuelles et celles des Etats fédérés[41]. L'ACLU ne s'oppose pas à l'utilisation des techniques biométriques, ni à l'emploi d'une technique particulière, mais reste vigilante sur les risques liés à l'utilisation d'une donnée personnelle et unique qui pourrait servir de base à l'institution d'une carte d'identité ou d'un système national d'identification. De son point de vue, la diversité des données biométriques utilisées constitue une garantie pour les libertés et un gage de sécurité.

Les critiques formulées par l'ACLU reposent sur une analyse des différentes mesures arrêtées depuis le 11 septembre et rendues possibles grâce à l'insuffisance du cadre juridique protégeant la vie privée. Dans le domaine de la sécurité aérienne notamment, divers dispositifs de surveillance renversent le principe de la présomption d'innocence de telle sorte que l'individu doit désormais apporter la preuve qu'il est innocent. Dans le cadre du système de contrôle assisté par ordinateur, le traitement de données officielles et officieuses opère ainsi un tri parmi les passagers, entre ceux qui présentent un risque extrême (rouge), ceux pour lesquels une fouille s'avère nécessaire (jaune) et ceux autorisés à entrer sans formalités particulières (vert). Les personnes ne peuvent, en raison du secret défense qui leur est opposé, contester le code qui leur a été attribué, ni même savoir s'ils sont classés « vert » ou « jaune », à cause des contrôles aléatoires effectués. Dans la même logique selon laquelle un individu n'a pas à prouver son identité ou sa nationalité sans motifs valables, l'ACLU a exprimé son opposition au projet de carte d'identité facultative développé par la TSA en raison des risques de généralisation qu'il comporte.

b) Les travaux menés au sein de l'OACI

Dans son discours prononcé à Montréal, le 5 décembre 2001, le Président du Conseil de l'OACI, Dr Assad KOTAITE, a évoqué la biométrie pour

[41] La loi sur la sécurité aérienne a confié à l'Etat fédéral les compétences exercées auparavant par le secteur privé dans le domaine de la sécurité aérienne pour pouvoir édicter des dispositions uniformes applicables à tous les aéroports.

restaurer la confiance du public après les attentats du 11 septembre en faisant allusion à un usage judicieux de ces nouvelles technologies[42].

Une stratégie globale sur la sécurité aérienne a été par ailleurs mise en place. En septembre 2002, un document émanant de l'OACI (PIO 11/2002) soulignait la nécessité d'assurer la fluidité en maintenant le plus haut niveau de sécurité, en partie à travers les nouvelles technologies telles que l'identification biométrique.

Le Conseil de l'OACI, composé de représentants de trente-trois Etats, adopte les normes et les pratiques recommandées. Celles-ci figurent dans les Annexes à la Convention de Chicago qui a institué l'OACI en 1944.

Une instance, placée auprès du Secrétaire Général, a été constituée en 1986 au sein de l'OACI, le *Technical Advisory Group on Machine Readable Travel Documents* (**TAG/MRTD**)[43]. Il se compose de treize experts issus de treize pays membres de l'OACI, dont la France, les Etats-Unis, le Royaume Uni, l'Allemagne et le Japon et des « observateurs » peuvent être invités aux réunions du Groupe, tels INTERPOL (*International Criminal Police Organization*), l'ACI (*Airports Council International*) et l'ISO (*International Organization for Standardisation*). Les réunions du Groupe se tiennent en général tous les 18 mois. Il s'agit d'une instance de proposition visant à inciter les Etats à adopter ses recommandations.

En son sein, un groupe de travail sur les nouvelles technologies est chargé de rechercher et d'analyser les incidences des nouvelles technologies sur l'utilisation des MRTD[44]. Son attention est actuellement concentrée sur la sécurité

---

[42] "*The judicious use of new technologies like biometrics and machine readable travel documents (MRTDs)*".

[43] Dès 1920 le principe d'une souhaitable standardisation fut établi. Le développement du trafic international conduisit dès 1968 l'OACI à envisager l'introduction d'un passeport lisible par machine afin d'accélérer les flux lors des contrôles des passeports et, le cas échéant, supprimer ou automatiser les cartes d'embarquement/débarquement. Un groupe d'étude fut constitué, composé de huit Etats dont la France, la RFA et les Etats-Unis et auquel INTERPOL fut associée. En 1978, après cinq réunions, le groupe émit cinq recommandations et l'OACI publia en 1980 le « Doc 9303 ». Trois pays (le Canada, les Etats-Unis et l'Australie) furent les premiers à appliquer ces recommandations. En 1981 et 1982, le Conseil de la Communauté européenne adopta des résolutions devant permettre la délivrance de passeports uniformes par les pays membres d'ici le 1er janvier 1985 en s'alignant sur les recommandations formulées dans le « Doc 9303 ». En 1986 fut constitué le TAG/MRTD qui s'intéressa en premier lieu aux passeports puis étendit ses attributions aux visas et aux documents de voyage officiel. De 1986 à décembre 2002, le TAG/MRTD a tenu 13 réunions.

[44] Le Doc 9303 est une publication de l'OACI donnant les spécifications des MRTD qui sont actuellement regroupées en trois catégories, les passeports, les visas et les documents de voyage officiel. Le MRTD y est défini comme un document officiel délivré par un Etat ou une organisation qui est utilisé par son possesseur pour des voyages internationaux et qui contient obligatoirement des données visibles (pouvant être lues visuellement) et des données dans un format permettant leur lecture par une machine. Selon un document émanant du TAG/MRTD, intitulé « *A Guide to Doc 9303* », le MRTD est susceptible de faciliter le contrôle d'un document

des documents. Dans ce cadre, il s'est intéressé notamment aux techniques de confirmation de l'identité par la biométrie.

Un rapport technique sur la sélection et le test des technologies biométriques servant à la confirmation d'identité au moyen des MRTD a été élaboré, dans le cadre de la révision du Document 9303 par le TAG/MRTD. Il s'agissait de prendre en compte le souhait d'un Etat ou d'une organisation d'avoir les moyens de confirmer l'identité des personnes dans le cadre de l'utilisation des MRTD.

En 1999, le TAG/MRTD a initié une étude dont le double objectif est, d'une part, de déterminer la compatibilité des technologies biométriques actuelles avec les procédures d'émission (*issuance*) et d'inspection des documents lisibles par machine et, d'autre part, d'identifier une ou plusieurs technologies présentant la meilleure compatibilité et pouvant constituer un standard international pour l'utilisation des MRTD.

Parmi les six technologies utilisées aujourd'hui (face, yeux, doigts, main, signature et voix), aucune, reconnaît le rapport, n'est absolument performante[45].

