LIVRE BLANC
DU GROUPE DE TRAVAIL SUR LES BIOMETRIES

16 mai 2011

(Confidentiel)

ALAIN BENSOUSSAN

TABLE DES MATIERES

PREFACE

A l'heure où le Tribunal de grande instance de Paris rend la première décision en matière de biométrie, décision au sein de laquelle le principe de précaution est préféré au droit à l'expérimentation, les réflexions du groupe de travail sur la biométrie ainsi que le présent livre blanc et la « Charte des biométries » trouvent pleinement leur sens.

Dans un monde où la sécurité milite en faveur du développement des techniques de biométrie, à l'heure où les Etats se sont tous lancés dans des programmes de déploiement de titres d'identité biométriques, il importe que ces technologies ne soient pas victimes d'un risque liberticide non démontré et que l'on évite de considérer l'interdit comme le seul moyen d'évier le danger.

Pendant près d'un an, industriels et utilisateurs se sont réunis pour mieux comprendre les enjeux juridiques de la biométrie.

Ces travaux ont donné lieu à la rédaction du présent livre blanc et de la Charte des biométries qui ne sont que les premières étapes d'une réflexion indispensable au développement de la biométrie.

Charles Copin Alain Bensoussan

1. INTRODUCTION

La biométrie est longtemps restée confinée à des secteurs d'activité privilégiant la mise en place de politiques de sécurité forte comme ceux liés au nucléaire, à l'aéroportuaire ou encore à la chimie.

Les attentats terroristes de septembre 2001 ont incontestablement joué un rôle d'impulsion du développement de la biométrie et de son extension au grand public.

Les Etats-Unis, en imposant aux autres Etats l'adoption de passeports et de documents de voyage intégrant des identifiants biométriques, privilégient une mise en place rapide de ces nouveaux moyens d'identification basés sur les caractéristiques physiques intrinsèques aux personnes que sont les solutions biométriques et obligent les Etats à se mettre en conformité bon gré, mal gré avec ces obligations.

Plutôt que « la » biométrie, il est plus juste d'évoquer « les » biométries que l'on peut d'ailleurs distinguées selon deux typologies : une typologie technique et un typologie par finalité.

La typologie technique permet de distinguer plus de quinze techniques de biométrie différentes et parmi celles-ci d'identifier des sous-catégories en fonction de celles qui laissent des traces et de celles qui n'en laissent pas, mais aussi en fonction du caractère comportemental ou non de la technologie.

La typologie par finalité permet, elle, de distinguer la biométrie sécuritaire de la biométrie de confort sans qu'elles soient nécessairement exclusives l'une de l'autre.

La biométrie est un secteur en pleine mutation porté par des projets nationaux, européens ou internationaux

Ainsi l'Union européenne se dote d'un règlement novateur qui encadre depuis décembre 2004 la mise en place en son sein de passeports et documents de voyage sur lesquels seront stockés la photo numérisée et les empreintes digitales de leur titulaire.

La France, pour sa part, a lancé un programme dénommé « INES[1] » ayant pour objectif, à l'horizon 2006, la mise en place de cartes d'identité électroniques sécurisées intégrant les mêmes éléments biométriques que ceux utilisés pour les passeports européens.

Si le développement des biométries est une réalité, son environnement juridique est encore balbutiant.

[1] Identité Nationale Electronique Sécurisée.

Au niveau national, la loi informatique et libertés modifiée en 2004 prend en compte pour la première fois les données biométriques et encadre le traitement qui pourrait en être fait. Au niveau européen, le règlement relatif à la mise en place de passeports biométriques constitue le premier texte encadrant la mise en œuvre d'une solution biométrique. Au plan international aucun texte ne prévoit un tel encadrement juridique, mais l'Organisation de l'Aviation Civile Internationale a élaboré un ensemble de normes relatives à l'utilisation de systèmes de reconnaissance biométrique dont s'inspire les Etats dans l'élaboration de leur réglementation.

La biométrie est à tel point importante que plusieurs autorités ou organismes se sont saisis de la question et ont fait valoir leur propre analyse qu'il s'agisse de l'OCDE, du Conseil de l'Europe[2], de l'Union européenne, ou encore du parlement français à travers le rapport sur les méthodes scientifiques d'identification des personnes à partir des données biométriques et techniques de mise en œuvre, plus connus sous le nom de rapport Cabal du nom du député Christian Cabal, auteur dudit rapport.

Ces rapports s'enquièrent tous de l'usage des biométries, de la nécessaire régulation ou non du secteur et proposent les uns ou les autres recommandations et suggestions[3].

Au niveau de l'Union européenne, la commission des libertés civiles, de la justice et des affaires intérieures a édité un rapport[4] relatif à la mise en œuvre de solutions biométriques dans la société, partant du postulat que la biométrie va se développer et passer d'une utilisation par les pouvoirs publics à une utilisation civile et commerciale de masse.

Le rapport fait état de plusieurs recommandations :

- la finalité des applications biométriques doit être clairement définie ;
- la biométrie doit être utilisée pour renforcer la protection de la vie privée et permettre d'authentifier les personnes sans révéler leur identité ;
- une industrie biométrique européenne dynamique doit être encouragée ;
- des procédures de secours en cas de faille des solutions biométriques doivent être prévues ;
- la recherche doit se poursuivre dans les domaines du développement technologique, des systèmes biométriques multimodaux et des essais biométriques à grande échelle.

[2] Rapport d'étape sur l'application des principes de la convention 108 à la collecte et au traitement des données biométriques, Comité consultatif de la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (T-PD), Conseil de l'Europe, 2-4 février 2005. Les conclusions de ce rapport sont présentées en annexe du présent livre blanc.

[3] Le député Christian Cabal dans son rapport de l'Office parlementaire d'évaluation des choix scientifiques et technologiques sur les méthodes scientifiques d'identification des personnes à partir des données biométriques et les techniques de mise en oeuvre , n° 938, Assemblée nationale, n° 355, Sénat, juin 2003, propose notamment quatre recommandations qui sont reprises en annexe du présent livre blanc.

[4] Biometrics At the Frontiers : Assessing the impact on Society – For the European Parliament Committee on Citizens, Freedoms and rights, Justice and Home Affairs (LIBE), European Commission, 2005.

Le rapport analyse également les aspects juridiques relatifs à la biométrie. A ce titre il précise que le cadre juridique actuel s'il permet une utilisation commerciale des données personnelles n'est pas assez normatif et ne contient que peu d'éléments relatifs aux questions d'éthique. Il insiste également sur le fait que l'utilisation de la biométrie à titre de preuve judiciaire nécessite d'être réglementée.

Le rapport de l'OCDE relatif aux technologies biométriques[5] a quant à lui pour objet d'étudier les différentes technologies biométriques et d'analyser les problématiques liées à leur développement, notamment en ce qui concerne la protection de la vie privée. Le rapport rappelle que le développement des technologies biométriques est envisagé comme une possible résolution des problèmes liés au développement de la criminalité et du terrorisme. La biométrie serait une méthode de preuve ultime d'identification.

Ce rapport identifie les différentes techniques biométriques existantes et donne des exemples d'utilisations de celles-ci. Il étudie également l'efficacité et la performance des différentes technologies biométriques et explique le fonctionnement du système de mesure de performance des technologies biométriques. Enfin, ce rapport rend compte du développement économique du marché de l'industrie biométrique.

L'OCDE formule des recommandations relatives au développement du secteur de la biométrie. A ce titre, il indique qu'il est impératif d'encourager et de promouvoir le développement de technologies, de techniques et de méthodologies favorisant le respect de la sécurité et de la vie privée des personnes.

Face à cet intérêt nouveau pour les biométries, les industriels et utilisateurs de la biométrie ont jugé opportun de ne pas être écartés du débat et ont décidé de se réunir afin de réfléchir aux problématiques de la biométrie et de proposer des solutions adaptées à leur réalité technique et juridique actuelle.

Le groupe de travail sur les biométries regroupe des industriels du secteur bancaire, des industriels spécialisés dans les transactions et moyens de paiement sécurisés intéressés par la biométrie de sécurité, des industriels spécialisés dans l'ingénierie et le développement technologique, des industriels du secteur des télécommunications, des professionnels du consulting intéressés par la biométrie de sécurité mais également par la biométrie de confort et des organismes privés et publics directement ou indirectement concernés par les multiples développements de ces nouvelles techniques.

Le groupe de travail s'est attaché à analyser les problématiques juridiques et techniques posées par les biométries et à apporter des réponses qui soient à la fois pragmatiques, non liberticides et soucieuses de préserver le développement d'un secteur économique en pleine expansion.

[5] Organisation de Cooperation et de Développement Economiques, « Biometric-based technologies », Directorate for science, technology and industry, Committee for information, computer and communications policy, Working party on information security and privacy, 23 décembre 2004.

2. LE GROUPE DE TRAVAIL

Le groupe de travail sur les biométries, co-présidé par Charles Copin et Alain Bensoussan, ouvert à toute personne, réunit des professionnels, industriels ou utilisateurs des biométries.

Il se fixe comme objectif d'être un observatoire de la biométrie et de mettre en place une charte des biométries évolutive au regard du développement du cadre juridique de la biométrie.

Une présentation des membres du groupe de travail est annexée au présent livre blanc.

Les travaux du groupe de travail se sont organisés en réunions mensuelles aux cours desquelles des thématiques prédéfinies ont été étudiées au titre desquelles :

- la définition de la biométrie ;
- le référentiel légal dédié et le référentiel légal générique de la biométrie ;
- les notions d'identification et d'authentification ;
- les problématiques de responsabilités et de garanties ;
- la problématique de la propriété ;
- la problématique informatique et libertés et ;
- la problématique propre au déploiement des biométries dans l'entreprise et de droit du travail.

Ces réunions ont permis au groupe de travail d'analyser ces différentes problématiques et le cas échéant d'adopter une position de principe.

Ces travaux ont permis la rédaction du présent « livre blanc des biométries » destiné à exposer les réflexions du groupe de travail.

Le livre blanc lui-même est complété d'une charte des biométries qui, en forme de synthèse, précise les engagements mais également les recommandations des industriels et des utilisateurs des biométries.

3. DEFINITION DE LA BIOMETRIE

A titre liminaire, il est apparu indispensable de s'entendre sur le terme de biométrie qui, à lire les rapports d'ores et déjà publiés sur le sujet n'est pas apprécié de manière homogène.

Différentes définitions du terme « biométrie » ont pu être élaborées dans les différents rapports susvisés, mais il n'existe aucune définition légale à ce jour.

Ainsi, la Cnil a défini, dans ses rapports d'activités, les systèmes biométriques comme étant « des applications permettant l'identification automatique ou l'éligibilité d'une personne à se voir reconnaître certains droits ou services (notamment l'accès) basés sur la reconnaissance de particularités physiques (empreinte digitale, iris de l'œil, contour de la main...), de traces (ADN, sang, odeurs) ou d'éléments comportementaux (signature, démarche) »[6].

L'OCDE[7] pour sa part rappelle que la biométrie viendrait du grec « bio » (vie) et « métrie » (mesure) et insiste sur le fait que, bien que la biométrie ait été définie comme étant l'utilisation automatique de caractéristiques physiologiques ou comportementales pour déterminer ou vérifier l'identité, il paraît important d'insister sur le fait qu'il ne s'agit pas tant d'utilisations automatiques que d'utilisations « automatique-assistées », l'identification finale relevant en général d'une décision humaine. L'OCDE insiste également sur le fait que la biométrie se limite à l'étude de caractéristiques humaines uniquement.

Enfin, l'OCDE définit le « système biométrique » comme incluant tous les équipements informatiques, logiciels associés, progiciels et composants de réseaux requis pour permettre l'enrôlement biométrique final et le procédé d'appariement.

La Commission européenne, dans un rapport[8] récent relatif à la biométrie, définit le terme d'indicateur biométrique comme étant « une caractéristique physique ou biologique d'une personne pouvant être mesurée et utilisée à des fins d'identification automatisée ou semi-automatisée ».

Elle présente l'identification biométrique, quant à elle, comme « une technique qui utilise des caractéristiques biométriques pour identifier des êtres humains ».

Le groupe de travail après avoir analysé et apprécié chacune de ces définitions a jugé opportun de définir et préciser le périmètre de son étude et de proposer une définition.

[6] 22ème rapport d'activité de la Cnil, 2001, p. 157.

[7] OCDE, « Biometric-based technologies », Directorate for science, technology and industry, Committee for information, computer and communications policy, Working party on information security and privacy, 23 décembre 2004.

[8] « Biometrics at the Frontiers : Assessing the Impact on Society – For the European Parliament Committee on Citizens Freedoms and Rights, Justice and Home Affaires (LIBE), European Commission.

3.1 COMPOSANT « BIO »

Il importe à titre premier de s'interroger sur le sens du terme « bio » qui peut être appréhendé selon trois approche :

- une approche génétique ;
- une approche interne ou externe au corps humain ;
- une approche statique ou dynamique.

Le groupe de travail considère que le fait d'inclure la génétique dans la définition de la biométrie pourrait avoir des conséquences négatives et particulièrement difficile à maîtriser et ce d'autant plus qu'il semble exister une distinction technique entre le monde de la génétique et le monde de la biométrique.

Le fait d'inclure des éléments génétiques dans la biométrie induirait une appréciation émotionnelle et éthique majeure rendant de fait son développement extrêmement complexe et délicat pour ne pas dire quasiment impossible.

Compte tenu de cette réflexion, le groupe de travail décide d'écarter la génétique de la définition de la biométrie.

L'approche interne ou externe au corps humain repose sur la question de savoir si la biométrie s'intéresse aux seules caractéristiques externes d'un individu ou inclut des éléments internes.

Certains éléments du corps humain utilisés dans le cadre de la biométrie tels le réseau veineux sont des éléments considérés comme « internes ».

Le groupe de travail considère que la biométrie peut intégrer la solution dite interne sous réserve qu'elle ne soit ni intrusive ni ne viole l'intégrité du corps humain.

Cette limitation trouve son fondement dans le respect des droits de l'Homme et de la dignité humaine, selon lesquels l'intervention sur le corps humain d'une personne est interdite sans son consentement sauf en cas de besoin vital.

A l'instar de la réglementation relative à l'utilisation du fichier national des empreintes génétiques, le fait d'inclure un élément intrusif au corps humain dans le champs de la définition de la biométrie aurait pour conséquence immédiate d'imposer le respect de la réglementation relative à l'intégrité du corps humain.

Enfin s'agissant de l'approche statique ou dynamique, la biométrie repose sur des éléments statiques du corps humain, comme l'empreinte digitale, l'iris, ou de manière générale, tout élément biologique ou physique du corps humain utilisé dans le cadre de techniques de reconnaissance biométrique.

A ces éléments s'ajoutent ceux qui peuvent être qualifiés de dynamiques ou cinématiques et impliquent un mouvement du corps humain identifiable et mesurable. Tel est notamment le cas de la signature dynamique, de la frappe du clavier ou encore de la démarche.

Au vu de ces différentes approches, une définition plus précise du composant « bio » peut être élaborée comme comportant les éléments suivants :

- ensemble d'informations du corps humain non intrusifs à l'individu ;
- à l'exclusion des éléments génétiques ;
- et incluant des caractéristiques comportementales de l'individu.

3.2 COMPOSANT « METRIE »

Il est également apparu nécessaire d'apprécier le terme « métrie » en s'interrogeant sur le fait de savoir si cet élément restreint la biométrie aux seuls systèmes automatiques d'identification.

Une réponse affirmative exclurait du champ de la biométrie la reconnaissance d'une photographie par un contrôle final humain.

En conséquence, la « métrie » doit être considérée comme tout système mettant en oeuvre de la reconnaissance fondé, non seulement sur la mesure par des moyens techniques, mais également par des moyens humains.

Le groupe de travail propose ainsi une définition du composant « métrie » comme suit :

- « la métrie permet l'identification ou l'aide à l'identification par des systèmes automatiques et/ou des moyens humains ».

4. REFERENTIEL LEGAL

Le référentiel légal dédié peut généralement être différencié du référentiel légal générique, le premier s'entendant de l'ensemble de la réglementation faisant référence directe à la biométrie et le second, de la réglementation générique applicable à la mise en place d'un système biométrique.

Le référentiel légal dédié à la biométrie est encore peu développé mais même à l'état embryonnaire il est primordial de le maîtriser.

A côté du référentiel légal dédié se situe le référentiel légal générique qui comprend notamment le droit social, le droit des contrats, le droit relatif à la signature électronique et à la preuve, le droit relatif à la sécurité des données, le droit des assurances, ou encore la réglementation relative à la cryptologie.