Ce rapport souligne que l'utilisation d'une seule technique biométrique par tous les Etats serait préférable, car ainsi l'interopérabilité globale du système serait assurée c'est-à-dire qu'une personne présentant un document émis n'importe où dans le monde pourrait prouver qu'il est son détenteur légal. Cependant, il reconnaît que certains Etats pourraient juger souhaitable de déployer deux techniques biométriques sur le même document.

Pour répondre aux exigences d'un système associé au MRTD, une technique biométrique devrait, selon le rapport, assurer à la fois les fonctions de vérification (confirmation de l'identité en comparant l'identité proclamée d'un individu donné à celle enregistrée pour cet individu) et d'identification

---

de voyage à partir d'une liste de surveillance, la vérification de l'authenticité du document et/ou la transmission de l'information contenue dans le document vers d'autres bases de données et ces avantages seront renforcés grâce aux progrès issus notamment des techniques biométriques. Selon le même document, il s'agit d'avantages pour les gouvernements ; notamment le MRTD rend possible l'utilisation de systèmes API (*Advance Passenger Information*) qui permettent aux opérateurs aériens d'envoyer une liste de passagers à diverses autorités telles que les douanes, les services d'immigration ou d'autres et aux officiers des frontières de traiter avant l'arrivée du vol l'information reçue ; les lecteurs permettent aussi de détecter les faux passeports ; les criminels peuvent être rapidement et précisément identifiés…Les voyageurs y trouvent aussi des avantages (rapidité notamment), ainsi que les autorités portuaires (gains de place, gestion plus facile des flux) et les compagnies (sécurité).

[45] "*It is recognized that not all biometric technologies may be capable of supporting the complete set of unique requirements imposed on machine-assisted identity confirmation when a person applies for or renews their MRTD or when they present their MRTD for inspection, for example at border/frontier or at an airline check-in point*".

(détermination de l'identité possible en comparant les éléments de celle d'un individu donné à ceux enregistrés et relatifs à un certain nombre d'individus), ces fonctions devant être réalisables à chaque étape du processus : lors de l'émission du document, lors de son renouvellement et au moment du contrôle du document et de la personne qui l'a en sa possession.

Pour apprécier la compatibilité des techniques biométriques avec les systèmes des documents lisibles en machine, le rapport a défini sept critères : compatibilité avec les exigences de la procédure d'enrôlement MRTD, compatibilité avec les exigences de la procédure de renouvellement, compatibilité avec les exigences de la vérification d'identité par machine, redondance, perception du public, exigence de stockage, performance.

A titre provisoire, le rapport a identifié trois groupes au regard des critères fixés :

- 1- meilleur taux de compatibilité (85%) : face
- 2- second niveau de compatibilité (65%) : doigts et yeux
- 3- moins bon niveau de compatibilité (moins de 50%) : signature, main, voix.

A titre définitif, le rapport a constaté, d'une part, que certaines technologies biométriques sont plus compatibles que d'autres avec les exigences du système MRTD et que, d'autre part, certains facteurs autres que celui de la performance ont un fort impact sur le taux de compatibilité.

Le rapport indique que trois techniques (face, doigts et yeux) seront testés en prenant en compte l'environnement réel du système, ce qui n'avait pas été le cas au stade de la première évaluation. Les tests doivent se poursuivre pour apprécier la capacité de chaque technologie de répondre aux exigences des autorités délivrant les documents (vérification à partir d'un « template » dérivé d'un échantillon tel qu'une photographie, identification à partir de données biométriques archivées obtenues directement ou indirectement) et à celles des autorités de contrôle.

Une décision retenant la reconnaissance faciale et l'empreinte digitale a été arrêtée à Montréal, lors de la quatorzième réunion du TAG/MRTD des 6-9 mai 2003. Le dispositif repose finalement sur le principe d'une généralisation des photographies numérisées et la possibilité pour les Etats d'introduire l'empreinte digitale ou l'iris, selon les décisions adoptées à Montréal le 28 mai dernier.

c) Les réalisations et les hésitations européennes

Les initiatives visant, au niveau européen, à utiliser des techniques biométriques reflètent la complexité et surtout la diversité du processus décisionnel au sein de l'Union. Les procédures diffèrent sensiblement selon que

les décisions s'inscrivent dans le cadre des « affaires communautarisées » par le Traité d'Amsterdam ou dans celui du « troisième pilier », chaque Etat membre étant par ailleurs compétent pour régler directement certaines questions qui doivent pourtant être traitées en aval ou en amont des procédures européennes engagées à l'un ou l'autre titre.

Le Traité d'Amsterdam, entré en vigueur le 1er mai 1999, a transféré dans l'ordre communautaire les questions relatives aux visas, à l'asile, à l'immigration et à d'autres politiques liées à la circulation des personnes et intégré l'acquis Schengen. Pendant une période transitoire de cinq années à compter de son entrée en vigueur, les décisions relèvent du Conseil qui statue en général à l'unanimité sur proposition de la Commission ou à l'initiative d'un Etat membre et après consultation du Parlement européen. Après ce délai, le Conseil statuera selon la procédure de codécision sur proposition de la Commission uniquement, celle-ci devant toutefois examiner toute demande d'un Etat membre visant à ce qu'elle soumette une proposition au Conseil.

En revanche, pour les domaines relevant du « troisième pilier », et en particulier la coopération policière, le Conseil, statuant à l'unanimité à l'initiative de tout Etat membre ou de la Commission, arrête des positions communes, des décisions cadres et des décisions ou établit des conventions.

Il paraît dès lors difficile d'identifier une position à la fois commune et cohérente. Aussi, les travaux engagés au niveau européen ne peuvent-ils être présentés que sous une forme « kaléidoscopique », préjudiciable au débat démocratique et à l'efficacité des politiques publiques, comme à l'implication des acteurs économiques et des chercheurs.

C'est principalement dans le domaine de l'harmonisation et de la sécurisation des titres et documents délivrés par les pays membres que s'exprime cette carence.

La création d'un espace de libre circulation des personnes rend nécessaire un renforcement du contrôle des frontières extérieures, dans l'intérêt des Etats membres et de leurs ressortissants, dans l'intérêt aussi des ressortissants des pays tiers en situation régulière qui doivent pouvoir aisément circuler à l'intérieur de la Communauté et enfin dans l'intérêt des pays tiers ayant passé des accords pour faciliter l'entrée des ressortissants des Etats membres sur leur territoire.

Parallèlement, la volonté des pays européens, agissant souvent en coopération avec d'autres pays, de renforcer l'efficacité de leurs dispositifs de lutte contre la criminalité organisée, le terrorisme, la fraude internationale, la traite des êtres humains devrait se traduire par des moyens appropriés facilitant l'identification des criminels, en particulier lors de leurs déplacements à l'intérieur de cet espace et à l'entrée comme à la sortie de celui-ci.