4.1 REFERENTIEL LEGAL DEDIE

Le référentiel dédié à la biométrie est encore peu développé à l'heure actuelle. Le premier texte national mentionnant la biométrie datant seulement de 2004 est issu de la modification de la loi Informatique et libertés. Fin 2004, un décret est venu compléter ce référentiel légal national pour réglementer la création à titre expérimental d'un traitement de données à caractère personnel relatives aux ressortissants étrangers sollicitant la délivrance d'un visa.

Depuis lors, un règlement européen relatif aux passeports biométriques a été adopté et le projet national relatif aux cartes d'identité et passeports biométriques a été mis en oeuvre.

Ces premières réglementations font notamment suite aux travaux de l'Organisation de l'aviation civile internationale sur l'établissement de standards relatifs à la biométrie et au rapport de l'OCDE sur les techniques biométriques.

4.1.1 Référentiel légal dédié national

4.1.1.1 Loi 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée par la loi 2004-801 du 6 août 2004

2004 a vu la naissance de la première réglementation nationale relative aux données biométriques.

La loi Informatique et libertés modifiée pour transposer la Directive européenne 95 /46/CE encadre désormais le traitement de données biométriques.

Les articles 25 et 27 de la loi modifiée prévoit les conditions de la mise en œuvre de traitements de données biométriques en ce qui concerne l'obligation d'autorisation des traitements à la Cnil.

L'article 25 prévoit :

- « I. - Sont mis en oeuvre après autorisation de la Commission nationale de l'informatique et des libertés, à l'exclusion de ceux qui sont mentionnés aux articles 26 et 27 :

1° (…) ;
8° Les traitements automatisés comportant des données biométriques nécessaires au contrôle de l'identité des personnes.

II. - Pour l'application du présent article, les traitements qui répondent à une même finalité, portent sur des catégories de données identiques et ont les mêmes destinataires ou catégories de destinataires peuvent être autorisés par une décision unique de la commission. Dans ce cas, le responsable de chaque traitement adresse à la commission un engagement de conformité de celui-ci à la description figurant dans l'autorisation.

III. - La Commission nationale de l'informatique et des libertés se prononce dans un délai de deux mois à compter de la réception de la demande. Toutefois, ce délai peut être renouvelé une fois sur décision motivée de son président. Lorsque la commission ne s'est pas prononcée dans ces délais, la demande d'autorisation est réputée rejetée.

L'article 27 prévoit :

- « I. - Sont autorisés par décret en Conseil d'Etat, pris après avis motivé et publié de la Commission nationale de l'informatique et des libertés :
1° (…)
2° Les traitements de données à caractère personnel mis en oeuvre pour le compte de l'Etat qui portent sur des données biométriques nécessaires à l'authentification ou au contrôle de l'identité des personnes.

Sur ce point, il est renvoyé à la partie du Livre blanc consacrée à la réglementation des traitements de données biométriques.

4.1.1.2 Décret n° 2004-1266 du 25 novembre 2004 portant création à titre expérimental d'un traitement automatisé des données à caractère personnel relatives aux ressortissants étrangers sollicitant la délivrance d'un visa[9].

Une expérimentation d'une durée de deux ans a été mise en place dans sept consulats qui vise, afin de faciliter l'authentification des détenteurs de visa aux frontières, à intégrer les images numérisées de la photographie et les empreintes digitales des dix doigts des demandeurs de visas dans un support de stockage associé au visa demandé.

Ce support de stockage pourrait prendre la forme d'une puce sans contact et devrait dans ce cas faire l'objet de mesure de sécurités suffisantes contre les risques d'intrusion et de détournement.

[9] Décret n° 2004-1266 du 25 novembre 2004 pris pour l'application de l'article 8-4 de l'ordonnance no 45-2658 du 2 novembre 1945 relative aux conditions d'entrée et de séjour des étrangers en France et portant création à titre expérimental d'un traitement automatisé des données à caractère personnel relatives aux ressortissants étrangers sollicitant la délivrance d'un visa.

Le décret du 25 novembre 2004 prévoit que cette expérimentation doit avoir pour finalité de « mieux garantir le droit au séjour des personnes en situation régulière et de lutter contre l'entrée et le séjour irrégulier des étrangers en France, en prévenant les fraudes documentaires et les usurpations d'identité et en améliorant la vérification de l'authenticité des visas ainsi que de l'identité des étrangers lors des contrôles aux frontières extérieures des Etats partis à la convention signée à Schengen le 19 juin 1990, aux points de contrôle français mentionnés » par le décret.

Le décret prévoit en outre une durée de conservation des données ainsi collectées de deux ans pour les demandes de visas uniformes de court séjour et de cinq ans pour les demandes de visas long séjour et les refus de visas.

Les droits d'accès et de rectification prévus par la loi du 6 janvier 1978 pourront être exercés auprès du ministre des affaires étrangères, du ministre de l'intérieur, et de la chancellerie consulaire ou du consulat où la demande de visa est déposée. Il n'est par contre pas offert aux demandeurs de visas la possibilité d'user de leur droit d'opposition à ce traitement.

4.1.2 Un référentiel légal national en devenir, le programme INES

Le programme INES - Identité Nationale Electronique Sécurisée – a fait l'objet d'une présentation officielle par le Ministère de l'intérieur, de la sécurité intérieur et des libertés locales le 1er mars 2005.

Ce projet est présenté comme visant la mise en place de passeports et cartes d'identité biométriques au plan national.

Il a parmi ses objectifs, celui de « délivrer des titres hautement sécurisés conformes aux exigences internationales » et « d'offrir aux citoyens les moyens de prouver leur identité sur Internet et de signer électroniquement afin de favoriser le développement de l'administration électronique ».

Les nouveaux documents d'identité intégreront des éléments biométriques. Il s'agit de la photo faciale et des empreintes digitales.

Le projet INES prévoit la mise en place de garanties technologiques contre les utilisations et les intrusions illégales dans les données biométriques enregistrées. Les mesures de sécurité devraient permettre de protéger les composants du système, les installations et les titres en vue d'attaques physiques et logiques.

La carte sécurisée devrait être constituée de blocs séparés en ayant recours à la cryptographie. Parmi ces blocs figureront les blocs « identité », « authentification de la carte », « identification authentifiée du porteur » mais aussi et surtout « signature électronique » permettant de signer électroniquement des documents authentiques et « portefolio personnel » encore à l'état de projet mais dont l'objectif est de donner la possibilité à leur titulaire de conserver des informations supplémentaires dans la carte.

Le projet INES entre aujourd'hui dans sa phase active.

La problématique centrale du projet INES porte sur les fonctions que pourrait assurer la carte d'identité biométrique.

A ce titre, il semble acquis que le projet INES comportera à la fois un premier volet « Identité » et un volet autour de la « signature électronique ».

Il subsiste une interrogation quant à un troisième volet sur les « compléments d'usage » ou l'utilisation multifonction.

Il semble que, sur ce dernier volet, des questions d'ordre juridique subsistent quant à la constitutionnalité d'une telle perspective.

La problématique posée par le troisième volet, à savoir l'utilisation multifonction, n'est pas sans poser de difficultés et présente bien entendu des avantages et inconvénients, des adeptes et des détracteurs.

Au titre des avantages, on pourra noter que, si la carte d'identité peut être utilisée à d'autres fins que la simple identité et/ou la signature électronique, ceci aura nécessairement un impact sur son déploiement et devrait, en tout état de cause, le faciliter.

Il semble acquis que plus l'usager pourra trouver en cette carte des services qui lui sont nécessaires, notamment au titre de la vie courante, plus il pourrait être amené à l'utiliser, plus vite alors se développerait la signature électronique.

Ce mécanisme aurait également l'avantage de gérer les problématiques de ce qu'il est convenu d'appeler aujourd'hui la « multi-identité ».

Si les avantages sont certains, les problématiques à résoudre le sont tout autant et notamment celles de :

- l'interopérabilité ;
- la sécurité ;
- la conservation, l'archivage et l'accès aux données.

Au titre de cette réflexion générale, il est intéressant d'examiner la situation de la carte Sésam Vitale.

Il faut ici rappeler qu'un projet de décret est en préparation visant à définir les conditions d'émission de la carte et notamment l'intégration d'une photo stockée dans la puce.

Il a été précisé que la carte Sésam Vitale comportait bien trois volets :

- un volet identitaire ;
- un volet signature électronique ; et
- un volet libre pour le porteur.

Par ailleurs, le projet INES fait actuellement l'objet d'un débat national confié par le Ministère de l'intérieur au Forum des droits sur l'internet.

La première étape du débat a permis de prendre en compte les résultats de l'expérimentation menée en Gironde de la délivrance de la carte d'identité électronique en mairie.

Plusieurs points ressortent de cette première expérience :

- la mise en œuvre d'une telle carte et la prise d'empreintes se sont effectués dans un climat de confiance ;

- il serait souhaitable que la carte ne contienne pas de données liées à la santé et à caractère sanitaire et social, une telle disposition étant en tout état de cause anticonstitutionnelle ;

- la carte devrait être gratuite ;

- la production des passeports biométriques et de la carte d'identité devrait être mutualisée afin d'optimiser les coûts.

La question de la création d'une base centralisée de données biométriques semble encore débattue.

Si la création d'une telle base est pour certains une source de danger potentiel, le ministère de l'intérieur semble la privilégier, celle-ci permettant notamment de diminuer le risque d'usurpation d'identité et d'éviter la délivrance à une même personne de titres sous plusieurs identités différentes[10].

Le projet INES a reçu l'aval du Premier ministre à l'issue du comité interministériel du 11 avril 2005 donnant la possibilité au ministre de l'Intérieur de le mettre en œuvre et il semble que les arbitrages relatifs au caractère obligatoire et au caractère payant de la carte d'identité biométrique ait été rendus puisque cette même carte devrait être tout à la fois obligatoire et payante.

Un projet de loi encadrant le projet INES devrait être soumis par le Premier ministre au Parlement après avis préalable de la Cnil et du Conseil d'Etat.

Il est prévu dans ce projet de loi que « les fichiers seront tous séparés et l'état civil restera géré de façon autonome par l'INSEE sous le contrôle de la justice. La sécurisation des systèmes et l'accès aux données seront fixées par la loi, qui prévoit une aggravation des peines en cas de pénétration illicite dans les fichiers »[11].

La Cnil a quant à elle, rappelé, le 18 février 2005, l'historique de ses avis relatifs à la carte nationale d'identité. Elle insistait alors sur le caractère facultatif que devait conserver une telle carte.

La Cnil recommandait également qu'une dissociation soit faite entre les fonctions de fabrication et de contrôle de la carte, les fonctions de fabrication devant appartenir aux industriels et celles de contrôle aux autorités judiciaires.

[10] « Première étape du débat national sur la carte d'identité électronique » Le Forum des droits sur l'internet, 21 février 2005.
[11] France soir, interview de Monsieur le ministre de l'Intérieur Dominique de Villepin, 12 avril 2005.

Elle a également émis l'avis que la signature du titulaire de la carte nationale d'identité ne devait servir qu'à l'impression du titre et que la donnée ne devait pas être conservée « au-delà du délai strictement nécessaire à l'impression du fac-similé » de cette signature.

La Cnil a souligné que la numérisation de la photographie présentait l'inconvénient d'imposer la constitution d'une base d'images de français et a pris acte que le Ministère de l'intérieur n'envisage pas de conserver ces photographies numérisées au-delà du délai strictement nécessaire à leur impression.

Elle a également rappelé qu'il ne sera en aucun cas constitué un fichier manuel, mécanographique ou automatisé centralisé au niveau national des empreintes digitales.

Enfin, en cas de circonstances exceptionnelles, la Cnil rappelle qu'il devra être procédé à la destruction du système notamment en cas de crise grave. Elle renvoie en cela à ses délibérations de 1980 et 1986 relatives à la carte nationale d'identité[12].

La Cnil considère que le projet INES du ministère de l'Intérieur visant à remplacer la carte d'identité actuelle par une carte à puce intégrant empreintes digitales et photo soulève des questions majeures au regard des principes de protection des données personnelles.

Elle doit être consultée pour avis par les pouvoirs publics.

Elle a décidé d'ouvrir sur son site le dossier « biométrie et titres d'identité » et a entrepris un certain nombre d'actions pour, dit-elle, nourrir le débat de fond.

La Cnil considère que ces projets « parce qu'ils visent à identifier chaque individu non plus seulement par son état civil et le document qui en atteste mais aussi et surtout par sa biométrie, c'est-à-dire par ses caractéristiques physiques, et à les conserver dans des fichiers », soulèvent des questions de société qui doivent être bien appréhendées à travers une évaluation des avantages et des risques qu'ils comportent.

La Cnil précise avoir formulé auprès du ministère de l'intérieur un argumentaire qui s'articule autour des points suivants :

- la situation actuellement constatée en matière d'usurpation d'identité ;

- les finalités et les modalités selon lesquelles seraient utilisées les données biométriques (consultation par lecture directe de la carte d'identité ou conservation dans une base de données centrale des empreintes digitales) ;

- la présentation des solutions techniques alternatives susceptibles d'améliorer la sécurisation des modalités pratiques de délivrance des titres dans le but de mieux garantir l'identité des personnes.

[12] Cnil, délibération 80-19 du 3 juin 1980 portant avis relatif à la création d'un traitement automatisé d'informations nominatives concernant la fabrication de cartes nationales d'identité.
Cnil, délibération 86-76 du 1er juillet 1986 portant avis sur un projet de décret relatif à la création d'un système de fabrication et de gestion informatisé des cartes nationales d'identité.
Cnil, délibération 86-105 du 21 octobre 1986 portant avis sur le relevé d'une empreinte digitale à l'occasion d'une demande de carte nationale d'identité.

Par ailleurs, la Cnil précise avoir engagé les actions suivantes :

- recueil du point de vue de personnalités, historiens, sociologues, philosophes, responsables d'associations des droits de l'homme ;

- rencontres avec industriels du secteur et chercheurs.

4.1.3 Mission d'information de la Commission des lois du Sénat sur la nouvelle génération de documents d'identité et la fraude documentaire

La mission d'information de la Commission des lois du Sénat a tenu sa réunion constitutive le 9 février 2005 sur la nouvelle génération de documents d'identité et la fraude documentaire, ces travaux ayant débuté le 16 février 2005.

Les travaux de cette mission d'information devraient porter sur l'évaluation de la fraude à l'identité et les réponses apportées par les pouvoirs publics, l'évaluation de l'efficacité des nouveaux titres d'identité et enfin l'évaluation de leurs conséquences sur les libertés publiques.

La mission d'information de la Commission des lois du Sénat est notamment mise en place à l'heure où le projet d'identité nationale électronique sécurisée dit INES se met en place.

Le groupe de travail note qu'aucun travail n'a été réalisé en France en ce qui concerne l'évaluation de la fraude, alors qu'il existe un rapport de la FTC aux Etats-Unis sur la fraude et qu'une étude menée en Grande-Bretagne montre que la fraude d'identité engendrerait un coût de plus de 1,5 milliards de livres. Le vrai problème apparaît donc comme étant le vol d'identité.

Le groupe de travail estime qu'il est primordial que le Sénat tout comme la Cnil aient ainsi un rapport direct avec les industriels.

4.1.4 Référentiel légal dédié européen

4.1.4.1 Règlement (CE) n° 2252/2004 du Conseil du 13 décembre 2004 relatifs aux passeports biométriques

Le Conseil de l'Union européenne a adopté le premier texte européen relatif à la réglementation d'un système de reconnaissance biométrique au niveau de l'Union européenne.

Il s'agit du règlement (CE) n° 2252/2004 du 13 décembre 2004 établissant des normes pour les éléments de sécurité et les éléments biométriques intégrés dans les passeports et les documents de voyage délivrés par les États membres.

A la différence d'une directive, un « règlement » communautaire n'a pas besoin de textes nationaux de transposition.

Ce règlement s'applique donc directement dans les pays de l'Union visés.

Sont en effet exclus du champs d'application du règlement le Royaume-Uni et l'Irlande. Le Danemark peut quant à lui décider de s'y conformer dans un délai de six mois.

Le choix d'un règlement comme texte communautaire implique une seconde conséquence immédiatement induite par la première. Dans la mesure où aucun texte de transposition n'est nécessaire à son application dans les Etats membres, il ne peut donc y avoir de débat national, l'ensemble des dispositions ayant été fixées une fois pour toute au niveau communautaire.

Cela implique donc, tant pour le choix des éléments biométriques retenus que pour les conditions juridiques et matérielles relatives aux titres de transport considérés, que les principes soient définitivement arrêtés.