De ce double point de vue les techniques biométriques peuvent constituer une réponse adaptée aux besoins, mais il existe très peu de réalisations.

Dans le domaine de la coopération policière[46], la mise en place opérationnelle le 1er juillet 1999 de l'office européen de police, EUROPOL, n'a pas donné les résultats espérés, les relations bilatérales semblant privilégiées. Alors que le fichier d'information générale n'était toujours pas opérationnel en février dernier, des divergences sur le rôle d'EUROPOL subsistaient encore ; l'Allemagne souhaitait en faire un « FBI européen », tandis que la France y voyait un instrument de coopération intergouvernementale spécialisée dans le renseignement et la gestion de systèmes d'information[47]. L'efficacité de cet outil dépend aussi de sa capacité de définir les conditions dans lesquelles peuvent être organisés des échanges de données avec les pays tiers et d'autres organismes intergouvernementaux tels qu'INTERPOL. Qu'il s'agisse de coopération entre les Etats membres, ou de coopération avec les pays tiers tels que les Etats-Unis[48], le développement de standards internationaux permettant l'échange de données biométriques constitue un enjeu important[49].

Dans le domaine de la gestion des documents de circulation et de séjour, la mise en place d'EURODAC[50], le système européen de collecte et de comparaison des empreintes digitales des demandeurs d'asile et, dans certaines conditions des étrangers en situation irrégulière, entré en vigueur le 15 janvier 2003, est actuellement la seule réalisation européenne. Ce dispositif, qui s'inscrit dans le cadre de la Convention de Dublin et du Règlement Dublin II, vise à éviter qu'une même personne présente des demandes d'asile dans plusieurs Etats membres[51], l'unité asile et immigration de la Commission ayant estimé à 10 ou

---

[46] Dans le cadre du programme GROTIUS (1996-2000), une étude sur la preuve pénale et le progrès scientifique en Allemagne, en France, en Grande-Bretagne et aux Pays-Bas a été réalisée – http://www.enm.justice.fr.

[47] Délégation pour l'Union européenne du Sénat – Réunion du 5 février 2003 – http://www.senat.fr.

[48] Délégation pour l'Union européenne du Sénat – Réunion du 10 décembre 2003 sur le projet d'accord entre les Etats-Unis et EUROPOL relatif à l'échange de données à caractère personnel – http://www.senat.fr. Délégation pour l'Union européenne de l'Assemblée nationale – Rapport de M. Pierre LEQUILLER et Christian PHILIP n°512. Rapport d'information de M. Didier Quentin au nom de la Délégation de l'Assemblée nationale pour l'Union européenne n°716 (19 mars 2003).

[49] Interpol s'emploie quant à lui à élaborer et à faire accepter des normes internationales permettant l'interopérabilité entre tous les systèmes automatisés de reconnaissance d'empreintes digitales (AFIS), quel qu'en soit le constructeur et coordonne les travaux d'un groupe international d'experts sur l'utilisation de l'analyse de l'ADN comme technique d'enquête (site internet d'Interpol).

[50] Sur la base d'une proposition de la Commission, le Parlement européen a été consulté et le Règlement du Conseil concernant cette création a été adopté (règlement n° 2727/2000 du 11 décembre 2000), complété par le règlement (CE) n° 407/2002 du Conseil du 28 février 2002, lequel prescrit pour l'échange des données le format ANSI/NIST – CSL 1 1993.

[51] Le traitement automatisé relatif à la dactyloscopie des demandeurs du statut de réfugié mis en place par l'OFPRA en 1987 a également pour « finalité d'éviter qu'une même personne puisse sous des identités différentes demeurer en France, malgré une décision de rejet de sa demande par

20% la proportion des demandes multiples d'asile sur 400 000 demandes déposées chaque année. Participent à ce système tous les pays de l'Union à l'exception du Danemark, ainsi que la Norvège et l'Islande qui sont associées à la Convention de Dublin. Chaque Etat membre doit procéder à l'enregistrement et à la transmission à une unité centrale des empreintes digitales (des dix doigts) de toute personne âgée de plus de quatorze ans qui dépose une demande d'asile ou est appréhendée en situation irrégulière au moment où elle franchit les frontières d'un Etat membre, la durée de conservation des données étant d'une année pour les demandeurs d'asile et de deux ans pour les clandestins arrêtés à la frontière. Les coûts liés à la mise en œuvre du dispositif, à la charge du budget communautaire, s'élèvent à 6,5 millions d'euros, le coût de chaque transaction à la charge des Etats membres étant fixé à 2,76 euros.

Plusieurs documents émanant d'institutions ou d'Etats membres évoquent l'utilisation de techniques biométriques sans que l'on puisse apprécier correctement les perspectives de réalisations concrètes.

D'une part, une communication de la Commission au Conseil et au Parlement européen sur la gestion intégrée des frontières extérieures des Etats membres de l'Union européenne[52] du 7 mai 2002 définit plusieurs axes pour *« identifier les risques sur le lieu même de la frontière extérieure »* parmi lesquels *« la veille technologique »*. Sur ce point, le texte précise que *« l'analyse du risque devrait anticiper les conséquences des progrès technologiques sur le travail des gardes frontières, par exemple pour l'utilisation des bases de données électroniques, des données biométriques numérisées ou des moyens de surveillance des frontières extérieures par télédétection »*.

En outre, le 13 juin 2002, le Conseil de l'Union européenne a adopté une décision (« décision ARGO ») portant adoption d'un programme d'action concernant la coopération administrative dans les domaines des frontières extérieures, des visas et de l'immigration, pour la période 2002-2006, le budget alloué pour 2002 étant de 3 millions d'euros. La Commission, dans un document publié au *JOCE* du 15 août 2002, intitulé « programme de travail annuel et appel à propositions pour l'année 2002 – ARGO – 2002/C 195/05 », a indiqué qu'en ce qui concerne les visas, afin d'améliorer la sécurité des documents, renforcer et développer une coopération consulaire commune et étudier la faisabilité d'un système d'information en matière de visas ainsi que d'un réseau de consultation des visas, l'un des *« objectifs spécifiques et priorités »* portait sur *« l'amélioration de la sécurité des documents à la suite des développements technologiques, notamment dans le domaine de la biométrie »*. En outre, l'étude de faisabilité sur les aspects techniques et financiers d'un système d'information en matière de visas, devait *« examiner la possibilité d'intégrer et de rechercher des photographies numérisées et d'autres données biométriques »*.

---

l'OFPRA et bénéficier plusieurs fois des avantages sociaux accordés aux demandeurs du statut de réfugié » - Délibération 87-106 de la CNIL du 3 novembre 1987.