Dans ces grandes lignes, le règlement fixe les règles suivantes :

Il vise les passeports et les documents de voyage délivrés par les Etats membres à l'exclusion des cartes d'identité délivrées par ces derniers à leurs ressortissants et des passeports et documents de voyage d'une durée de validité inférieure ou égale à douze mois.

Le règlement prévoit d'intégrer dans ces documents deux éléments biométriques : la photo faciale et les empreintes digitales. Ces deux technologies ont été privilégiées parmi la quinzaine de solutions biométriques existantes aujourd'hui comme la reconnaissance par l'iris, par la morphologie de la main, la rétine, le réseau veineux ou encore la signature dynamique. La raison de ce choix tient principalement au fait que la France et les autres Etats membres ont une forte tradition en matière d'empreintes digitales et que l'usage de photographies est commune sur les documents d'identité.

Le règlement prévoit les spécifications techniques des passeports biométriques. Il est prévu que ces spécifications seront complétées par d'autres, qui devront rester secrètes, afin de prévenir le risque de contrefaçon et de falsification.

En effet, les spécifications techniques seront définies par la Commission européenne, assistée d'un comité de réglementation composé des représentants des Etats membres ainsi que par le Conseil.

Ces spécifications techniques devront permettre de garantir la sécurisation du support de stockage et de prévenir les accès non autorisés. Les exigences en matière de qualité et de normes communes relatives aux photos et empreintes digitales devront également être définies. Le règlement précise que les éléments biométriques doivent être enregistrés dans un format interopérable sur un support de stockage (puce) doté d'une capacité suffisante pour garantir l'intégrité, l'authenticité et la confidentialité des données.

Un organisme unique désigné par chaque Etat membre sera chargé de la production des passeports dans chacun des Etats membres. Un même organisme pourra être désigné par un ou plusieurs Etats membres. Les spécifications techniques secrètes relatives aux éléments biométriques ne seront communiquées qu'aux organismes ainsi désignés et « aux personnes dûment habilitées par les Etats membres ou par la Commission ». Le règlement ne précise pas quelles seront ces personnes laissant ainsi libre choix aux Etats membres.

Par ailleurs, les nouveaux éléments de sécurité sont définis dans le règlement comme des normes de sécurité minimales à atteindre en ce qui concerne essentiellement la « page des données personnelles » des passeports.

L'annexe 1 du règlement détaille les spécifications techniques relatives aux matériaux, à la page des données personnelles, aux techniques d'impression, à la protection contre la reproduction et à l'intégration des éléments essentiels aux passeports. Le règlement précise que les spécifications techniques développées par l'OACI[13] devront être respectées dans un soucis de lutte contre les tentatives de contrefaçon et de falsification.

Le règlement prend en compte la protection des données biométriques considérées comme des données à caractère personnel et soumises aux dispositions de la Directive 95/46/CE[14]. II est ainsi prévu que chaque citoyen doit avoir le droit de vérification, de rectification ou de suppression, le cas échéant, des données enregistrées dans son passeport. La finalité de l'utilisation des données biométriques est précisée et limitée à la vérification de l'authenticité des documents et de l'identité du titulaire.

L'application dans le temps du règlement doit se faire en deux étapes. Les aspects relatifs au renforcement de la sécurité des passeports et des documents de voyage sont immédiatement applicables. La mise en œuvre de la partie relative à l'intégration dans ces mêmes documents d'éléments biométriques ne se fera, quant à elle, qu'après qu'aient été définies les « spécifications techniques ». Les délais de mise en œuvre prévus sont de 18 mois pour les photos faciales et de 36 mois pour les empreintes digitales à compter de l'adoption de ces mesures techniques.

4.1.4.2 Avis n° 7/2004 du groupe de l'article 29 sur l'insertion d'éléments biométriques dans les visas et titres de séjour

Le groupe de l'article 29 établi par la directive 95/46/CE a pris un avis le 11 août 2004 relatif à l'insertion d'éléments biométriques dans les visas et titres de séjour[15].

Cet avis fait suite à un projet de règlement de la Commission européenne proposé fin 2003 et modifiant les règlements n° 1683/95 et 1030/2002 relatifs au modèle type de visa et au modèle type de titre de séjour pour les ressortissants des pays tiers. Cette modification vise à intégrer dans les visas et titres de séjour des données biométriques, la photo numérisée de face et deux empreintes digitales, stockées sur une puce sans contact.

Le groupe de l'article 29 rappelle les principes que doit respecter la mise en place de tels documents biométriques.

Ainsi les principes de finalité et de proportionnalité doivent être pris en compte. Les personnes concernées doivent pouvoir accéder aux données contenues dans la puce et des garanties doivent être mises en place pour les personnes qui ne possèdent pas les données biométriques visées ou qui font l'objet de faux rejet. Des garanties spécifiques doivent également encadrer les possibilités d'interopérabilité des données biométriques conservées.

[13] Organisation de l'Aviation Civile Internationale.

[14] Directive 95/46/CE du Parlement européen et du Conseil 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 de ces données.

[15] Article 29 Groupe de protection des données, Avis n° 7/2004 sur l'insertion d'éléments biométriques dans les visas et titres de séjour en tenant compte de la création du système d'information Visas (VIS), 11 août 2004.

4.1.5 Travaux de l'OACI

L'une des missions de l'Organisation de l'Aviation Civile Internationale est l'établissement de normes, de pratiques recommandées et de procédures internationales dans les techniques de l'aviation. Ces normes sont ensuite mise en œuvre par les quelques 180 Etats contractants de l'OACI sur leur territoire national.

Très tôt, l'un des buts de l'OACI a été de réfléchir à la manière d'assurer un haut niveau de sécurité aérienne tout en assurant la rapidité des contrôles d'identité. L'introduction de techniques biométriques dans les passeports et autres documents d'identité a alors vu le jour afin d'allier sécurité et fluidité des contrôles.

L'OACI a créé en France une instance de proposition dont l'objet est de soumettre des recommandations aux Etats. Cette instance placée auprès du secrétaire général de l'OACI, constituée en 1986 est dénommée le « Technical Advisory Group on Machine Readable Travel Documents » (TAG/MRTD). Elle est notamment composée de 13 experts issus de pays membres de l'OACI dont la France, les Etats-Unis, le Royaume-Uni, l'Allemagne et le Japon et d'organismes qui peuvent être invités tels qu'Interpol, l'ACI (Airport's Council International) et l'ISO (International Organization for Standardization)[16]. L'OACI a notamment publié en 1980 le « Doc 9303 » qui donne les spécifications des MRTD, à savoir les passeports, les visas et les documents de voyage officiels.

L'OACI a pu identifier, dans un rapport technique visant à réviser le document 9303, les technologies biométriques présentant une bonne compatibilité et pouvant constituer un standard international pour l'utilisation des MRTD. Le rapport insiste sur le fait qu'une seule technique biométrique pour l'ensemble des Etats serait préférable et que cette technique devrait assurer à la fois les fonctions de vérification d'identité et d'identification 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[17]. L'OACI retient deux techniques biométriques, à savoir la reconnaissance faciale et par empreintes digitales comme étant les plus compatibles avec les exigences du système MRTD. L'OACI recommande finalement une généralisation des photographies numérisées et la possibilité pour les Etats d'introduire l'empreinte digitale ou l'iris dans les passeports ou documents de voyage.

4.2 REFERENTIEL LEGAL GENERIQUE

Le référentiel légal dédié à la biométrie est encore peu développé, même s'il fait l'objet à l'heure actuelle d'un développement croissant dans les domaines analysés précédemment.

Cependant, la mise en oeuvre de la biométrie n'en est pas moins encadrée juridiquement que ce soit par le droit social, le droit des contrats, le droit de la preuve, le droit relatif à la sécurité, le droit des assurances ou encore le droit relatif à la cryptologie.

[16] Rapport (2ème partie) de l'Office parlementaire d'évaluation des choix scientifiques et technologiques sur les méthodes scientifiques d'identification des personnes à partir des données biométriques et les techniques de mise en oeuvre, Monsieur le député Christian Cabal, n° 938, Assemblée nationale, n° 355 Sénat, juin 2003.

[17] Rapport (2ème partie) de l'Office parlementaire d'évaluation des choix scientifiques et technologiques sur les méthodes scientifiques d'identification des personnes à partir des données biométriques et les techniques de mise en oeuvre, Monsieur le député Christian Cabal, n° 938, Assemblée nationale, n° 355 Sénat, juin 2003.

4.2.1 Encadrement de la biométrie par le droit social

Le droit du travail doit s'appliquer dans l'entreprise en cas d'introduction de nouvelles technologies au sein de celle-ci. Le droit social constitue en effet un élément juridique majeur en matière de biométrie.

Certaines obligations s'imposent en effet à l'employeur lors de l'introduction d'une nouvelle technologie au sein de l'entreprise.

L'article L. 121-8 du Code du travail dispose que :

- « Aucune information concernant personnellement un salarié ou un candidat à un emploi ne peut être collectée par un dispositif qui n'a pas été porté préalablement à la connaissance du salarié ou du candidat à l'emploi ».

Ainsi, tout salarié ou candidat à un emploi doit être informé de la mise en oeuvre dans l'entreprise de dispositifs tels que la mise en place de badges permettant un contrôle des accès ou des horaires.

Une obligation d'information et de consultation préalable du comité d'entreprise s'impose également.

L'article L. 432-2 du Code du travail dispose que :

- « Le comité d'entreprise est informé et consulté, préalablement à tout projet important d'introduction de nouvelles technologies, lorsque celles-ci sont susceptibles d'avoir des conséquences sur l'emploi, la qualification, la rémunération, la formation ou les conditions de travail du personnel. Les membres du comité reçoivent, un mois avant la réunion, des éléments d'information sur ces projets et leurs conséquences mentionnés ci-dessus ».

En outre, aux termes de l'article L. 434-6 du Code du travail, le comité d'entreprise peut faire appel à un expert en nouvelles technologies.

Par ailleurs, en vertu de l'article L. 432-2-1, alinéa 3, du Code du travail, le comité d'entreprise doit également être informé et consulté :

- « Préalablement à la décision de mise en oeuvre dans l'entreprise, sur les moyens ou les techniques permettant un contrôle de l'activité des salariés ».

Ainsi, préalablement à l'introduction d'une solution biométrique, une entreprise devrait informer et consulter son comité d'entreprise dans le respect de la procédure et des conditions du Code du travail.

Il est rappelé que le non respect de ces obligations est susceptible d'être sanctionné pénalement.

L'article L. 483-1 du Code du travail dispose en effet que :

- « Toute entrave apportée, soit à la constitution d'un comité d'entreprise, d'un comité d'établissement ou d'un comité central d'entreprise, soit à la libre désignation de leurs membres, soit à leur fonctionnement régulier, notamment par la méconnaissance des dispositions des articles L. 433-13, L. 436-1 et L. 436-3 et des textes réglementaires pris pour leur application, sera punie d'un emprisonnement d'un an et d'une amende de 3 750 euros ou de l'une de ces deux peines seulement (...) ».

Enfin, les problématiques liées à l'accessibilité des personnes handicapées aux solutions biométriques mises en oeuvre par les entreprises clientes des industriels devront être prises en compte. En effet, aucune mesure discriminatoire ou excluant les personnes handicapées ne devra être mise en oeuvre dans ce cadre.

De la même manière, la biométrie, dans la mesure où elle serait utilisée pour surveiller les salariés, c'est-à-dire dans un cadre de cybersurveillance, devrait au préalable faire l'objet d'une information des salariés.

Cette information des salariés passe notamment par la mise en place de chartes internes prévoyant l'existence et les conditions d'exercice de la vie privée résiduelle des salariés.

Le groupe de travail mentionne que c'est là l'objectif de la charte qu'il rédige dans le cadre du livre blanc, à savoir permettre aux industriels de s'engager sur la transparence afin d'être labellisés par la Cnil et de pouvoir, dans un second temps, mettre en place des solutions biométriques sans avoir l'obligation d'être autorisés pour ce faire par la Cnil.

Le groupe de travail note qu'il sera nécessaire de mettre en place des chartes adaptées à chaque type de solution biométrique envisagé. Les industriels devront avertir leurs clients des obligations qui leur incombent lors de la mise en place de solutions biométriques dans leur entreprise afin de leur faciliter les démarches auprès de la Cnil et de leur comité d'entreprise.

4.2.2 Encadrement de la biométrie par le droit des contrats

Le droit des contrats aura vocation à s'appliquer lors de la mise en oeuvre d'une solution biométrique afin de sécuriser contractuellement le projet. Un contrat sera évidemment nécessaire entre le fournisseur et le client.

Certaines clauses spécifiques de ce contrat devront notamment décrire les phases de réalisation (définition, fourniture, recette et maintenance) et les garanties à la charge du fournisseur en termes de sécurité de la solution (tests, évaluation des taux de fausse acceptation et de faux rejet), de solutions de contournement proposées en cas de défaillance de la solution, de fiabilité de la solution dans le temps, d'adaptation de la technique aux normes ou aux nouvelles dispositions juridiques.

Un contrat devra également être mis en oeuvre entre le client de la solution biométrique qu'il a mise en place dans son entreprise et les utilisateurs de celle-ci. Ce contrat pourrait prendre la forme de conditions générales d'utilisation détaillées mentionnant notamment les conditions de responsabilité des utilisateurs, les risques encourus, les dangers de la technologie, les conséquences en cas de perte ou de vol des produits biométriques mis à la disposition des utilisateurs comme une carte contenant les empreintes digitales par exemple.

4.2.3 La biométrie utilisée à titre de signature électronique et gestion de la preuve

La biométrique pourra être utilisée dans certains cas à titre de signature électronique. Ainsi un élément biométrique pourrait être converti en code puis utilisé afin de signer électroniquement des documents authentiques ou des transactions d'ordre privée.

Une telle utilisation devra alors tenir compte la loi du 13 mars 2000 relative à la preuve et à la signature électronique.

Par ailleurs, l'utilisation de solutions biométriques à titre de preuve devra faire l'objet, lorsqu'elle n'entre pas dans le cadre de la signature électronique, de conventions de preuve intervenant entre les personnes concernées ou, lorsqu'il s'agit de preuve judiciaire, de garanties spécifiques protégeant les droits des personnes à l'encontre desquelles la preuve biométrique est utilisée.

Enfin, la conservation des données biométriques à titre de preuve devra tenir compte de la norme Afnor Z42-013[18] relative à l'archivage électronique. Cette norme précise que les données conservées doivent être stockées sur un support doté d'une capacité suffisante pour garantir l'intégrité, l'authenticité et la confidentialité des données et le système d'archivage doit assurer la traçabilité des enregistrements.

4.2.4 Biométrie et sécurité des données

L'article 34 de la loi Informatique et libertés du 6 janvier 1978 impose au responsable du traitement de données à caractère personnel, dont les données biométriques font partie, de prendre toute précaution utile, au regard de la nature des données et des risques présentés par le traitement pour préserver la sécurité des données et empêcher que des tiers non autorisés y aient accès.

Une entreprise qui mettra en place une solution biométrique et procèderait ainsi au traitement de données biométriques devrait en conséquence mettre en place des mesures techniques et logiques pour garantir la fiabilité, la non déformation et la confidentialité des données.

Cette obligation de sécurité s'impose également à toute personne à qui le traitement des données biométriques serait sous-traité. Un tel sous-traitant devrait présenter des garanties suffisantes pour assurer la sécurité et la confidentialité des données, cette délégation à un sous-traitant ne dégageant pas le responsable du traitement des données biométriques de ses obligations.

[18] Norme Z42-013 « Archivage électronique – spécifications relatives à l'exploitation de systèmes informatiques en vue d'assurer la conservation et l'intégrité des documents stockés dans ces systèmes ».

La mise en oeuvre de solutions biométriques doit, d'une manière générale, répondre à des critères de sécurité et de fiabilité élevés.

A ce titre, toute entreprise mettant en oeuvre une telle technique devra envisager des audits de sécurité afin d'évaluer les taux de fausse acceptation et de faux rejet des solutions proposées.

4.2.5 Biométrie et droit des assurances

La mise en place de solutions biométriques dans une entreprise a, très logiquement, un impact sur le niveau de sécurité existant au sein de celle-ci. Un tel niveau de sécurité amélioré aura des conséquences sur les polices d'assurance auxquelles adhèrent les entreprises concernées et la mise en place de systèmes biométriques devra en conséquence être prise en compte lors de la rédaction de telles polices d'assurance.

4.2.6 Biométrie et réglementation relative à la cryptologie

La mise en place de solutions biométriques s'accompagnera très fréquemment du cryptage des données biométriques. Or, la cryptologie fait l'objet d'une réglementation modifiée récemment par la loi n° 2004-575 pour la confiance dans l'économie numérique du 21 juin 2004.

Si cette loi libéralise entièrement l'utilisation de la cryptologie, la fourniture, l'importation et l'exportation de moyens de cryptologie ainsi que la fourniture de prestations de cryptologie restent soumises à des obligations de déclaration et d'autorisation du premier ministre.

Les fournisseurs de moyens de cryptologie et les prestataires de cryptologie intervenant dans la mise en place des solutions biométriques devront ainsi respecter ces obligations de déclaration et d'autorisation auprès des services du premier ministre, à savoir le secrétariat général à la Défense nationale (SGDN).

5. IDENTIFICATION ET AUTHENTIFICATION

Les notions d'identification et d'authentification ne sont pas définies en tant que telles sur un plan légal et l'usage souvent indifférent de l'une et de l'autre ne simplifie pas la démarche.

Une réflexion nécessaire devait être engagée quant à la définition du terme « authentification » dans un souci constant de ne pas en élaborer une définition exagérément complexe.

5.1 PROBLEMATIQUES LIEES A LA NOTION D'AUTHENTIFICATION

Le groupe de travail s'est attaché à définir la notion d'authentification et à étudier les raisons d'être d'une distinction entre identification et authentification, s'agissant plus particulièrement de la biométrie.

La problématique posée par la notion d'authentification est liée à la difficulté de trouver une définition admise par tous.

Les notions d'« identification » et d'« authentification » sont extrêmement complexes et leur différentiation réelle l'est tout autant.

Une rapide analyse des différents codes français (civil, commercial, pénal, administratif,…) fait apparaître que :

- il n'y a aucune définition de l'un ou l'autre de ces termes ;
- ils sont souvent utilisés l'un à la place de l'autre.

Ainsi le code du travail et le code électoral mélangent les genres et évoquent « l'authentification de l'identité du votant ».

L'article 27 de la loi dite Informatique et libertés pour sa part utilise la terminologie suivante « d'authentification et de vérification d'identité », ce qui là encore ne milite pas en faveur d'une distinction évidente entre « identification » et « authentification ».

Le dictionnaire lui-même garant de la définition des termes ne nous est pas d'un grand secours qui précise que l'authentification est « l'action de certifier la vérité, l'exactitude de quelque chose… » alors que l'identification serait « l'action d'établir l'identité de quelqu'un ; déterminer la nature de quelque chose ».

Ce difficile exercice de définition et la relative complexité d'expliquer de manière claire ces deux notions et particulièrement celle d'« authentification » sont sans nul doute l'un des freins majeurs au développement de la signature électronique.

Pour éviter que la biométrie ne connaisse les mêmes difficultés que la signature électronique et qu'elle ne soit sclérosée par une inutile syntaxique entre « identification » et « authentification », le groupe de travail s'est intéressé à l'existence ou non d'une définition claire et autonome de l'authentification et à la nécessité de retenir une telle distinction sémantique s'agissant de la biométrie.

5.2 TENTATIVES DE DEFINITION

Plusieurs définitions et/ou conceptions ont été proposées par le groupe de travail.

Une première opposition entre « authentification » et « identification » pourrait naître de ce que l'identification aurait trait à une personne alors que l'authentification aurait trait à un objet.

Ainsi, l'usage de la carte à puce permet l'authentification d'une personne.

La réalité est plus complexe dans la mesure où même en face de processus de « simple identification », il est souvent demandé à une personne d'attester de cette identité par un moyen quelconque (carte d'identité, passeport, carte de séjour, ou tout autre document de même nature).

Une autre distinction reposerait sur une opposition entre l'identification qui serait la phase initiale permettant de « connaître une personne » alors que l'authentification ne serait qu'un processus de réitération ultérieure de cette identification.

En réalité, on distinguerait ici l'identification de l'authentification en tant que deux phases du processus d'identification.

On voit ici immédiatement la limite de cette approche qui implique un lien direct entre authentification et identification, l'authentification n'étant qu'un élément de l'identification.

Une troisième tentative de définition a pris pour socle la notion de « processus ».

Ici, le processus d'identification serait un processus qui impliquerait la présence physique de la personne alors que le processus d'authentification serait un processus qui n'impliquerait pas une telle présence physique ; soit parce que la personne est représentée par un objet, soit parce que la personne est représentée par un élément qui la caractérise (login, password, code d'accès…).

Ainsi donc, la distinction revêtirait, en matière de biométrie, un intérêt majeur dans la mesure où elle reposerait sur un mécanisme d'identification (présence impérative de la personne physique) alors que toute autre procédure d'authentification est par nature plus faible puisqu'elle n'implique pas nécessairement la présence physique de la personne.

En effet, même si sur un plan juridique la pratique est condamnable, il est possible à n'importe qui de confier sa carte à puce, son badge RFID, un login ou un password ou encore un code d'accès à n'importe quelle autre personne.

Cette tierce personne utilisatrice serait alors authentifiée comme le porteur légitime alors qu'elle ne l'est pas.

Une autre dichotomie a été soulevée qui opposerait l'identification de type « actif » par opposition à l'authentification qui serait un processus d'identification de type « passif ».

Il est rappelé qu'il existe cependant un certain nombre de produits (RFID) ou de services (identification de terroristes dans la foule) qui sont liés à un processus d'identification alors qu'ils sont éminemment passifs.

Une autre solution a été proposée et qui permettait de distinguer l'identification de l'authentification en ce sens que l'identification serait synonyme de « Qui êtes-vous ? » là où l'authentification serait synonyme de « Prouvez-le ? ».

La réalité veut qu'en principe le processus qu'il s'agisse d'un processus d'identification et/ou d'authentification, joue sur les deux éléments.

Lorsqu'on identifie une personne (par exemple, lors d'une ouverture de compte) il s'agit d'un processus où l'on demande à la personne de s'identifier et où l'on vérifie son identité (par la carte d'identité et un justificatif de domicile).

« Qui êtes-vous » et « Prouvez-le » sont donc généralement extrêmement liés pour ne pas dire fusionnant.

Il est difficile dans ces circonstances d'utiliser ces terminologies comme permettant de distinguer l'authentification et l'identification.

5.3 PROPOSITION DE DEFINITION

Après moult discussions, les membres du groupe de travail se sont entendus sur la définition suivante :

L'identification est une notion qui regroupe l'ensemble des paramètres permettant de distinguer une personne.

Le terme « authentification » est parfois assimilé, parfois distingué de la notion d'identification.

Pour les distinguer, il est possible de retenir la summa divisio suivante :

- l'identification est un processus de détermination de l'identité d'une personne qui comprend la personne elle-même dans le processus ;

- l'authentification est un processus d'identification qui comprend un ou plusieurs éléments représentant la personne.

Exemples :

- la biométrie est un processus d'identification par nature ;
- la carte RFID ou la carte à puce est un processus d'authentification par nature.

En matière de biométrie, la présence physique d'une personne, qui mettrait alors en œuvre un processus d'identification, empêcherait toute possibilité de substitution ou de transfert de code ou d'autres éléments matériels du porteur et toute utilisation des identifiants par un tiers sauf à tromper le système lui-même.

Jusqu'alors le processus d'identification/authentification des personnes, notamment dans un environnement électronique, a reposé sur un mécanisme d'authentification fort (authentification par carte à puce par exemple) et d'identification faible.

A l'inverse, le processus de biométrie implique un mécanisme d'authentification fort associé à un mécanisme d'identification fort au sens où l'identification a lieu en présence de la personne elle-même et le processus d'authentification ne porte que sur un couplage identification/authentification par le porteur physique lui-même.

Dès lors, le fait de retenir une distinction identification/authentification permet de renforcer le caractère probant des mécanismes d'identification biométrique par rapport à tous les autres mécanismes d'identification du marché.

Le groupe de travail estime cependant qu'une définition légale de l'identification et, le cas échéant et sous réserve que cela soit nécessaire, de l'authentification est indispensable et que l'occasion d'adopter la loi relative au programme INES serait sans doute une occasion unique pour clore le débat.

6. RESPONSABILITES ET GARANTIES

L'idée maîtresse en matière de garantie est d'apprécier la situation non pas au regard d'un objectif de fiabilité 100% que chacun sait impossible à mettre en œuvre mais au regard d'un double objectif :

- celui de déterminer les « garanties raisonnables » ;
- celui de combiner le « zéro rejet à tort » avec le « zéro acceptation à tort ».

6.1 REGIME LEGAL DE RESPONSABILITES

La mise en oeuvre de solutions biométriques doit prendre en compte les garanties auxquelles s'engagent les professionnels de ce secteur et la responsabilité qui sera la leur.

A ce titre, se pose la question de savoir si le régime de responsabilité et de garanties des fournisseurs de solutions biométriques sera contractuel ou légal.

En effet, d'une manière générale, une seule garantie s'impose légalement aux fournisseurs de solutions biométriques. Il s'agit de la garantie des vices cachés des articles 1641 et suivants du Code civil.

Les autres garanties relèvent de la relation contractuelle établie entre les fournisseurs et les acheteurs.

Il existe cependant des secteurs techniques autres que la biométrie dans lesquels le législateur a choisi d'imposer légalement un régime de garanties et de responsabilités aux fournisseurs.

Il s'agit notamment du cadre de responsabilité spécifique renforcée des fournisseurs de prestations de cryptologie à des fins de confidentialité et des prestataires de services de certification électronique, tel que cela résulte des articles 32 et 33 de la loi pour la confiance dans l'économie numérique[19] :

- l'article 32 prévoit :

- « Sauf à démontrer qu'elles n'ont commis aucune faute intentionnelle ou négligence, les personnes fournissant des prestations de cryptologie à des fins de confidentialité sont responsables au titre de ces prestations, nonobstant toute stipulation contractuelle contraire, du préjudice causé aux personnes leur confiant la gestion de leurs conventions secrètes en cas d'atteinte à l'intégrité, à la confidentialité ou à la disponibilité des données transférées à l'aide de ces conventions » ;

[19] Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.

- l'article 33 prévoit :

- « Sauf à démontrer qu'ils n'ont commis aucune faute intentionnelle ou négligence, les prestataires de services de certification électronique sont responsables du préjudice causé aux personnes qui se sont fiées raisonnablement au certificat présenté par eux comme qualifié dans chacun des cas suivants :
1. les informations contenues dans le certificat, à la date de sa délivrance, étaient inexactes ;
2. les données prescrites pour que le certificat puisse être regardé comme qualifié étaient incomplètes ;
3. la délivrance du certificat n'a pas donné lieu à la vérification que le signataire détient la convention privée correspondant à la convention publique de ce certificat ;
4. les prestataires n'ont pas, le cas échéant, fait procéder à l'enregistrement de la révocation du certificat et tenu cette information à la disposition des tiers.
Les prestataires ne sont pas responsables du préjudice causé par un usage du certificat dépassant les limites fixées à son utilisation ou à la valeur des transactions pour lesquelles il peut être utilisé, à condition que ces limites figurent dans le certificat et soient accessibles aux utilisateurs.
Ils doivent justifier d'une garantie financière suffisante, spécialement affectée au paiement des sommes qu'ils pourraient devoir aux personnes s'étant fiées raisonnablement au certificat qualifié qu'ils délivrent, ou d'une assurance garantissant les conséquences pécuniaires de leur responsabilité civile professionnelle ».

La loi impose ainsi aux fournisseurs de prestations de cryptologie, même en présence de dispositions contractuelles contraires, une responsabilité relative à la confidentialité, à l'intégrité et à la disponibilité des données cryptées.

Comme pour les fournisseurs de prestations de cryptologie, les prestataires de services de certification électronique peuvent se soustraire à leur responsabilité dès lors qu'ils démontrent n'avoir commis aucune faute intentionnelle ou négligence.

Les prestataires de services de certification électronique ne sont également pas responsables du préjudice causé aux utilisateurs dès lors que ceux-ci dépassent les limités fixées à l'utilisation du certificat ou à la valeur des transactions pour lesquelles il peut être utilisé.

Cependant, une double condition s'impose dans ce cas :

- les limites doivent figurer dans le certificat ; et
- elles doivent être accessibles aux utilisateurs.

Une double obligation d'information est donc imposée aux prestataires de services de certification électronique :

- une obligation d'information relative à la technique ;
- une obligation d'information contractuelle disponible dans les conditions d'utilisation.

Par ailleurs, les prestataires de services de certification électronique doivent justifier d'une garantie financière suffisante.

La garantie légale imposée par le législateur dans ces secteurs est donc particulièrement contraignante.

A l'inverse, des régimes de garanties contractuelles existent, à titre d'exemple, dans les contrats informatiques. Ces contrats comprennent alors de très nombreuses exclusions de garanties et des clauses de limites de responsabilité.

De telles clauses de garanties sont, cependant, très souvent jugées excessives par les juges et requalifiées.

La question qui se pose au groupe de travail est de savoir s'il est souhaitable de prévoir un régime de garanties légales aux fournisseurs et aux prestataires de solutions biométriques, et dans la négative de définir un comportement contractuel idoine permettant d'éviter qu'un tel dispositif ne soit mis en œuvre par le gouvernement.

Tel pourrait être le cas si les professionnels de la biométrie ne parvenaient pas à présenter des garanties suffisantes à la mise en oeuvre de solutions biométriques.

Il appartient donc aux professionnels de bien éclairer leurs clients sur les garanties accordées et de les mettre en garde sur les fonctionnalités des produits.

Une triple obligation s'impose aux professionnels de la biométrie qui doivent la remplir avec diligence:

- une obligation d'information ;
- une obligation de conseil ; et
- une obligation de mise en garde et d'alerte.

En l'état actuel, le groupe de travail estime que toute obligation légale ou régime de responsabilité défini dans la loi en dehors de celui relatif aux vices cachés serait de nature à nuire au bon développement du marché de la biométrie et n'apporterait pas nécessairement d'avantages au bénéfice des utilisateurs.

6.2 GARANTIES APPROPRIEES AU SECTEUR DE LA BIOMETRIE

6.2.1 Des garanties adaptées aux finalités des solutions biométriques

Les solutions biométriques semblent avoir deux finalités de mise en oeuvre différentes :

- une finalité de confort ; ou
- une finalité de sécurité.

La mise en oeuvre de solutions biométriques a pour unique finalité le confort lorsque aucune nécessité de sécurité ne s'impose à l'utilisateur.

Tel est le cas, par exemple, lors de l'utilisation de la biométrie pour obtenir le réglage des équipements d'assise et de visualisation d'une automobile.

Les solutions biométriques ayant une finalité de sécurité sont, quant à elles, mises en œuvre, soit dans un cadre supervisé, soit dans un cadre non supervisé.

Il s'agit d'un cadre supervisé lorsque le système de sécurité biométrique est renforcé par un système de contrôle humain. Au contraire, le cadre est dit non supervisé lorsqu'il n'existe pas de double contrôle.

A titre d'exemple, l'intégration par un gouvernement d'éléments biométriques dans des visas ou des passeports, ou encore l'utilisation de la biométrie pour permettre des accès aéroportuaires sont des solutions biométriques à finalité de sécurité dans un cadre supervisé.

A l'inverse, l'utilisation d'un distributeur de billets accessible par empreintes digitales est une solution biométrique à finalité de sécurité dans un cadre non supervisé.

Les garanties proposées par les professionnels doivent donc être appropriées à la technologie biométrique utilisée.

6.2.2 Des garanties adaptées aux niveaux de risques

Les garanties offertes seront différentes selon le niveau de sécurité offert par les systèmes biométriques.

Les garanties devront ainsi être adaptées selon que la solution biométrique permet l'accès à une centrale nucléaire ou simplement à une école.

Outre le niveau de sécurité proposé par le système biométrique, le niveau d'attaquants devra être pris en compte pour déterminer les garanties à offrir.

A titre d'exemple, lorsque la biométrie est utilisée pour permettre un accès parental à des chaînes télévisées, le niveau d'attaquants sera considéré comme faible.

Il faut noter que les niveaux de sécurité proposés par les systèmes biométriques font l'objet de tests, évaluant les taux de fausse acceptation et les taux de faux rejet. S'il est difficile d'évaluer les taux de fausses acceptations, les taux de faux rejets peuvent être estimés dans la mesure où les personnes rejetées signalent toujours la défaillance dont ils sont victimes.

Il est dès lors possible de s'engager à obtenir un taux de fausses acceptations déterminé et assurer le niveau de faux rejets obtenu.

Seuls les niveaux de sécurité des systèmes biométriques reposant sur le vivant (liveness check) ne sont pas actuellement évaluables.

Des scénari correspondants à des listes d'attaques sont cependant actuellement étudiés pour évaluer les niveaux de sécurité de ces derniers.