[52] Com (2002)0233.

Les décisions concernant la mise en œuvre d'un « système commun d'échange des données relatives aux visas », dénommé *« VIS – Visa Information System »*, devraient intervenir en juin, la Commission ayant d'ores et déjà déposé son étude de faisabilité. La structure du VIS devrait s'inspirer de celle retenue pour le SIS, le Système d'Information Schengen, dont la « deuxième génération » (le SIS – II) devrait comporter des données biométriques. Ce système d'échange d'informations en matière de visas entre les Etats membres, qui devrait concerner environ 10 millions de visas par an, voire un nombre plus important à terme en raison de l'élargissement, est destiné à la fois à lutter contre la fraude documentaire, à faciliter les contrôles aux frontières extérieures ou lors des contrôles d'immigration ou de police et contribuer au développement de la politique commune en matière de visas ainsi qu'à la lutte contre le terrorisme.

Surtout, le 27 février 2003, une déclaration commune franco-allemande sur l'utilisation de la biométrie a été adressée au Conseil JAI[53] afin d'améliorer les normes de sécurité des documents de voyage (passeports, visas et titres de séjour).

Cette déclaration insiste sur la nécessité d'introduire des normes d'utilisation de la biométrie reconnues au niveau international et de parvenir à une harmonisation entre les pays membres des modes d'utilisation des données biométriques pour ces documents.

A cette fin, la France et l'Allemagne ont demandé que le Conseil confie à la Commission le soin de préparer l'adaptation des instruments juridiques 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[54] et, pour le modèle uniforme de titre de séjour, le règlement du 13 juin 2002 n°1030/2002[55],

---

[53] Voir Annexe 6

[54] Lors de sa session du 20 septembre 2001, le Conseil avait reconnu l'importance de la sécurité documentaire en tant que moyen de lutte contre le terrorisme et mis l'accent sur les possibilités offertes par la biométrie. A la suite de ce conseil, la Commission avait présenté une nouvelle proposition de règlement modifiant le règlement de 1995 en matière de modèle uniforme de visa et prévoyant l'inclusion sur ce document d'une photographie digitale. Le Règlement (CE) n°334/2002 du 18 février 2002 modifiant le règlement 1683/95 prévoit l'insertion d'une photographie, le sixième considérant précisant que « l'insertion d'une photographie répondant à des normes de sécurité élevées constitue une première étape vers l'utilisation d'éléments établissant un lien plus fiable entre le modèle type de visa et son titulaire, ce qui contribue sensiblement à garantir que le modèle type de visa est également protégé contre une utilisation frauduleuse » et que « les spécifications du document 9303 de l'OACI sur les documents lisibles à la machine seront prises en considération ».

[55] Le sixième considérant dudit Règlement précise que « pour renforcer la protection des titres de séjour contre la contrefaçon et la falsification, les Etats membres et la Commission, examinent à intervalles réguliers, au fur et à mesure de l'évolution technologique, les changements à apporter dans les éléments de sécurité incorporés dans le titre, et notamment l'intégration et l'utilisation de nouveaux éléments biométriques ». L'article 4 du règlement dispose que *« le titre de séjour ne contient aucune information lisible à la machine, sauf dans les cas prévus à l'annexe du présent règlement ou si ces données figurent sur le document de voyage correspondant »*. L'annexe

relatif à l'élaboration uniforme d'un titre de séjour pour les ressortissants des pays tiers.

Concernant la sécurisation des passeports et des autres documents de voyage, la déclaration commune demande aux Etats membres d'examiner les conditions de modification de la résolution du Conseil du 17 octobre 2000 (2000/C 310/01)[56] en vue de parvenir à une harmonisation des normes ainsi que des techniques de production et de sécurisation des données, en suggérant que ces règles puissent également s'appliquer aux cartes d'identité, lesquelles peuvent être utilisées comme documents de voyage par les ressortissants communautaires ou en fonction d'accords particuliers par des ressortissants d'Etats tiers.

Dans le respect notamment de 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, des positions communes, propres à garantir la compatibilité des systèmes mis en place par les Etats membres et à leur donner la capacité de s'opposer à la fixation unilatérale de normes biométriques, devraient définir la ou les données biométriques retenues en complément de la photographie d'identité ainsi que les moyens de stockage et de lecture.

La déclaration propose, en outre, que les Etats membres mettent en place à court terme une coopération technique renforcée afin d'évaluer les différentes techniques et de disposer d'une « expertise commune indépendante et de qualité ».

Lors de son audition par la délégation pour l'Union européenne de l'Assemblée nationale le 29 avril dernier, M. Nicolas SARKOZY a indiqué que si les Allemands préféraient avoir recours à l'iris et les Français plutôt aux empreintes digitales, l'adoption de contrôles identiques restait essentielle.

En effet, alors qu'une harmonisation devrait être recherchée afin d'accroître l'efficacité des contrôles aux frontières, certains Etats membres plaident pour l'introduction sur une base unilatérale de données biométriques.

---

précise que le titre *« s'inspire des spécifications définies par l'OACI »*. L'article 9 du Règlement prévoit par ailleurs l'insertion d'une photographie dans le délai de cinq ans.

[56] Cette résolution définit des normes minimales de sécurisation qui doivent être introduites au plus tard le 1er janvier 2005 pour les passeports et le 1er janvier 2006 pour les cartes d'identité et les passeports valables à court terme ayant une validité de plus de six mois. Ces normes consistent notamment à intégrer les données personnelles y compris la photographie et la signature du titulaire dans les matériaux du document et à respecter les spécifications du document 9303 de l'OACI relatives à la lecture par machine de la page réservée aux données personnelles. Cette résolution n'a pas de valeur contraignante, à la différence des règlements sur les titres de séjour et les visas, les procédures d'adoption différant cependant selon l'objet desdits règlements (unanimité pour les titres dé séjour, majorité qualifiée pour les visas). Depuis le traité de Nice, les passeports relèvent de la compétence exclusive des Etats membres et des réflexions sont en cours pour faire entrer les éléments sécuritaires de ces documents dans les compétences européennes.

Cette position avait déjà conduit à écarter la question de l'insertion d'une donnée biométrique sur les permis de séjour en juin 2001.

Par ailleurs, lors de son audition par la Délégation pour l'Union européenne du Sénat, le 13 mars 2003, M. Nicolas SARKOZY, Ministre de l'intérieur, a indiqué que cette déclaration avait été bien accueillie par nos partenaires européens et par la Commission et précisé qu'avant l'été seraient introduits à l'aéroport de Roissy des dispositifs de lecture optique et biométriques, sur la base du volontariat des compagnies aériennes.