A ce titre, il faut noter qu'il n'existe pas à l'heure actuelle de laboratoires en France permettant de procéder à l'évaluation du niveau de sécurité des solutions biométriques proposées.

Il serait ainsi souhaitable de voir la création de laboratoires permettant d'évaluer les niveaux de sécurité offerts par les solutions biométriques et de donner à la DCSSI les moyens d'assurer la qualification des systèmes de sécurité biométriques en France.

En ce qui concerne les systèmes biométriques ayant pour finalité la sécurité dans un cadre supervisé, peu de garanties semblent devoir être offertes par les professionnels.

En effet, le système étant souvent mis en place au niveau étatique, l'Etat se garantit lui-même.

En revanche, lorsque la solution biométrique est proposée pour une finalité de sécurité dans un cadre non supervisé, les fournisseurs doivent s'engager à garantir l'état de l'art.

Il s'agit dès lors de définir l'état de l'art dans le domaine de la biométrie.

Il est nécessaire pour cela de déterminer qui est capable de définir l'état de l'art au fur et à mesure de l'avancée et de la mise en oeuvre des solutions biométriques.

Des mécanismes de normes et de standards communs pourraient être mis en place tel que cela est déjà mis en oeuvre par l'observatoire de la Banque de France donnant des avis a posteriori.

A l'heure actuelle, il existe le Bioconsortium qui rédige des études objectives sur la biométrie.

Les normes BEM (Biometric Evaluation Methodology) pourraient également être prises en compte pour déterminer l'état de l'art des systèmes biométriques[20].

En tout état de cause, l'état de l'art semble différent selon chaque technique biométrique dont les taux de fausses acceptations et les taux de faux rejets sont différents.

Le groupe de travail insiste enfin sur le fait que la biométrie a pour finalité de renforcer la sécurité et non d'assurer seule la sécurité.

En conséquence, les professionnels doivent garantir aux clients que le système biométrique utilisé est un système de sécurité supplémentaire à celui qui existait déjà et non garantir un système sans faille.

6.2.3 Des garanties adaptées aux besoins des clients

Les garanties proposées par les professionnels de la biométrie devront être adaptées aux besoins mêmes du client.

Il s'agira donc d'établir un compromis entre les solutions proposées et les besoins et moyens du client.

[20] Common criteria, common methodology for information technology security evaluation, biometric evaluation methodology supplement (BEM), août 2002.

6.3 GARANTIES DE CONTOURNEMENT ET DE SUBSTITUTION

Pour toutes les solutions biométriques proposées, il semble essentiel que les professionnels garantissent des modes dégradés d'utilisation des systèmes et des solutions de contournement de ceux-ci.

En effet, des solutions de substitution ou de contournement semblent indispensables dans la mesure où la défaillance d'un système biométrique peut se produire.

Il faut en effet noter que les systèmes biométriques sont dépourvus de déterminisme. Reposant sur des éléments humains, ils ne peuvent pas assurer une fiabilité totale.

Ceci explique la raison pour laquelle il existe pour toute solution biométrique un taux de faux rejet alors que ceci n'est pas le cas pour d'autres systèmes d'accès sécurisés comme les badges d'accès par exemple.

En cas de défaillance, à défaut de solution de substitution ou de contournement, les utilisateurs n'auraient aucun recours pour faire fonctionner le système biométrique et cette situation entraînerait incontestablement le rejet à long terme des systèmes biométriques par les clients.

Il est donc nécessaire que les professionnels proposent des solutions de contournement. A titre d'exemple, la vente d'un système biométrique permettant un accès sécurisé devrait s'accompagner de l'offre d'un code de substitution afin de palier la défaillance éventuelle du système biométrique.

Cette garantie, dans la mesure où elle induit un coût, doit rester optionnelle.

Le client doit quant à lui avoir la possibilité de refuser une telle option.

6.4 ALERTES ET MISES EN GARDE

La biométrie peut être, comme l'est le nucléaire, la chimie ou l'informatique, considérée comme un domaine « dangereux » au sens juridique s'entend.

Or, la conséquence d'une telle qualification implique, de la part des professionnels, une obligation d'alerte et de mise en garde en matière de conseil.

Il s'agit en effet de ne pas confondre l'objectif poursuivi par le client et la réalité du niveau de sécurité proposé.

Les professionnels semblent donc devoir mettre en garde le client sur les risques qu'il encourt lors de l'utilisation d'un système biométrique.

6.5 SERVICE DE VEILLE

Il semble important que les professionnels proposent une garantie de veille technologique permettant de prendre en compte le facteur temps dans la mise en oeuvre de la biométrie.

En effet, les professionnels doivent garantir que les solutions biométriques qu'ils proposent seront utilisables et fiables dans le temps.

A ce titre, la norme Afnor Z42-013 relative à l'archivage pourra être prise en compte par les professionnels pour prévoir les conditions de conservation des solutions biométriques proposées.

La responsabilité des fournisseurs de solutions biométriques devra être limitée à la garantie de l'état de l'art de la solution proposée et des attaques susceptibles d'avoir lieu.

Par ailleurs, les professionnels de la biométrie pourraient s'engager à réaliser des audits du niveau de sécurité des solutions biométriques proposées.

Un régime de maintenance pourrait également être mis en place par les fournisseurs afin de délivrer un certificat relatif au niveau d'attaques supporté par le système biométrique. Dans les cas, peu probables, où l'audit se révèlerait négatif, les fournisseurs s'engageraient à mettre en oeuvre des mesures de correction des failles de sécurité.

6.6 MATRICE DE RESPONSABILITES

Il semble que la distinction entre obligation de moyen et de résultat soit inadaptée au secteur de la biométrie.

Le groupe de travail rappelle dans un premier temps que la différence entre une obligation de moyen et de résultat ne tient pas à la nature de l'obligation imposée au professionnel mais tient à la charge de la preuve.

En effet, lorsque le professionnel a une obligation de résultat, sa responsabilité ne sera pas engagée dès lors qu'il peut apporter la preuve soit d'un fait constitutif de force majeure, soit de la responsabilité du client.

A l'inverse, lorsque le professionnel a une obligation de moyen, c'est au client d'apporter la preuve que le professionnel n'a pas rempli ses obligations.

Dans la mesure où un contrat, dans lequel les professionnels n'auraient à leur charge que des obligations de moyens, pourrait être requalifié, cette distinction n'a pas lieu d'être retenue.

Il est donc plus adapté de mettre en place une matrice de responsabilités, notamment en période de test, dans laquelle les différents acteurs présents dans la relation contractuelle et les obligations à la charge de chacun d'entre eux seraient identifiés.

Dans la plupart des cas, le fournisseur de solutions biométriques aurait une obligation de moyen pour ce qui concerne la garantie de l'état de l'art de la solution proposée et une obligation de résultat correspondant par exemple aux délais prévus au contrat.

6.7 CONDITIONS D'UTILISATION ET RESPONSABILITE DES CLIENTS

La responsabilité des fournisseurs de solutions biométriques doit également être limitée par les obligations mises à la charge des utilisateurs qui devront s'engager à respecter les conditions générales d'utilisation des solutions biométriques.

Les conditions générales d'utilisation devront ainsi être particulièrement bien définies et détaillées.

Toute utilisation par un client d'un système biométrique au-delà des limites fixées par les conditions générales d'utilisation exonérerait ainsi les professionnels de toute responsabilité.

7. PROPRIETE

La propriété en matière de biométrie peut être appréciée autour des six classes suivantes :

- classe 1 : propriété des équipements et matériels ;
- classe 2 : propriété de la carte ;
- classe 3 : propriété de l'usage de la carte ;
- classe 4 : propriété des informations sur la carte ;
- classe 5 : propriété interface, interopérabilité, co-usage ;
- classe 6 : informations et données amont/aval.

Concernant la problématique de la propriété de la carte, il semble acquis que la propriété est l'attribut de l'émetteur de la carte.

La question se pose toutefois, tant en termes de responsabilité que de sécurité, de la transférer au bénéfice du titulaire porteur.

Une analyse relative aux notions de propriété sur les cartes existantes (cartes bancaires, cartes Sesam Vitale et cartes d'identité) et dans la plupart des textes y étant relatifs (Code monétaire et financier, Code de la consommation, Code de la sécurité sociale) a permis de constater que la notion de propriété n'est jamais évoquée. Il n'est question que de titulaire et de bénéficiaire de la carte et du problème de la remise des cartes en cas de perte et de vol.

Pour l'heure, il reste acquis que, dans la majorité des cas, la propriété reste celle de l'émetteur.

Ceci est spécifié dans le cadre du contrat porteur carte bancaire. Ceci est également précisé lors de l'envoi de la carte Sesam Vitale à chacun des titulaires. Il est aussi d'usage de trouver cette même information sur la carte elle-même.

Sur la problématique des éléments amonts, c'est-à-dire essentiellement des éléments recueillis lors de la phase d'initialisation des éléments biométriques composant la carte ou le titre support, le groupe de travail souhaite qu'une réflexion de fond soit menée par les pouvoirs publics sur la nécessaire mutualisation de ces éléments.

Si les mêmes éléments biométriques sont en effet utilisés pour plusieurs titres, on peut effectivement s'interroger sur les raisons qui ne permettraient pas de réutiliser les mêmes empreintes biométriques prises une fois pour l'ensemble des titres qui les utiliseraient.

Si, en effet, la photographie faciale est utilisée pour la carte d'identité comme pour la carte Sesam Vitale ou encore le passeport et si les empreintes sont également utilisées à la fois pour le passeport et pour la carte d'identité nationale, il semblerait judicieux que cette prise d'empreintes biométriques soit réalisée une seule fois.

La question corrélative se pose alors d'une centralisation via un fichier unique.

Une autre question est également posée, celle de la nécessaire adaptation des éléments biométriques, notamment s'agissant des photographies faciales et des empreintes digitales lorsqu'elles font suite à un éventuel traumatisme.

Sur la problématique de la propriété des données, la question est posée de savoir avec précision qui détient cette propriété, étant entendu qu'il existe en la matière une interaction entre l'émetteur de la carte, le cas échéant celui qui détient la donnée ou qui la maîtrise au plan juridique, s'il n'est pas le même que l'émetteur ; mais également le porteur lui-même qui peut dans certains cas adapter et modifier les données ou plus simplement encore être celui qui inscrit ces mêmes données au sein du titre d'identité.

Tel sera par exemple le cas de la partie porte folio personnel prévue dans la carte d'identité électronique au titre du programme INES.

S'agissant enfin de la propriété relative à la lecture et/ou à l'usage des informations, celle-ci doit nécessairement être définie par voie réglementaire tenant compte des spécificités de tel ou tel document.

Les trois questions de base qui se posent s'agissant de la problématique de la propriété sont les suivantes :

1) Faut-il poser la problématique de la propriété ? Y a-t-il ou non possibilité d'appropriation de tout ou partie des éléments figurant au sein des six classes ?

2) Si le principe d'une propriété est admis, peut-il y avoir une liberté sur les règles de propriété ou faut-il un cadre réglementaire qui vienne, pour chaque titre, fixer les règles de propriété de chacune des classes ? Et dans cette hypothèse, s'agirait-il d'une règle d'ordre public ou supplétive ?

3) Enfin, si le principe d'une règle légale est posée qui viendrait traiter la question de la « propriété », quelles pourraient être les règles alors arrêtées tant en matière de propriété intellectuelle, de propriété matérielle que de cessibilité ?

Pour le groupe de travail, la problématique de la propriété est une question qui devrait relever de la seule responsabilité de l'émetteur.

Se pose cependant une problématique particulière en matière de multiservices car, si la propriété est celle de l'émetteur, alors, lorsque plusieurs services sont proposés au sein du même titre, la démarche d'identification du ou des responsables juridiques peut être plus délicate.

8. INFORMATIQUE ET LIBERTES

8.1 NOUVELLE REGLEMENTATION DES TRAITEMENTS DE DONNEES BIOMETRIQUES

La loi Informatique et libertés[21] a été amendée en août 2004 et protège pour la première fois les données biométriques comme des données particulièrement sensibles.

La loi prévoit un régime de formalités préalables à la mise en œuvre des traitements qui s'avère différent selon que les traitements sont mis en œuvre pour le compte de l'Etat ou non.

Les traitements de données à caractère personnel mis en oeuvre pour le compte de l'Etat qui portent sur des données biométriques nécessaires à l'authentification ou au contrôle de l'identité des personnes doivent être autorisés par décret en Conseil d'Etat pris après avis motivé et publié de la Commission nationale de l'informatique et des libertés[22].

Lorsque les traitements automatisés comportent des données biométriques nécessaires au contrôle de l'identité des personnes et ne sont pas mis en oeuvre pour le compte de l'Etat, ils doivent être autorisés par la Commission nationale de l'informatique et des libertés[23].

La biométrie utilisée à des fins de contrôle de l'identité des personnes, donc à des fins sécuritaires, est stigmatisée par la loi Informatique et libertés qui dans son article 25-8° la soumet à un régime très strict d'autorisation préalable : ce traitement est considéré comme étant susceptible de porter atteinte à la vie privée ou aux libertés.

Les traitements de données à caractère personnel mis en œuvre pour le compte de l'Etat qui portent sur des données biométriques nécessaires à l'authentification ou au contrôle de l'identité des personnes doivent quant à eux être autorisés par décret en Conseil d'Etat, pris après avis motivé et publié de la Cnil (article 27-2°).

Dans les autres cas, par exemple pour la biométrie dite de confort, il est possible de considérer que cette dernière est soumise au régime déclaratif commun, à savoir celui de la déclaration : le traitement peut être mis en œuvre après simple déclaration auprès de la Cnil et délivrance d'un récépissé de déclaration par cette dernière.

En revanche, il convient de noter que l'article 25 précité comporte des critères de rattachement qui peuvent en pratique - en fonction du contexte du projet déterminé - faire entrer la biométrie de confort en régime d'autorisation :

- interconnexion de fichiers d'une ou plusieurs personnes et dont les finalités sont différentes ;

[21] Loi 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée par la loi 2004-801 du 6 août 2004.
[22] Article 27 de la loi Informatique et libertés.
[23] Article 25 de la loi Informatique et libertés.

- utilisation de la biométrie dans un contexte où la finalité pourrait avoir pour conséquence ou objectif, du fait de la nature ou de la portée du traitement envisagé, d'exclure des personnes du bénéfice d'un droit, d'une prestation ou d'un contrat en l'absence de toute disposition législative ou réglementaire.

Il faut noter que la Cnil peut prendre une décision unique afin d'autoriser la mise en œuvre de traitements de données dès lors que les fichiers répondant à une même finalité, portent sur des catégories de données identiques et ont les mêmes destinataires ou catégories de destinataires.

Ceci permet de déclarer à la Cnil, par un simple engagement de conformité à cette autorisation unique, les traitements correspondant à cette décision.

A ce titre le groupe de travail pourrait établir une recommandation visant à proposer à la Cnil les termes d'une autorisation unique relative à des traitements de données biométriques ayant pour finalité l'identification des personnes.

8.2 DOCTRINE DE LA CNIL RELATIVE A L'UTILISATION DE SOLUTIONS BIOMETRIQUES

La Cnil a eu à plusieurs reprises l'occasion d'émettre des recommandations portant sur la mise en place de solutions biométriques, établissant une doctrine fixant de grandes orientations.

La biométrie est considérée comme un enjeu technologique actuel clé par la Cnil[24].

Dans son 24ème rapport annuel[25], le président de la Cnil précise sur ce point :

- « je pense, par exemple, à la biométrie qui incontestablement passe de l'âge de l'expérimentation à celui de l'application dans le domaine de la sécurité, au point d'apparaître comme un instrument décisif des politiques de contrôle aux frontières et de lutte contre le terrorisme. Mais à côté de cette dimension régalienne, la CNIL est aussi confrontée à des utilisations plus locales de simples contrôles d'accès. »

La Cnil a eu à connaître de cas mettant en œuvre les technologies et domaines suivants :

- empreinte digitale, contour de la main, iris et cite l'ADN comme entrant dans la famille des identifiants présentant un caractère biométrique ;

- utilisation des techniques pour renforcer la sécurité des accès à des locaux, contrôler les horaires de travail des salariés ou des agents publics.

La Cnil opère une distinction[26] entre les technologies biométriques selon qu'elles permettent ou non de générer des traces c'est-à-dire des données existantes pouvant être utilisées à posteriori à des fins de comparaison pour réaliser l'identification d'une personne présente dans un lieu à un moment déterminé.

[24] Communication de M. Philippe Lemoine, commissaire de la Cnil, devant la Cnil : Enjeux technologiques et la protection des données personnelles, 4 mars 2004.
[25] Cnil, 24ème rapport d'activité 2003.
[26] Biométrie : la position de la Cnil, 25 novembre 2004.

Elle classe parmi les techniques les plus sensibles celles qui reposent sur la reconnaissance de caractéristiques physiques qu'elle considère comme laissant des traces : empreintes digitales, ADN…

La Cnil pose un postulat selon lequel seul un impératif de sécurité peut rendre nécessaire la centralisation de données biométriques laissant des traces. La centralisation est définie par la Cnil comme regroupant les caractéristiques anthropométriques de plusieurs personnes que cela soit dans une base centrale ou dans un lecteur biométrique.

Dans les autres cas, elle recommande que les caractéristiques biométriques soient uniquement conservées sur un support individuel (carte à puce, ordinateur…).

En revanche, dans le cas de procédés biométriques considérés comme ne laissant pas de traces, la Cnil considère que la conservation des gabarits peut être réalisée indifféremment sur support individuel ou dans une base de données.

La Cnil a eu l'occasion, à plusieurs reprises, d'émettre des délibérations et des avis concernant la mise en place de solutions biométriques dans divers secteurs.

Le 22 mai 2003, elle rendait un avis relatif à l'utilisation de la reconnaissance de la morphologie de la main pour permettre l'accès à des établissements pénitentiaires[27]. Le ministre de la justice soumettait à la Cnil un projet d'arrêté pour la création d'un modèle type de traitement de données nominatives relatif à l'identité des détenus, avec production d'une carte d'identité infalsifiable et contrôle biométrique de la morphologie de la main.

La Cnil rend un avis favorable à ce projet d'arrêté en rappelant les principes de protection des données personnelles applicables à ce type de traitement.

Elle indique que la technique de reconnaissance par morphologie de la main ne soulève pas de difficulté particulière en ce qu'elle ne peut pas être mise en oeuvre à l'insu des personnes concernées contrairement à l'utilisation d'empreintes digitales.

La Cnil indique également qu'elle privilégie les projets ne prévoyant pas la création de bases de données biométriques centralisées dans la mesure où ceci pourrait permettre des interconnections de fichiers avec d'autres traitements.

Enfin, la Cnil revient sur l'importance du respect des principes de protection des données personnelles habituels. Ainsi, la durée de conservation des données biométriques doit être pertinente au regard de la finalité du traitement impliquant ainsi que les données soient effacées dès que les cartes d'accès aux établissements pénitentiaires ne sont plus utilisées et que les personnes concernées aient un droit d'accès direct aux informations les concernant.

[27] Cnil, délibération 03-027 du 22 mai 2003.

Quelques mois plus tard, la Cnil rendait un avis relatif à l'utilisation d'une reconnaissance par empreinte digitale permettant l'accès à un parc sportif et se déclarait défavorable à l'utilisation d'une telle technique biométrique dans ce cadre[28]. Pour justifier son avis, la Cnil précise que « les empreintes digitales sont des données biométriques qui « laissent des traces » pouvant ensuite être exploitées à des fins d'identification de personnes ». Cette technique biométrique constitue donc un risque d'atteinte aux libertés individuelles puisqu'elle pourrait être utilisée à des fins étrangères à la finalité du traitement. Par ailleurs, la création d'une base de données centralisée pourrait faciliter cette utilisation à des fins étrangères.

La Cnil ne se montre donc pas favorable à l'utilisation de la reconnaissance par empreinte digitale dans ce type de circonstance considérant que seules « des circonstances particulières ou l'exigence de sécurité et d'identification des personnes est impérieuse » justifient un tel procédé.

Elle confirme sa position en avril 2004 dans une délibération relative à la mise en oeuvre d'un dispositif de reconnaissance de l'empreinte digitale ayant pour finalité la gestion du temps de travail du personnel par le centre hospitalier de Hyères[29]. La Cnil considère en effet que « seul un impératif particulier de sécurité est susceptible de justifier la centralisation de données biométriques » et que l'utilisation d'empreintes digitales pouvant laisser des traces et ainsi être utilisées pour des fins étrangères constitue un risque particulier de violation des libertés fondamentales.

A l'inverse, le même jour, la Cnil rend une délibération relative à l'utilisation de la reconnaissance de l'empreinte digitale pour permettre l'accès des employés aux établissements publics Aéroports de Paris dans laquelle elle émet un avis favorable au projet présenté[30]. La Cnil constate en effet que le gabarit de l'empreinte digitale est stocké sur le badge seul, que la durée de conservation des données biométriques est limitée au temps pendant lequel les employés disposent du droit d'accès aux zones réservées de sûreté, ce qui permet au projet d'être adapté et proportionné à la finalité qui lui est assignée.

La Cnil a également eu l'occasion de confirmer sa préférence pour les techniques biométriques qui ne laissent pas de trace, telle que l'utilisation de la reconnaissance par l'iris ou par le contour de la main plutôt que celles laissant des traces comme la reconnaissance par empreintes digitales.

Ainsi, elle a rendu un avis défavorable à la création d'un système de contrôle d'accès à une cantine scolaire reposant sur l'enregistrement, dans une base de données, des empreintes digitales des élèves alors qu'elle a donné un avis positif à la même création reposant sur une technique biométrique différente, la reconnaissance du contour de la main.

[28] Cnil, délibération 03-065 du 16 décembre 2003.

[29] Cnil, délibération 04-018 du 8 avril 2004 relative à une demande d'avis présentée par le centre hospitalier de Hyères concernant la mise en oeuvre d'un dispositif de reconnaissance de l'empreinte digitale ayant pour finalité la gestion du temps de travail de son personnel.

[30] Cnil, délibération 04-017 du 8 avril 2004 relative à une demande d'avis de l'établissement public Aéroports de Paris concernant la mise en oeuvre d'un contrôle d'accès biométrique aux zones réservées de sûreté des aéroports d'Orly et de Roissy.

La Cnil a eu l'occasion de rappeler, de manière synthétique, quelle était sa position relative à l'utilisation de la biométrie[31]. Elle indique ainsi que les techniques biométriques peuvent être classées selon qu'elles représentent des techniques plus ou moins sensibles. Les techniques biométriques les plus sensibles sont celles qui reposent sur « la reconnaissance de caractéristiques physiques « laissant des traces » dans la vie quotidienne (empreinte digitale, ADN...) ».

Elle confirme également qu'il est nécessaire de privilégier le stockage des données biométriques sur un support individuel tel qu'une carte à puce ou un ordinateur et d'éviter le recours à une base de données centralisée.

La Cnil a encore eu l'occasion de se prononcer le 21 décembre 2004 sur la mise en place de visas biométriques lors d'une expérimentation dans sept consulats visant à relever les empreintes digitales des demandeurs de visa et de les enregistrer dans une base centralisée[32].

Elle a ainsi donné son avis sur un projet de décret, finalement pris le 25 novembre 2004, autorisant « la création à titre expérimental et pour une durée de deux ans d'une base de données recensant les empreintes digitales et la photographie numérisée des personnes sollicitant des visas dans sept postes consulaires et l'inscription de ces données dans une puce électronique associée aux visas délivrés ». La Cnil demandait notamment que les conditions de mise en oeuvre d'alimentation, de consultation, de mise à jour et d'effacement de la base de données centralisée soient définies dans le décret et que les demandeurs de visa n'ayant pas obtenu celui-ci voient leur empreinte digitale effacée de la base de données centralisée. Ce dernier point n'a pas été pris en compte et la Cnil estime que « ce choix fait courir le risque d'une stigmatisation des étrangers demandant un visa sans l'obtenir alors qu'il s'agit somme toute d'une procédure administrative normale dont l'issue défavorable ne préjuge pas des résultats d'une nouvelle demande et qui ne fait pas pour autant de la personne « refusée » un suspect ». Ce point est notamment repris dans le 25ème rapport de la Cnil[33].

8.3 EVALUER LES AVANTAGES ET LES INCONVENIENTS D'UN DISPOSITIF BIOMETRIQUE

La nécessité d'évaluer les avantages et les inconvénients des dispositifs biométriques ressort des recommandations faites par la Cnil dans le cadre de l'expérimentation d'un traitement automatisé de données à caractère personnel destiné à contrôler les conditions d'entrée et de séjour des étrangers en France et à la sollicitation d'un visa[34].

Dans ce cadre, la Cnil précise dans sa délibération d'octobre 2004 une grille de lecture qu'elle souhaite mettre en œuvre afin d'évaluer les avantages et les inconvénients du dispositif biométrique :

- du protocole d'évaluation qui aura été établi, lequel devrait intégrer la prise en compte d'incidents ou de défaillances techniques graves ou une défaillance due à une compromission interne ;

[31] Biométrie : la position de la Cnil, 25 novembre 2004.
[32] L'expérimentation de visas biométriques : la position de la Cnil, 21 décembre 2004 – écho des séances.
[33] 25ème rapport d'activité de la Cnil 2004, « l'identification biométrique des voyageurs ».
[34] Délibération 04-075 du 5 octobre 2004.

- du descriptif des procédures prévues dans l'hypothèse où une personne bénéficiaire d'un visa valide se verrait refuser son entrée en France après comparaison de ses empreintes avec les informations la concernant enregistrées dans le composant associé à son visa ou dans la base expérimentale ;

- d'un bilan des éventuels avantages retirés de l'enregistrement dans la base centralisée des empreintes des dix doigts des intéressés ;

- d'un bilan concernant les différents composants électroniques testés et les avantages et inconvénients respectifs qu'ils présentent au regard de la finalité du traitement, comparés à ceux d'une base centralisée ;

- d'un rapport d'évaluation de la fiabilité des dispositifs et outils de lecture des empreintes digitales et du contenu du composant électronique associé au visa installés dans les postes frontières.

9. CONCLUSION

Le groupe de travail sur les biométries, après s'être réuni au cours de réunions mensuelles et avoir identifié et analysé les thématiques relevant de problématiques liées au développement des biométries, a souhaité synthétiser le résultat de ses réflexions dans ce livre blanc.

Les professionnels de la biométrie estiment aujourd'hui que la maturité du secteur et son développement impose la rédaction d'une « Charte des biométries ».

La rédaction d'une charte est d'une manière générale l'expression première du droit réglementant une nouvelle technologie. Le développement de nombreuses chartes en témoigne.

Ainsi ont d'ores et déjà été mises en place la charte sur l'offre de musique et sur la lutte contre la piraterie, la charte des prestataires de services d'hébergement en ligne ou encore la charte Marianne, destinée à tous les services administratifs de l'État et dont l'objet est de réglementer l'accueil des usagers.

Il s'agit ainsi de privilégier une auto-régulation de la biométrie par la rédaction d'une charte qui lui est dédiée.

D'une manière générale, les chartes relatives aux nouvelles technologies peuvent revêtir différentes formes. Elles peuvent établir des règles de droit ou fixer des objectifs à réaliser.

Le groupe de travail sur la biométrie a pour volonté de définir des engagements, des objectifs et des principes qui viendront guider la mise en œuvre de la biométrie à grande échelle.

En l'état actuel, la biométrie n'est pas encadrée par un droit construit et dédié à cet effet. La charte des biométries sera donc la première expression du droit l'encadrant et prendra la forme, comme peut l'être la coutume, d'une communauté de pensée relative à un élément juridique.

Une telle charte pourrait être suffisante et ne pas faire l'objet de modifications ou de versions ultérieures.

Cependant si aucune modification du droit positif ne prend en compte le développement de la biométrie ou si au contraire des règles de droit très contraignantes venaient à être mises en place, la charte des biométries serait révisée par le groupe de travail afin de l'adapter à son cadre juridique.

Ainsi, aux yeux des membres du groupe de travail, la charte n'est qu'une première étape et celui-ci s'engage à envisager un autre stade de réflexion :

- développer un engagement qualité afin d'obtenir un label de la Cnil relatif aux systèmes biométriques ;

- maintenir l'évolutivité de la charte des biométries en tenant compte de l'évolution du cadre juridique qui lui est applicable.

10. ANNEXES

- Annexe 1 : Charte des biométries ;
- Annexe 2 : Présentation des membres du groupe de travail ;
- Annexe 3 : Technologies biométriques ;
- Annexe 4 : Bibliographie ;
- Annexe 5 : Référentiel légal ;
- Annexe 6 : Liste des avis de la Cnil ;
- Annexe 7 : Recommandations et conclusions du rapport Cabal et du rapport du Conseil de l'Europe.

ANNEXE 1

CHARTE DES BIOMETRIES

Le groupe de travail des industriels et utilisateurs des biométries,

Après avoir :

- organisé plusieurs réunions de travail réunissant des industriels et utilisateurs des biométries ;

- examiné les questions relatives à :

    - La définition de la biométrie ;
    - Les notions d'identification et d'authentification ;
    - Les problématiques de responsabilités et de garanties ;
    - Les problématiques relatives à la propriété ;
    - Les questions relatives au droit de la protection des données à caractère personnel ;
    - La problématique propre au déploiement des biométries dans l'entreprise et de droit du travail ;

- analysé les avis de la Cnil et la réglementation applicable à la biométrie ;

Considérant que :

- la biométrie est au service des libertés publiques et participe à la protection des personnes ;

- les entreprises ont un droit légitime à expérimenter les solutions biométriques ;

- les biométries ne sont pas liberticides par nature mais qu'il convient de sanctionner tout usage illicite ;

- la réglementation et la technique sont parfaitement à même de permettre d'identifier et de sanctionner des comportements illicites ;

- la biométrie est multiple tant par les techniques proposées que par les finalités recherchées ;

- la biométrie est un processus d'identification forte qui implique la présence de la personne identifiée ;

- la biométrie s'entend de technologies non-intrusives au corps humain et exclue de fait la génétique ;

*R **ecommande que :***

- soit privilégié le droit à l'expérimentation sur le principe de précaution ;

- soit privilégié les solutions de contrôle des usages au principe d'interdiction ;

- le développement de la biométrie ne soit freinée par une législation « sui generis » contraignante ;

- les obligations et le régime de responsabilité des professionnels de la biométrie soient laissés à l'appréciation et à la négociation des parties ;

- les notions d'identification et d'authentification soient mieux définies par la loi ;

- le soin soit laissé aux industriels et utilisateurs de déterminer les conditions relatives à la propriété ;

- les entreprises et organismes intègrent dans leurs chartes internes d'utilisation des systèmes d'information les conditions relatives à l'implémentation de technologies biométriques ;

- la CNIL propose une norme d'autorisation dédiée à la biométrie et à son interopérabilité s'agissant des biométries de sécurité ;

- la CNIL mette en place une méthode d'audit relative aux solutions biométriques dont les industriels pourront s'inspirer pour les proposer à leurs clients ;

- la carte d'identité biométrique soit multifonction et permette aux citoyens d'utiliser un volet d'informations personnelles à des fins privatives ;

- les pouvoirs publics mettent en œuvre des solutions homogènes et admises par tous qui permettraient de connaître l'état de l'art et les meilleurs pratiques en matière de biométrie.

*S**'engage à :***

- se tenir à la disposition de la CNIL et des pouvoirs publics pour apporter son éclairage sur les différentes solutions biométriques ;

- soutenir la mise en place du programme INES ;

- assumer leur obligation de conseil, d'alerte et de mise en garde relative aux risques encourus par les utilisateurs des systèmes biométriques ;

- assurer une niveau de sécurité et de performance des solutions biométriques contractuellement défini ;

- proposer des solutions de contournement optionnelles en cas de faille des systèmes biométriques proposés ;

- développer des services de veille technologique ayant pour objet d'assurer un niveau de sécurité adapté aux risques d'attaques ;

- favoriser la création d'une structure pérenne dédiée à la biométrie qui serait une force de propositions ;

- maintenir à jour la présente charte des biométries en tenant compte du développement du cadre juridique relatif à la biométrie.

ANNEXE 2

PRESENTATION DES MEMBRES DU GROUPE DE TRAVAIL

Alain BENSOUSSAN, Avocat à la Cour d'appel de Paris

Alain Bensoussan, a fondé en 1978 un cabinet entièrement dédié au droit des technologies avancées et, tout particulièrement, au droit de l'informatique et au droit des télécommunications.