La question de la transmission aux Etats-Unis, voire à d'autres pays tiers tels que le Canada, l'Australie et la Corée, par les compagnies aériennes, d'informations relatives aux passagers et aux membres d'équipage, a montré les difficultés de concilier les exigences émanant de pays tiers mais aussi, le cas échéant, de pays membres et liées à la sécurité de leurs frontières, avec les principes définis au niveau communautaire pour assurer la protection des données personnelles.

Cette question ne concernait pas directement le transfert de données biométriques, du moins dans l'immédiat[57], mais diverses données d'identification telles qu'elles figurent notamment dans les passeports et certaines données « sensibles » telles que la religion ou les habitudes alimentaires des passagers. La transformation en obligation juridique, assortie de sanctions pour les compagnies aériennes, des transmissions organisées auparavant sur la base d'arrangements volontaires et leur élargissement résultaient des dispositions prises par les Etats-Unis (*Aviation and Transportation Security Act* et *Enhanced Border Security and Visa Entry Reform Act*) visant à renforcer la sécurité du territoire américain. Des négociations ont été engagées par la Commission, critiquée avec virulance au Parlement européen[58], tandis que certains Etats membres avaient pris l'initiative de négociations bilatérales avec les Etats-Unis.

Les enjeux économiques des réflexions menées aux Etats-Unis, au sein de l'OACI et dans le cadre de l'Union européenne sont considérables, tant pour les Etats qui sont prêts à supporter des dépenses importantes pour sécuriser les titres qu'ils délivrent et doivent contrôler que pour les producteurs de systèmes biométriques et de titres susceptibles de répondre à une telle demande.

---

[57] Néanmoins, à cette occasion, dans son avis 6/2002 du 24 octobre 2002, le Groupe « article 29 » sur la protection des données, après avoir rappelé que pour les Etats participant au « Visa Waiver Program », le transfert de données biométriques devrait être rendu obligatoire d'ici octobre 2004, a indiqué qu'un tel transfert était soumis aux dispositions de la directive 95/46/CE et a considéré que les identifiants biométriques « pourraient être visés » par la disposition de la directive qui « impose » aux Etats membres de déterminer les conditions de traitement de tout « identifiant de portée générale ».

[58] Proposition de résolution sur le transfert des données personnelles par les compagnies aériennes au service de l'immigration des Etats-Unis- B5-0157/2003, 12 mars 2003

2 - Le contexte économique international : le marché de la biométrie

Les acteurs économiques de la biométrie exercent une pression importante pour promouvoir leurs produits et s'organisent.

Il convient dès lors d'examiner les tendances de ce marché, la normalisation étant susceptible de jouer un rôle dans cette compétition.

Le marché de la biométrie est largement dominé par les sociétés américaines. Néanmoins, deux entreprises françaises disposent d'atouts incontestables : la SAGEM qui maîtrise la technologie de l'empreinte digitale avec son produit « Métamorpho » et qui se présente comme le leader mondial de l'empreinte digitale et des titres d'identité biométriques et THALES qui propose des solutions intégrées innovantes dans le domaine de la sécurisation des titres en utilisant notamment des procédés biométriques. Aussi paraît-il nécessaire de décrire les positions de ces deux sociétés dans le domaine étudié.

a) Une croissance annoncée

Diverses études sur le marché de la biométrie et ses perspectives d'évolution ont été produites, mais les estimations dans ce domaine varient considérablement, tant en ce qui concerne les analyses portant sur la situation actuelle que s'agissant des études prospectives. Néanmoins un double consensus se dégage : l'empreinte digitale constitue la technologie dominante et le marché de la biométrie connaîtra dans les prochaines années un développement important.

Que représente actuellement le marché de la biométrie ?

Les montants afférents à l'année 2001 sont extrêmement divergents : de l'ordre de 66 millions de dollars US pour les uns à 230 millions de dollars US pour les autres. Il en est de même des prévisions qui varient pour 2006 de 520 à 900 millions de dollars, représentant selon les sources une progression sur cinq ans de près de 100% à environ 1 400%, le chiffre d'un milliard de dollars US pour 2004 ayant par ailleurs été avancé, soit cinquante fois plus que celui estimé par l'organisme considéré en 2001 !

Et pourtant, les études disponibles n'ont apparemment guère anticipé les évolutions liées à la modernisation et l'harmonisation des instruments d'identification judiciaire dans la perspective d'une coopération renforcée des Etats, ni aux réflexions en cours sur les « titres biométriques ». Il est vrai toutefois que les analyses ne prennent pas toujours en compte les dispositifs biométriques à usage gouvernemental.

Une analyse datant de 2001 plaçait ainsi l'accès physique au premier rang des secteurs d'utilisation avec un taux de 42% et prévoyait une consolidation de ce domaine d'application. Elle annonçait un développement rapide de la biométrie dans les secteurs de l'informatique, des finances et des télécommunications, lesquels représentaient pour l'année considérée respectivement 25, 15 et 4% des domaines d'utilisation. En revanche, la justice (7%), l'immigration (1%), la santé (3%) et l'assistance sociale (1%) ne devaient pas constituer, selon cette étude, des secteurs prometteurs. Mais une autre étude effectuée deux ans plus tôt donnait un classement sensiblement différent, avec par ordre décroissant, le contrôle de l'accès physique (38%), l'ordre public (19%), les finances (17%), la santé (10%), l'immigration (5%), les prestations sociales (4%) à égalité avec la sécurité informatique et enfin les télécommunications (3%).

D'un point de vue géographique, la biométrie serait en outre deux fois moins implantée en Europe qu'en Amérique du Nord.

Les études portant sur la répartition des parts de marché selon les technologies ne sont pas non plus concordantes, même si l'empreinte digitale est unanimement reconnue comme la technique la mieux placée. Elles n'opèrent pas de distinction entre les grands systèmes d'identification largement dominés par l'empreinte digitale et les petits terminaux biométriques qui privilégient actuellement la technologie de la main, laquelle semble toutefois « vieillissante » et connaît un infléchissement de ses taux de croissance.

En 2001, l'empreinte digitale représentait 50% du chiffre d'affaires du secteur, suivie par la main (15%), le visage (12%), la voix (10%), la signature (8%) et l'iris (4%). Mais selon une autre étude (2002), basée sur les ventes de terminaux biométriques, une répartition différente était mise en évidence, la main représentant 27%, suivie de l'iris (15%), la face (13%), la signature (4%) et la voix (2%), tandis que 39% du marché étaient absorbés par l'empreinte digitale.

Le marché de la biométrie est ainsi difficile à appréhender dans sa globalité.

Lors de la vingt-troisième conférence internationale des commissaires à la protection des données personnelles qui s'est tenue à Paris, en septembre 2001, les chiffres suivants concernant le seul marché de l'empreinte digitale ont été donnés : le marché du traitement automatique de l'empreinte digitale représenterait à lui seul 250 à 500 millions de dollars, dont 150 à 200 millions pour les systèmes de lutte contre la criminalité, 50 à 100 millions pour les systèmes civils liés à la délivrance de titres et 35 à 100 millions pour les terminaux biométriques. Même limitée à une technologie particulière, les estimations manquent donc aussi de précision.

b) Les enjeux de la standardisation

On assiste actuellement dans le secteur de la biométrie à un large mouvement tendant à établir des normes et des standards et dont les enjeux sont à la fois politiques et économiques.

Il s'agit tout d'abord de normes de sécurité, sur la base des « critères communs » de sécurité des technologies de l'information qui font l'objet depuis 1999 d'une norme ISO (15 408) et qui définissent des exigences fonctionnelles et des exigences d'assurance. La consultation du site[59] qui sert de ressource internationale en la matière sans toutefois fournir une liste exhaustive, révèle ainsi que certains produits biométriques ont été soumis à cette évaluation. Tel est le cas de Bioscrypt[60] et d'Iridian[61], pour un niveau d'assurance EAL (*Evaluation Assurance Level*) 2, sur une échelle de un à sept. Parallèlement, divers travaux se poursuivent, notamment au sein du *Biometric Working Group* constitué au sein du CESG (*Communication Electronic Security Group*) du Gouvernement britannique, pour définir les conditions dans lesquelles les produits et systèmes biométriques doivent être testés sur la base des critères communs dans la perspective notamment de fournir des avis aux administrations britanniques souhaitant utiliser cette technologie.

Des normes de compatibilité et d'interface ont été par ailleurs élaborées pour faciliter l'utilisation des techniques biométriques et parvenir à l'interopérabilité des systèmes.

Beaucoup d'efforts ont d'ores et déjà été déployés ces dernières années dans les domaines de l'interface et de l'intégration (API – *Application Program Interface*). L' HAAPI (*Human Authentification Application Programmer Interface*) dont les spécifications ont été développées par le *National Registry Inc* sous contrat avec le Département de la Défense américain puis placées dans le domaine public et le BAAPI (*Biometric Authentification Application Programmer Interface*) sont ainsi largement adoptés[62]. Le BioAPI Consortium a proposé un standard générique qui a été approuvé le 13 février 2002 par l'ANSI.

Le CBEFF (*Common Biometric Exchange File Format*) a par ailleurs été publié par le NIST en janvier 2001. Il décrit les éléments nécessaires pour supporter les technologies biométriques dans une voie commune. Ce groupe a été sponsorisé par le NIST et le Biometric Consortium pour aboutir à un consensus sur un format commun des empreintes digitales puis sur une compatibilité avec les autres technologies. Cette norme a été retenue par l'OACI. En 2002, l'OASIS (*Organisation for the Advancement of Structured Information Standards*) a par

[59] www.commoncriteria.org
[60] *Bioscrypt Entreprise for NT Logon*, Version 2.1.3 a été certifiée en juin 2001.
[61] *Iridian Technologies Kno Who Authentification Server and Private ID* était pour sa part en cours d'évaluation en février dernier.
[62] F. DERAVI *op.cit.*

ailleurs constitué un groupe de travail chargé de définir les bases d'un langage de description des données et des fonctions biométriques reposant sur le langage XML (projet XCBF – *XML Common Biometric Format*).

Ces différents efforts visent à promouvoir les techniques biométriques en recherchant à la fois un consensus entre les professionnels et la confiance des utilisateurs. Parmi les différents utilisateurs potentiels, certains Etats tiennent une place particulière.

C'est ainsi qu'en 2002, les Chefs d'Etat présents au sommet du G8 se sont entendus pour travailler à formuler des recommandations sur les normes minimales régissant l'application 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 mis en évidence.

Dans ce domaine, une véritable stratégie de normalisation semble mise en œuvre aux Etats-Unis.

Depuis les évènements du 11 septembre 2001, des directives précises ont en effet été définies aux Etats-Unis afin d'aboutir rapidement, aux plans national et international, à l'élaboration de normes afin de doter les administrations américaines des moyens nécessaires pour assurer la sécurité intérieure du pays et lutter contre la fraude documentaire. Dans ce cadre, le NIST s'est vu confier un rôle moteur.

Il s'agit d'une politique volontariste visant à consolider et accélérer le processus engagé depuis plusieurs années aux Etats-Unis et marqué par la constitution en 1995 du *Biometric Consortium*, lequel est coprésidé par le NIST et compte aujourd'hui quelque 900 membres dont une soixantaine d'agences fédérales et dont les deux cinquièmes ne sont pas américains, puis par le développement en 1999 des spécifications BioAPI adoptées par l'ANSI-INCITS au plan national et par l'élaboration, en collaboration avec la NSA et le NIST, du CBEFF, approuvé également par l'ANSI.

Cette politique s'est traduite notamment sur le plan budgétaire, plusieurs millions de dollars étant alloués au projet national de sécurité biométrique[63], et par la création de structures adaptées capables de porter les projets de standardisation aux niveaux national et international, avec la constitution d'un groupe de travail (*Biometric Interoperability, Performance and Assurance Working Group*) associant le NIST et le *Biometric Consortium*, l'institution en novembre 2001 d'un groupe biométrie (M1) au sein de l'INCITS (*InterNational Committe for Information Technology Standards*) puis celle, au sein du comité ISO/CEI des technologies de l'information (JTC1), d'une sous-commission biométrie (SC37) dont la première réunion s'est tenue le 4 décembre 2002 et dont la présidence est assurée par le NIST, un lien organique étant par

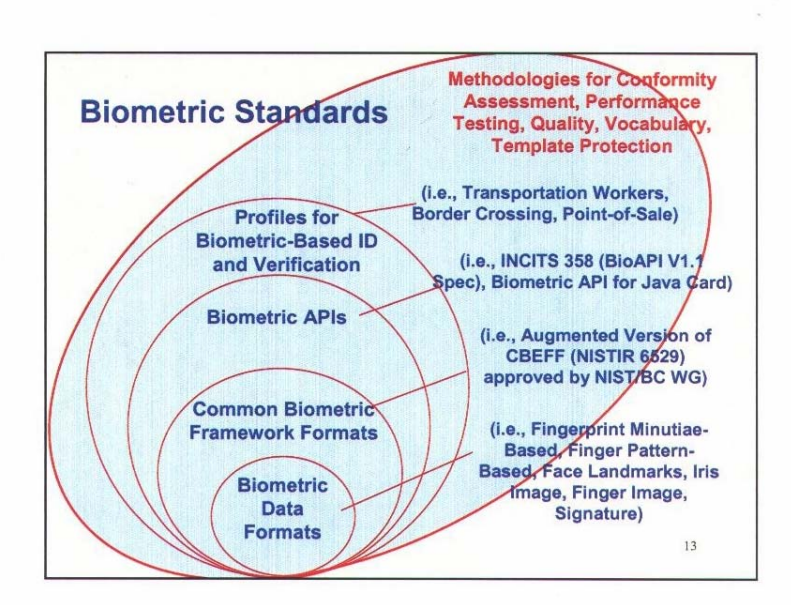
[63] Pour 2003, une enveloppe de 15 millions de dollars a été prévue.