ACTIVITES COMPLEMENTAIRES

- Arbitre auprès de l'Organisation mondiale de la propriété intellectuelle
- Tiers-aviseur auprès du Centre de Médiation et d'Arbitrage de Paris
- Membre du Conseil de Présidence de l'Union internationale des avocats (UIA), Conseiller du Président
- Chargé de conférences à l'Ecole centrale de Paris
- Président d'honneur et membre du Conseil d'administration de l'Association française de droit de l'informatique et de la télécommunication (AFDIT)
- Chroniqueur juridique dans la revue 01 INFORMATIQUE

OUVRAGES

- "Informatique, Télécoms, Internet", Editions Francis Lefebvre, 3ème éd. 2004
- "Les arrêts - tendances de l'informatique", éditions Hermès, 2003
- "Informatique, Télécoms, Internet", Editions Francis Lefebvre, 2ème éd. 2001
- "Les arrêts - tendances de l'internet", éditions Hermès, 2000
- "Cryptologie et signature électronique : aspects juridiques", éditions Hermès, 1999
- "Commerce électronique : aspects juridiques", éditions Hermès, 1998

ALAIN BENSOUSSAN - AVOCATS

ALAIN BENSOUSSAN SELAS
29, rue du Colonel Pierre Avia – 75508 Paris Cedex 15
www.alain-bensoussan.com

Equipe : 120 personnes

Créé en 1978, le cabinet s'est orienté, dès l'origine, vers le droit de l'informatique. Autour de son coeur de métier constitué par l'informatique et les communications électroniques, il se consacre, tant en conseil qu'en contentieux, à de nombreux secteurs relevant des technologies avancées, associant la connaissance de ce secteur technique et du droit spécifique qui s'y applique, à celle des grandes catégories du droit. Il met l'accent sur les stratégies innovantes et l'élaboration de concepts nouveaux anticipant sur les questions de droit générées par le développement des nouvelles technologies. Installé à Paris, le cabinet s'est développé en région avec un bureau secondaire à Lyon et à Grenoble.

L'équipe, composée d'avocats et de juristes, apporte son savoir-faire suivant les quatre axes de l'exercice de son métier :

- contrat et pilotage de projet ;
- conseil, audit et assistance juridique ;
- précontentieux, contentieux et arbitrage ;
- infogérance juridique.

Il est privilégié une approche concrète des dossiers grâce à une connaissance approfondie des techniques et des métiers

Eric BARBRY, Avocat au Barreau de Paris

Directeur du Pôle « Communications électroniques »

Eric Barbry dirige le pôle « Communications électroniques » du Cabinet Alain Bensoussan qui regroupe les départements « Internet », « Industrie des télécoms », « Electronique de défense » et « Informatique et libertés ». Il assure la direction du département Internet. Eric Barbry a débuté sa carrière comme juriste d'entreprise à la Cité des Sciences et de l'Industrie. Il est l'auteur de plusieurs ouvrages et articles consacrés au droit de l'Internet et au multimédia. Il est membre fondateur de Cyberlex.

Tél : 01 41 33 35 35 – Fax 01 41 33 35 36 - Portable : 06 09 95 17 89
Adresse mail : eric-barbry@alain-bensoussan.com

ALAIN BENSOUSSAN - AVOCATS

ALAIN BENSOUSSAN SELAS
29, rue du Colonel Pierre Avia – 75508 Paris Cedex 15
www.alain-bensoussan.com

Equipe : 120 personnes

Créé en 1978, le cabinet s'est orienté, dès l'origine, vers le droit de l'informatique. Autour de son coeur de métier constitué par l'informatique et les communications électroniques, il se consacre, tant en conseil qu'en contentieux, à de nombreux secteurs relevant des technologies avancées, associant la connaissance de ce secteur technique et du droit spécifique qui s'y applique, à celle des grandes catégories du droit. Il met l'accent sur les stratégies innovantes et l'élaboration de concepts nouveaux anticipant sur les questions de droit générées par le développement des nouvelles technologies. Installé à Paris, le cabinet s'est développé en région avec un bureau secondaire à Lyon et à Grenoble.

L'équipe, composée d'avocats et de juristes, apporte son savoir-faire suivant les quatre axes de l'exercice de son métier :

- contrat et pilotage de projet ;
- conseil, audit et assistance juridique ;
- précontentieux, contentieux et arbitrage ;
- infogérance juridique.

Il est privilégié une approche concrète des dossiers grâce à une connaissance approfondie des techniques et des métiers

ANNEXE 3

LES TECHNOLOGIES BIOMETRIQUES

Principes d'utilisation d'une solution biométrique

L'utilisation d'une solution biométrique, quelle qu'elle soit, met en oeuvre le même processus technique.

Dans un premier temps, l'outil biométrique collecte un échantillon d'où est extraite une caractéristique biométrique.

Celle-ci permet alors la création de la donnée ou du gabarit biométrique.

Le gabarit biométrique est conservé dans une base de données ou tout autre élément de conservation tel qu'une puce électronique pour pouvoir être utilisé à titre d'élément de référence.

Dans un second temps, l'outil biométrique collecte un échantillon dont il est créé un gabarit biométrique. Ce gabarit biométrique est alors comparé au premier gabarit présent dans la base de données ou la puce électronique[35].

La comparaison des gabarits biométriques peut s'effectuer « de l'un à l'autre » (« one-to-one ») ou « de l'un à plusieurs » (« one-to-many »).

La comparaison « one-to-many » est utilisée pour permettre l'identification ou la reconnaissance d'une personne par ses identifiants biométriques.

Lors d'une telle identification, le gabarit biométrique de la personne est comparé aux gabarits biométriques contenus dans une base de données, ce qui permet de reconnaître l'identité d'une personne parmi celles d'un groupe de personnes.

La comparaison des gabarits biométriques « one-to-one » permet quant à elle d'authentifier une personne comme étant celle qu'elle prétend être.

Dans un tel cas, le gabarit biométrique de la personne est comparé à un seul autre gabarit biométrique pré-enregistré sur un support biométrique, tel qu'une carte à puce. Il n'est dès lors pas question de base de données biométriques.

[35] OCDE, « Biometric-based technologies », Directorate for science, technology and industry, Committee for information, computer and communications policy, Working party on information security and privacy, 23 décembre 2004.

Principes de mesure de la fiabilité des solutions biométriques

Il est unanimement reconnu que le recours à des solutions biométriques n'est pas fiable à 100 % et qu'un certain nombre d'erreurs peut se produire.

Un premier risque d'erreur peut résulter du fait que plusieurs personnes soient détentrices de caractéristiques biométriques dont les points de comparaison sont identiques. Dans un tel cas, l'outil biométrique utilisé pour les comparer pourrait commettre une erreur en confondant les personnes concernées.

A titre d'exemple, le risque de confondre deux empreintes digitales serait, pour dix points de comparaison, de un sur un million et pour quatorze à dix-sept points de comparaison de un sur dix-sept milliards[36].

D'autres risques d'erreurs sont également possibles. L'outil biométrique utilisé peut reconnaître une personne qui n'aurait pas dû être reconnue ou, au contraire, rejeter une personne qui aurait dû être acceptée.

Ces risques sont évalués et calculés sous forme de taux de fausse acceptation et de taux de faux rejet.

Le taux de fausse acceptation « false match rate » ou « false acceptation rate » détermine le rapport entre le nombre de personnes non autorisées qui ont été acceptées par le système biométrique et le nombre total de personnes non autorisées qui se sont présentées.

Le taux de faux rejet mesure quant à lui le rapport entre le nombre de personnes autorisées et ayant été refusées de manière erronée par le système biométrique et le nombre total de personnes autorisées s'étant présentées[37].

Présentation des différentes techniques biométriques existantes

Les différentes techniques biométriques peuvent être classées selon différentes catégories. Ainsi, il existe les techniques biométriques physiologiques ou anatomiques dans lesquelles peuvent être classés :

- l'empreinte digitale : La reconnaissance par empreinte digitale est la technique biométrique la plus ancienne, utilisée dans le contrôle policier des individus dès le début du XXème siècle[38].

[36] Criminalistique et criminologie – http://www.ifrance.com in Rapport du député Christian Cabal de l'Office parlementaire d'évaluation des choix scientifiques et technologiques sur les méthodes scientifiques d'identification des personnes à partir des données biométriques et les techniques de mise en oeuvre , n° 938, Assemblée nationale, n° 355, Sénat, juin 2003.

[37] Rapport du député Christian Cabal de l'Office parlementaire d'évaluation des choix scientifiques et technologiques sur les méthodes scientifiques d'identification des personnes à partir des données biométriques et les techniques de mise en oeuvre , n° 938, Assemblée nationale, n° 355, Sénat, juin 2003.

[38] Rapport du député Christian Cabal de l'Office parlementaire d'évaluation des choix scientifiques et technologiques sur les méthodes scientifiques d'identification des personnes à partir des données biométriques et les techniques de mise en oeuvre , n° 938, Assemblée nationale, n° 355, Sénat, juin 2003.

La technique repose sur la prise de l'image d'un doigt par un capteur et sur l'analyse par un logiciel des emplacements remarquables de l'empreinte digitale. Ces derniers sont appelés des « minuties ». Il s'agit notamment des sillons, crêtes, vallées, arches, boucles et tourbillons qui peuvant être relevés sur une empreinte digitale.

Le logiciel utilisé transforme les minuties en codes informatiques. Plus le nombre de minuties analysées est élevé, moins le risque d'erreur est élevé. Selon les systèmes techniques utilisés, l'exactitude de la reconnaissance par empreinte digitale sera plus ou moins fiable.

Un lecteur prend une image du doigt qui sera stockée dans une base de données. La personne utilisant le système biométrique devra ensuite placer son doigt sur un lecteur permettant l'accès à des locaux protégés.

La capture d'images initiale peut être réalisée grâce à des lecteurs reposant sur différentes techniques. Ainsi, il peut s'agir de lecteurs optiques (appareil photo numérique), capacitives (maillage de pixels sensible), radio (transmission d'une onde radio de faible intensité au doigt), par pression (surface piézo-électrique sensible à la pression), MEMS (micro-électro-mecanical system), thermiques (pyro-électrique convertissant une différence de température en une différence de tension) et par ultrasons.

Les deux images d'empreintes digitales comparées ne sont jamais totalement identiques. Cependant, la comparaison de deux empreintes digitales appartenant à la même personne doit donner un niveau élevé de similitudes. Le seuil d'acceptation sera donc déterminé par les utilisateurs du système biométrique[39].

La technique d'empreinte digitale n'est pas la technique biométrique la plus fiable. Elle est notamment moins fiable que le recours à la technique biométrique de l'iris. Le taux de faux rejet peut ainsi atteindre de 2,5 % à 11 % selon le type de lecteur utilisé[40].

L'empreinte digitale est la technique la plus largement utilisée et, en conséquence, celle sur laquelle les industriels et utilisateurs ont le plus de recul.

En outre, les nouvelles applications miniatures permettent d'intégrer de nouvelles solutions biométriques utilisant l'empreinte digitale dans des technologies grand public telles que les téléphones portables, les ordinateurs PC, etc...

Le coût de cette technique reste peu élevé en comparaison des autres techniques existantes ayant des taux de faux rejet et de fausse acceptation supérieurs à ceux de l'empreinte digitale.

Cependant, certaines difficultés peuvent apparaître lors de l'utilisation de l'empreinte digitale dans le cadre d'un système biométrique.

[39] Rapport du député Christian Cabal de l'Office parlementaire d'évaluation des choix scientifiques et technologiques sur les méthodes scientifiques d'identification des personnes à partir des données biométriques et les techniques de mise en oeuvre , n° 938, Assemblée nationale, n° 355, Sénat, juin 2003

[40] Rapport du député Christian Cabal de l'Office parlementaire d'évaluation des choix scientifiques et technologiques sur les méthodes scientifiques d'identification des personnes à partir des données biométriques et les techniques de mise en oeuvre , n° 938, Assemblée nationale, n° 355, Sénat, juin 2003.

En effet, outre le fait que l'utilisation de cette technique renvoie à l'image policière du début du siècle, les cas de faux rejet peuvent être relativement importants.

La personne utilisant le système biométrique peut ainsi avoir les doigts sales ou abîmés. Le système peut aussi permettre un certain nombre de fausses acceptations dans la mesure où le moulage d'un doigt, ou encore un doigt coupé (ce qui pose en outre un problème de sécurité), peut être utilisé pour fausser le système biométrique.

La technique d'empreinte digitale est généralement utilisée pour tous les contrôles d'accès accessibles au grand public. Ce système a d'ailleurs été retenu par le Conseil européen pour la mise en place des passeports des citoyens de l'Union européenne contenant des éléments de biométrie[41] ;

- l'iris : La reconnaissance biométrique par l'iris est utilisée depuis les années 1950 et occupe aujourd'hui environ 6 % de parts du marché, cette technique étant relativement chère à mettre en place et sujette à une opposition culturelle relativement forte.

Une caméra scanne l'iris de l'oeil d'un individu, c'est-à-dire la zone colorée de l'oeil. Les caractéristiques relatives aux stries qui forment la base des muscles ciliaires du cristallin et l'enchevêtrement des tubes qui participent à la forme de l'iris sont enregistrées dans une base de données.

Elles permettront ensuite la comparaison avec l'iris d'un individu, sachant que si les deux iris d'un même individu ont à peu près la même couleur, leur forme est totalement différente. L'avantage de cette technique tient principalement à sa fiabilité, les caractéristiques retenues n'évoluant quasiment pas au cours de la vie[42].

D'autre part, cette technique est peu intrusive dans la mesure où la caméra peut scanner l'oeil à distance, la personne concernée devant simplement fixer une caméra.

Cependant, des inconvénients subsistent dans la mesure où l'analyse de l'iris d'une personne pourrait permettre d'obtenir des informations sur la santé de celle-ci. Par ailleurs, les techniques biométriques de reconnaissance par l'iris font actuellement l'objet de brevets, notamment américains.

Cette technique est favorisée par les pays anglo-saxons au contraire des pays européens qui préfèrent recourir à l'empreinte digitale.

(Analyse des choix différents relatifs aux techniques biométriques utilisées aux Etats-Unis, au Japon et dans le reste du monde) ;

[41] Règlement (CE) n°2252/2004 du Conseil du 13 décembre 2004 établissant des normes pour les éléments de sécurité et les éléments biométriques intégrés dans les passeports et les documents de voyage délivrés par les Etats membres.

[42] Rapport du député Christian Cabal de l'Office parlementaire d'évaluation des choix scientifiques et technologiques sur les méthodes scientifiques d'identification des personnes à partir des données biométriques et les techniques de mise en oeuvre , n° 938, Assemblée nationale, n° 355, Sénat, juin 2003

- la reconnaissance faciale : La technique biométrique de reconnaissance faciale s'est développée récemment, dans les années 1990, et occuperait aujourd'hui environ 15 % de parts de marché[43].

Une caméra capture l'image du visage d'une personne. Cette image est ensuite enregistrée dans une base de données sur un ordinateur. Un logiciel recherche alors les caractéristiques du visage permettant ensuite de le comparer à des images ultérieures. Ces caractéristiques sont notamment l'écart entre les deux yeux, l'écartement des narines, la largeur de la bouche ou l'analyse globale de l'image du visage par des techniques statistiques.

Cette technologie biométrique est très fiable lorsque la personne est immobile, elle l'est au contraire beaucoup moins lorsque le visage est en mouvement. Le taux de faux rejet peut alors atteindre 17 %[44].

Bien qu'étant d'une utilisation relativement simple, cette technique a de nombreux désavantages.

En effet, le système utilisé est relativement coûteux et les résultats obtenus peu fiables. Le taux de fausse acceptation et de faux rejet dépend notamment des changements que peut avoir subi le visage tels que le maquillage, la pilosité, la présence ou l'absence de lunettes, le vieillissement et l'expression d'une émotion.

En outre, l'environnement dans lequel se trouve l'individu au moment de la captation de l'image par la caméra a un impact sur la fiabilité du système. Les conditions d'éclairage peuvent ainsi rendre l'image peu exploitable.

Enfin, ce système ne permet pas de distinguer des jumeaux.

- la géométrie de la main : la forme de la main est mesurée par un outil biométrique généralement à infrarouge qui retient des caractéristiques relatives à la longueur, à l'épaisseur et à la position des doigts. Cette technique est peu intrusive et simple d'utilisation. Elle nécessite cependant la coopération de la personne et s'avère moins fiable que l'empreinte digitale ;

- la thermographie du visage : l'outil biométrique, utilisant une caméra infrarouge, mesure la répartition des zones de chaleur sur le visage. Cette technique a l'avantage de permettre de distinguer des jumeaux mais est actuellement très chère, étant encore à un stade expérimental ;

- le réseau veineux : l'outil biométrique sonde par infrarouge le dessin du réseau veineux d'un élément du corps humain qui peut être un doigt ou la main. Cette technique est actuellement à un stade expérimental mais pourrait permettre une prise d'empreinte sans contact difficile à déjouer ;

- la rétine : l'outil biométrique retient comme caractéristiques les vaisseaux sanguins de la rétine. Cette technique bien que très fiable est cependant particulièrement intrusive, obligeant la personne à accepter qu'on éclaire son oeil. Par ailleurs, cette technique est particulièrement chère ;

[43] Rapport du député Christian Cabal de l'Office parlementaire d'évaluation des choix scientifiques et technologiques sur les méthodes scientifiques d'identification des personnes à partir des données biométriques et les techniques de mise en oeuvre , n° 938, Assemblée nationale, n° 355, Sénat, juin 2003.