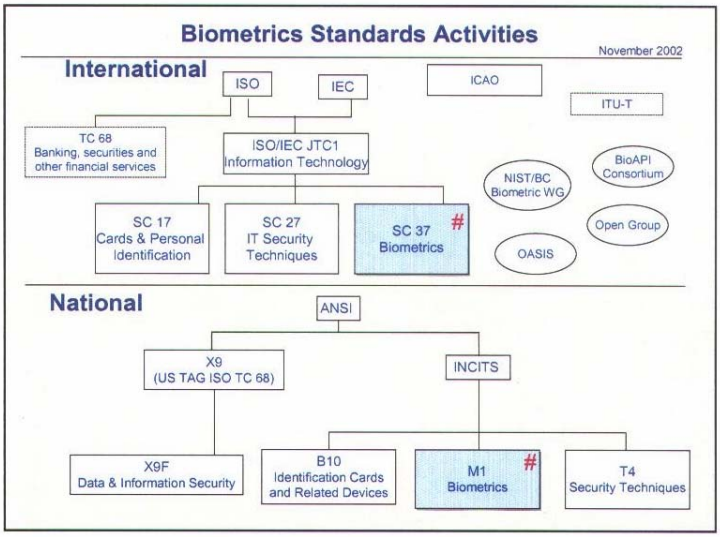
ailleurs établi entre le groupe M1 au niveau national et la sous-commission 37 au niveau international puisque le groupe M1 constitue l'organe technique américain (TAG-*Technical Advisory Group*) pour la sous-commission 37.

Tant au niveau national qu'au plan international, une synergie est recherchée entre le domaine de la biométrie désormais individualisé au sein des organisations de standardisation et les domaines de la sécurité informatique d'une part ainsi que des techniques d'identification personnelles en particulier des cartes d'autre part.

Les objectifs assignés au niveau national répondent aux préoccupations du gouvernement américain : il s'agit tout d'abord de faciliter les échanges et l'interopérabilité des systèmes biométriques, quels que soient les technologies utilisées (empreinte digitale, face, iris, signature) et les fournisseurs de celles-ci pour éviter que les utilisateurs ne soient dépendants des systèmes propriétaires, mais aussi d'harmoniser les méthodes et les principes d'évaluation des performances et de déterminer les outils nécessaires pour assurer la sécurité des frontières.

Les tableaux suivants, conçus par le NIST, permettent ainsi d'identifier les éléments de la « stratégie » américaine de normalisation.





Il convient également de noter qu'au Japon une association , dont votre Rapporteur a rencontré les responsables, regroupe pouvoirs publics et industriels afin de rechercher la mise en œuvre de normes communes

c) Présentation de deux entreprises françaises : SAGEM et THALES

En France, plusieurs sociétés, généralement spécialisées dans le contrôle d'accès physique et logique, proposent des solutions biométriques d'authentification, comme par exemple Agma Morpho, Vigivision, Zalix biométrie ou Zefyr tech, mais la mise en œuvre du concept d'identification des personnes à partir des données biométriques reste l'apanage de deux groupes.

Le Groupe **SAGEM** comporte deux branches, la branche Communication (téléphones mobiles, terminaux et Internet, réseaux et optiques) et la branche Défense (aéronautique et défense, sécurité). Son chiffre d'affaires s'élève à trois milliards d'euros, dont les deux tiers au titre de la branche Communication.

Au sein de la Branche Défense, le pôle « sécurité », qui regroupe les systèmes d'identification, les cartes et les terminaux, représente un chiffre d'affaires de 300 millions d'euros et le dixième du chiffre d'affaires du groupe. Le rachat du produit « Morpho » reposant sur l'empreinte digitale par la SAGEM en 1993 explique largement le succès de ce pôle.

Dans le secteur de l'empreinte digitale, la SAGEM occupe une place dominante au plan mondial.

C'est le cas pour les systèmes de traitement automatique d'empreintes digitales de lutte contre la criminalité (AFIS- *Automatic Fingerprint Identification*

Systems), compte tenu notamment des références dont elle peut se prévaloir (FBI, Interpol, diverses polices nationales). Sur ce segment, la SAGEM doit affronter la concurrence d'autres sociétés qui également commercialisent, installent et développent ces AFIS, telles que les sociétés NEC, MOTOROLA, LOOCKEED-MARTIN ou COGENT.

C'est aussi le cas pour les systèmes civils utilisant l'empreinte digitale dans le domaine de la délivrance et de la gestion des titres, la SAGEM intervenant en tant que producteur d'AFIS ou en offrant une prestation intégrée de fabricant d'AFIS et de production de titres sécurisés. Dans ce domaine la SAGEM a remporté de nombreux appels d'offres.

C'est enfin le cas des terminaux biométriques, la SAGEM ayant pénétré dans ce marché depuis quatre années environ.

De nombreuses réalisations peuvent ainsi être citées : quatre Etats européens ont choisi une solution SAGEM pour collecter, transmettre et traiter les données dans le cadre du système EURODAC, l'identification des populations du Kosovo sous l'autorité de l'ONU, les cartes d'identité du Liban, les cartes électroniques du citoyen délivrées dans les Emirats Arabes Unis, la gestion des pensions aux Philippines et en Afrique du Sud, la carte d'identité multifonctions délivrée en Malaisie, les cartes d'identité en cours dans différents Etats africains tels que la Namibie, le Nigeria, la Mauritanie ou la Côte d'Ivoire comme la gestion des prestations sociales et des permis de conduire de plusieurs Etats d'Amérique du Nord reposent sur la technologie mise en œuvre par SAGEM.

S'agissant du contrat conclu avec le ministère de l'intérieur des Emirats Arabes Unis pour la maîtrise d'œuvre, la conception, l'intégration et le déploiement sur vingt-deux sites régionaux, d'un système contrôlant la délivrance, la fabrication et l'usage de plusieurs millions de cartes électroniques d'identité et de résidents, pour un montant de 50 millions de dollars, la proposition de la SAGEM a été retenue en mars 2003 dans le cadre d'un appel d'offres international auquel avaient soumissionné douze intégrateurs.