[44] Rapport du député Christian Cabal de l'Office parlementaire d'évaluation des choix scientifiques et technologiques sur les méthodes scientifiques d'identification des personnes à partir des données biométriques et les techniques de mise en oeuvre , n° 938, Assemblée nationale, n° 355, Sénat, juin 2003.

- la géométrie du doigt : cette technique fonctionne comme la technique de reconnaissance de la géométrie de la main en utilisant seulement un ou deux doigt(s) ;

- la géométrie de l'oreille : cette technique biométrique est encore à l'heure actuelle à un stade expérimental ;

- l'odeur du corps : cette technique est également à l'heure actuelle à un stade expérimental.

Il existe une autre catégorie de techniques biométriques qualifiées de comportementales. Parmi celles-ci peuvent être classées :

- la reconnaissance vocale : l'outil biométrique retient comme caractéristique la fréquence, l'intensité ou la tonalité de la voix. Cette technique a l'avantage d'être communément bien acceptée, de ne pas imposer la coopération de la personne mais peut faire l'objet d'une fraude importante notamment par l'enregistrement de la voix ;

- la signature dynamique : l'outil biométrique analyse la manière dont une personne signe ;

- la frappe dynamique du clavier : cette technique biométrique mesure les caractéristiques de frappe sur un clavier et notamment la force de frappe. Cette technique, peu fiable, apparaît plus comme une technique de substitution d'un code que comme une technique de sécurité ;

- la démarche : cette technique biométrique analyse les caractéristiques de la démarche d'un individu. A l'heure actuelle, cette technique est encore expérimentale[45].

[45] « Laissez-passer biométriques : les techniques », Sciences et Avenir, septembre 2004.

ANNEXE 4

BIBLIOGRAPHIE

- Organisation de Cooperation et de Développement Economiques, « Biometric-based technologies », Directorate for science, technology and industry, Committee for information, computer and communications policy, Working party on information security and privacy, 23 décembre 2004 ;

- Machine Readable Travel Documents (Doc 9303) Part 1 — Machine Readable Passports, OACI ;

- Machine Readable Travel Documents (Doc 9303) Part 2 — Machine Readable Visas, OACI ;

- Machine Readable Travel Documents (Doc 9303) Part 3 — Size 1 and Size 2 Machine Readable Official Travel Documents - 2nd Edition, OACI ;

- Biometrics deployment of Machine Readable Travel Documents 2004 OACI, 21 mai 2004 et Annex A - Photograph Guidelines, Annex B - Facial Image Size Study 1, Annex C - Facial Image Size Study 2, Annex D - Face Image Data Interchange, Annex E - Iris Image, Annex F - Fingerprint Image, Annex G - Fingerprint Minutiae, Annex H - Fingerprint Pattern, Annex I - Use of Contactless Integrated Circuits, Annex J - ICAO May 2003 Press Release, Annex K - ICAO Supplementary Requirements to ISO14443 - v2 , Annex L - ePassports Data Retrieval Test Protocol ;

- PKI for Machine Readable Travel Documents offering ICC read-only access v1.1, OACI ;

- Common methodology for Information Technology Security Evaluation, Biometric Evaluation Methodology, Août 2002 ;

- Rapport d'étape sur l'application des principes de la convention 108 à la collecte et au traitement des données biométriques, Comité consultatif de la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (T-PD), Direction générale des affaires juridiques, Conseil de l'Europe ;

- Biometrics At the Frontiers :Assessing the impact on Society – For the European Parliament Committee on Citizens, Freedoms and rights, Justice and Home Affairs (LIBE), European Commission, 2005;

- Le Programme INES (identité nationale électronique sécurisée), Ministère de l'intérieur, de la sécurité intérieure et des libertés locales, secrétariat général direction de programme INES ;

- 25ème rapport d'activité de la Cnil 2004, « l'identification biométrique des voyageurs » ;

- 24ème rapport d'activité de la Cnil 2003, chapitre 1 « L'impératif de sécurité et ses contreparties » ;

- 22ème rapport d'activité de la Cnil 2001, « un siècle de biométrie » ;

- 20ème rapport d'activité de la Cnil 2000, chapitre 4 « Les contrôle d'accès par biométrie » ;

- Rapport du député Christian Cabal de l'Office parlementaire d'évaluation des choix scientifiques et technologiques sur les méthodes scientifiques d'identification des personnes à partir des données biométriques et les techniques de mise en oeuvre , n° 938, Assemblée nationale, n° 355, Sénat, juin 2003 ;

- Biometric data specification for personal identity verification, National Institute of Standards and Technology, Department of Commerce, USA, 24 janvier 2005;

- La biométrie au Japon, Arnaud Vigier, Ambassade de France au Japon, mai 2003.

ANNEXE 5

REFERENTIEL LEGAL

1. Au niveau international

- Recommandation n°R (92) 1 du 10 février 1992 du Comité des ministres du Conseil de l'Europe aux Etats membres sur l'utilisation des analyses de l'acide désoxyribonucléique (ADN) dans le cadre du système de justice pénale.

- Recommandation n°R (87) du 17 septembre 1987 du Comité des ministres du Conseil de l'Europe aux Etats membres visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police.

1. Au niveau de la Communauté européenne

- Règlement (CE) n°2252/2004 du Conseil du 13 décembre 2004 établissant des normes pour les éléments de sécurité et les éléments biométriques intégrés dans les passeports et les documents de voyage délivrés par les Etats membres.

- Avis n°7/2004 du Groupe de travail Article 29 sur l'insertion d'éléments biométriques dans les visas et les titres de séjour en tenant compte de la création du système d'information Visas (VIS) du 11 août 2004.

- Projet de rapport du Parlement européen du 10 mars 2004 sur la proposition de règlement du Conseil modifiant le règlement (CE) n°1030/2002 établissant un modèle uniforme de titre de séjour pour les ressortissants de pays tiers et le règlement (CE) n°1683/95 établissant un modèle type de visa.

- Proposition de règlement du Conseil modifiant le règlement (CE) n°1683/95 établissant un modèle type de visa et Proposition de règlement du Conseil modifiant le règlement (CE) n°1030/2002 établissant un modèle uniforme de titre de séjour pour les ressortissants de pays tiers du 24 septembre 2003.

- Résolution du Conseil de l'Union européenne du 25 juin 2001 relative à l'échange des résultats des analyses d'ADN (2001/C 187/01).

- Résolution du Conseil de l'Union européenne du 9 juin 1997 relative à l'échange des résultats des analyses d'ADN (1997/C 193/02).

- Directive 95/46/CE du Parlement européen et du Conseil 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 de ces données.

2. En France

- Décret n°2004-1266 du 25 novembre 2004 pris pour l'application de l'article 8-4 de l'ordonnance n°45-2658 du 2 novembre 1945 relative aux conditions d'entrée et de séjour des étrangers en France et portant création à titre expérimental d'un traitement automatisé de données à caractère personnel relatives aux ressortissants étrangers sollicitant la délivrance d'un visa.

- Code de la sécurité sociale, articles L161-31 et R 161-33-1 relatifs à la carte d'assurance maladie (modifié le 6 août 2004).

- Loi n°2004-810 du 13 août 2004 relative à l'assurance maladie.

- Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi 2004-801 6 août 2004 (articles 25 et 27).

- Loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.

- Loi n°2003-1119 du 26 novembre 2003 relative à la maîtrise de l'immigration, au séjour des étrangers en France et à la nationalité (article 12).

- Arrêté du 10 juin 2003 portant création d'un système de reconnaissance biométrique de l'identité des individus.

- Loi n° 2002-303 du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé.

- Circulaire CRIM 2000-08 F1 du 10 octobre 2000 présentant les dispositions relatives au fichier national automatisé des empreintes génétiques et au service central de préservation des prélèvements biologiques (Reproduite sous l'art. 706-54 du Code de procédure pénale, Ed. Dalloz).

- Code de procédure pénale, Art. R. 53-9 à R. 53-21 sur le fichier national automatisé des empreintes génétiques et du service central de préservation des prélèvements biologiques (codification du Décret n°2000-413 du 18 mai 2000).

- Code de procédure pénale, Art. A. 38 sur le fichier national automatisé des empreintes génétiques (codification de l'arrêté du 18 mai 2000).

- Code de procédure pénale, Art.706-54 à 706-56 relatifs au fichier national automatisé des empreintes génétiques (art.29 de la loi du 8 mars 2003 pour la sécurité intérieure).

ANNEXE 6

LISTE DES AVIS DE LA CNIL

- Cnil, délibération 04-075 du 5 octobre 2004 portant avis sur le projet de décret en conseil d'Etat pris pour l'application de l'article 8-4 de l'ordonnance du 2 novembre 1945 relative aux conditions d'entrée et de séjour des étrangers en France et portant création à titre expérimental d'un traitement automatisé de données à caractère personnel relatives aux ressortissants étrangers sollicitant la délivrance d'un visa ;

- Cnil, délibération 04-017 du 8 avril 2004 relative à une demande d'avis de l'établissement public aéroport de Paris concernant la mise en oeuvre d'un contrôle d'accès biométrique aux zones réservées de sûreté des aéroports d'Orly et de Roissy ;

- Cnil, délibération 04-018 du 8 avril 2004 relative à une demande d'avis présentée par le Centre hospitalier de Hyères concernant la mise en oeuvre d'un dispositif de reconnaissance de l'empreinte digitale ayant pour finalité la gestion du temps de travail de ses personnels ;

- Cnil, délibération 03-065 du 16 décembre 2003 portant avis sur le traitement automatisé d'informations nominatives mis en oeuvre par la Mairie de Levallois-Perret et destiné à contrôler l'accès au Roller-Parc par la reconnaissance des empreintes digitales ;

- Cnil, délibération 03-027 du 22 mai 2003 portant avis sur le projet d'arrêté du ministre de la Justice portant création d'une application informatique destinée à vérifier l'identité des détenus par reconnaissance de la morphologie de la main ;

- Cnil, délibération 99-052 du 28 octobre 1999 portant avis sur un projet de décret modifiant le code de procédure pénale et relatif au fichier national automatisé des empreintes génétiques et au service central de préservation des prélèvements biologiques ;

- Cnil, délibération 86-76 du 1er juillet 1986 portant avis sur un projet de décret relatif à la création d'un système de fabrication et de gestion informatisé des cartes nationales d'identité ;

- Cnil, délibération 86-105 du 21 octobre 1986 portant avis sur le relevé d'une empreinte digitale à l'occasion d'une demande de carte nationale d'identité ;

- Cnil, délibération 80-19 du 3 juin 1980 portant avis relatif à la création d'un traitement automatisé d'informations nominatives concernant la fabrication de cartes nationales d'identité.

ANNEXE 7

RECOMMANDATIONS ET CONCLUSIONS DU RAPPORT CABAL ET DU RAPPORT DU CONSEIL DE L'EUROPE

Recommandations du rapport du député Christian Cabal de l'Office parlementaire d'évaluation des choix scientifiques et technologiques sur les méthodes scientifiques d'identification des personnes à partir des données biométriques et les techniques de mise en oeuvre , n° 938, Assemblée nationale, n° 355, Sénat, juin 2003.

Recommandation n°1 :

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

Recommandation n°2 :

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

Recommandation n°3 :

Un observatoire devra être constitué, associant les représentants des différentes administrations, des médecins, des universitaires et des chercheurs, des industriels, des associations de consommateurs ou d'usagers et la CNIL. Cet observatoire sera chargé d'assurer une veille juridique, scientifique et technologique dans le domaine de la biométrie, de suivre l'évolution des dispositifs mis en oeuvre aux plans national, européen et international ainsi qu'à l'étranger et de veiller à ce que la France soit représentée dans les différentes instances techniques d'évaluation et d'élaboration des normes. Un rapport public devra rendre compte régulièrement des évolutions constatées et des incidences financières et juridiques au plan national des mesures prises et envisagées.

Recommandation n°4 :

Devra être envisagée la mise en place d'un organisme associant des personnes publiques et privées et doté des moyens de financement nécessaires :
- pour faire réaliser par des laboratoires indépendants des travaux d'évaluation et de recherche sur les techniques biométriques d'identification des personnes ainsi que sur les procédés techniques de lutte contre la fraude documentaire,
- pour recueillir l'avis d'experts ou d'universitaires sur la fiabilité des résultats de travaux menés dans ce même domaine par d'autres organismes,
- pour diffuser les travaux conduits en son sein et gérer les ressources documentaires.

Conclusions du rapport d'étape sur l'application des principes de la convention 108 à la collecte et au traitement des données biométriques, Comité consultatif de la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (T-PD), Direction générale des affaires juridiques, Conseil de l'Europe.

1. Les données biométriques doivent être considérées comme une catégorie spécifique des données dans la mesure où elles émanent du corps humain, restent les mêmes dans différents systèmes et sont inaltérables à vie. Toutefois, elles peuvent s'altérer par exemple par le vieillissement ou une intervention chirurgicale.

2. Avant de recourir à la biométrie, le responsable de traitement devrait évaluer, d'une part les avantages et inconvénients possibles pour la vie privée de la personne concernée et d'autre part les finalités envisagées, et prendre en compte de possibles solutions alternatives, portant une atteinte moindre à la vie privée.

3. La biométrie ne devrait pas être choisie uniquement parce qu'elle est pratique à utiliser. En effet, l'utilisation de la biométrie peut porter atteinte à la dignité humaine. Il faut prendre en compte les aspects socio-culturels et les réticences possibles à l'égard de l'utilisation instrumentale du corps humain.

4. Les données biométriques et toutes données associées générées par le système doivent être utilisées à des fins déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités.

5. Les données devraient être adéquates, pertinentes et non excessives par rapport à la finalité du traitement. Un système de traitement des données devrait être configuré de façon à exclure la collecte et le traitement de plus de données biométriques ou associées que sa finalité ne l'exige. Si des gabarits sont suffisants, la collecte ou le stockage de l'image biométrique devrait être évité.

6. Dans le choix de l'architecture du système, le responsable de traitement devrait mettre en balance d'une part les avantages et les inconvénients pour la vie privée de la personne concernée et d'autre part les finalités envisagées. Un choix raisonné devrait être opéré entre le stockage uniquement sur un support de stockage individuel, dans une base de données décentralisée ou dans une base de données centralisée, tout en gardant à l'esprit les aspects de sécurité.

7. L'architecture d'un système biométrique ne devrait pas être disproportionnée par rapport à la finalité du traitement. Ainsi, si la vérification suffit, le responsable de traitement ne devrait pas développer une solution d'identification. Les données biométriques qui sont uniquement utilisées à des fins de vérification devraient être stockées de préférence sur un support individuel sécurisé de stockage, par exemple une carte à puce, que détiendrait uniquement la personne concernée.

8. La personne concernée devrait être informée de la finalité du système et de l'identité du responsable de traitement, ainsi que des données traitées et des catégories de personnes auxquelles ces données seront communiquées dans la mesure où ces informations sont nécessaires pour garantir la loyauté du traitement.

9. La personne concernée a un droit d'accès, de rectification, de blocage et d'effacement de ses données. Ces droits s'étendent aux données biométriques faisant l'objet d'un traitement automatisé et nominatif, aux possibles données associées (comme la date et localisation de l'utilisation du système), et aux personnes à qui elles ont été communiquées.

10. Le responsable de traitement doit prévoir des mesures techniques et organisationnelles appropriées afin de protéger les données biométriques et les autres données à caractère personnel qui y sont associées contre la destruction – accidentelle ou illicite – et la perte accidentelle, ainsi que contre l'accès, la modification, la communication non autorisés ou toute autre forme de traitement illicite.

11. Une procédure de certification et de contrôle devrait être développée, en particulier dans le cas des applications de masse, dans le but d'établir des normes de qualité pour les logiciels, le matériel et pour la formation du personnel responsable de l'enrôlement et de la vérification. Un audit régulier testant les performances du système est recommandé.

12. Si une personne concernée enrôlée dans un système biométrique est rejetée, le responsable de traitement devrait, à sa demande, réexaminer le cas et, si nécessaire, lui proposer des solutions de remplacement appropriées. Des procédures devraient être établies afin d'informer la personne concernée lors d'une prétendue non reconnaissance par le système.