A la fin de l'année dernière la SAGEM a racheté 10% de GEMPLUS, premier fournisseur mondial de solutions basées sur la carte à puce et, en février 2003, un accord de coopération a été conclu entre la SAGEM et GEMPLUS, en vue de développer ensemble leurs activités dans le domaine des cartes d'identité sécurisées. En outre, un accord stratégique a été négocié entre SAGEM et IRIDIAN TECHNOLOGIES INC. qui détient les brevets exclusifs sur la technologie de la reconnaissance de l'iris. Enfin, en mai dernier un autre accord stratégique a été négocié avec COGNITEC SYSTEMS qui maîtrise la technologie de la reconnaissance faciale.

THALES, dont le chiffre d'affaires atteint plus de 10 milliards d'euros et dont 32,6% des actions sont détenues par l'Etat français, a développé ses activités d'identification au sein du pôle Technologies de l'information et

services, lequel représente 26% du chiffre d'affaires, à côté des pôles Aéronautique (18%) et Défense (56%) et couvre plusieurs unités centrées sur la notion de sécurité (transactions bancaires, communications/cryptographie, contrôles d'accès de sites physiques, cartes à puce…). Les activités d'identification représentent actuellement 27 millions d'euros.

Dans le domaine de la délivrance de titres d'identité de nombreuses réalisations ont été assurées par THALES tant en France (carte nationale d'identité, titres de séjour des étrangers) que dans d'autres pays européens tels que l'Espagne (carte nationale d'identité), la Pologne (permis de conduire), le Kosovo (carte d'électeur) ou la République tchèque (passeport et carte nationale d'identité) et sur d'autres continents, notamment aux Etats-Unis, mais aussi en Chine où a été mise en œuvre une unité de production de cartes à puce sans contact.

S'agissant plus spécifiquement de la biométrie, THALES a fourni à deux pays africains, le Kenya et la Namibie, des systèmes complets pour la gestion de titres (cartes nationales d'identité, titres de séjour et cartes de réfugiés avec empreintes digitales et photographies numérisées pour l'un, permis de conduire avec saisie de la photographie et de l'image de la signature ainsi que codification des empreintes digitales pour l'autre).

Dans le domaine de la sécurisation des titres, deux nouveaux concepts sont mis en œuvre : le principe de l'association machine/consommable destiné à éviter les falsifications et la technologie de « l'hologramme temps réel » qui est un hologramme personnalisé. Il s'agit d'introduire dans les titres, outre la photographie et les données biométriques du titulaire, un hologramme de la photographie associée au nom de l'intéressé qui permettrait un contrôle visuel de premier niveau plus sûr, l'image holographique étant unique et comportant un fond spécifique généré en usine et au premier plan une image (la photographie du titulaire) et un texte (le nom et le prénom du titulaire) personnalisés.

A la différence des Etats-Unis, la France n'a pas encore élaboré une véritable politique industrielle de la sécurité et les réflexions menées par les différentes administrations, les experts et les producteurs français restent extrêmement dispersées et généralement sectorisées.

Alors que le Gouvernement français développe au sein de l'Union européenne et du G8 une politique volontariste dans le domaine de la biométrie, les atouts scientifiques et technologiques français sont insuffisamment valorisés.

C'est ainsi notamment que la France n'est pas représentée au sein du *Biometrics Working Group* britannique qui travaille activement et qui compte parmi ses membres des représentants des gouvernements allemand, néerlandais et italien. Il en est de même au niveau européen, en ce qui concerne les comités techniques mis en place pour lutter contre la fraude documentaire.

De façon générale, la France semble ainsi sous représentée dans les différentes instances techniques chargées de mettre en œuvre concrètement les orientations définies par les Etats.

Par ailleurs, les travaux de recherche et d'évaluation restent éclatés et trop spécialisés, alors qu'une vision pluridisciplinaire s'avère nécessaire. Les projets européens développés depuis 1994 ont porté ainsi essentiellement sur la reconnaissance vocale et la reconnaissance multimodale associant la voix et le visage. Néanmoins, des initiatives intéressantes ont émergé depuis peu, telles que, par exemple, le projet initié par l'Institut national des télécommunications reposant sur une approche globale qui prendrait en compte les aspects techniques, pratiques et sociaux des systèmes biométriques d'authentification.

L'audition publique que votre Rapporteur a organisée met ainsi en évidence la nécessité d'instituer un lieu d'échanges entre les différentes parties prenantes en assurant l'information du public sur les débats en cours.

Conclusion

Au terme de l'étude confiée à votre Rapporteur par l'Office parlementaire d'évaluation des choix scientifiques et technologiques, une série de constats peuvent être dressés.

Les recherches et les travaux d'évaluation sont actuellement très fragmentés et la plupart des pays européens, dont la France, ont pris dans ce domaine un certain retard.

Ces travaux exigent, pour être conduits dans des conditions satisfaisantes, à la fois la mobilisation d'experts compétents et indépendants, des financements adéquats et un minimum de collaboration de la part tant des industriels naturellement attachés à protéger les brevets qu'ils détiennent que des utilisateurs disposant de larges bases de données biométriques déjà constituées. La confidentialité des données et le secret des affaires militent ainsi pour la formation d'équipes présentant des garanties déontologiques et techniques.

Il apparaît aussi nécessaire d'y associer plus étroitement des experts médicaux qui détiennent les connaissances les plus approfondies sur la constitution et l'évolution du corps humain et sont les mieux placés pour apprécier les effets sur la santé de certaines techniques d'observation de parties de ce corps.

Les besoins d'identification et d'authentification sont par ailleurs multiples, comme au demeurant les moyens susceptibles de les satisfaire, et ils seront de plus en plus intensément ressentis dans certains domaines, tant sur le plan collectif qu'individuel, comme en témoignent par exemple les réflexions en cours sur la fraude documentaire.

Les enjeux politiques, sociaux et économiques de cette évolution sont importants et appellent une réflexion globale, à laquelle le Parlement doit participer, pour garantir l'efficacité des moyens mis en œuvre, comme pour réguler les implications des dispositifs choisis.

A cet égard, votre Rapporteur estime que la publication du rapport et l'organisation, le 15 mai dernier, de l'audition publique sur les méthodes d'identification des personnes à partir des données biométriques révèlent l'intérêt d'une telle participation en mettant en évidence la nécessité d'assurer une meilleure collaboration des différents acteurs, tant publics que privés, et une plus grande transparence vis-à-vis du public.

Aussi, les recommandations préconisées s'articulent-elles autour de ces deux principes fondamentaux.

Voir la suite du rapport