N° 439

SÉNAT

SESSION ORDINAIRE DE 2004-2005

Annexe au procès-verbal de la séance du 29 juin 2005

RAPPORT D'INFORMATION

FAIT

au nom de la commission des Lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale (1) par la mission d'information (2) sur la **nouvelle génération** *de* **documents d'identité** *et la* **fraude documentaire**,

Par M. Jean-René LECERF,

Sénateur.

(1) Cette commission est composée de : M. Jean-Jacques Hyest, *président* ; MM. Patrice Gélard, Bernard Saugey, Jean-Claude Peyronnet, François Zocchetto, Mme Nicole Borvo Cohen-Seat, M. Georges Othily, *vice-présidents* ; MM. Christian Cointat, Pierre Jarlier, Jacques Mahéas, Simon Sutour, *secrétaires* ; M. Nicolas Alfonsi, Mme Michèle André, M. Philippe Arnaud, Mme Eliane Assassi, MM. Robert Badinter, José Balarello, Laurent Béteille, Mme Alima Boumediene-Thiery, MM. François-Noël Buffet, Christian Cambon, Marcel-Pierre Cléach, Pierre-Yves Collombat, Raymond Courrière, Jean-Patrick Courtois, Yves Détraigne, Michel Dreyfus-Schmidt, Pierre Fauchon, Gaston Flosse, Bernard Frimat, René Garrec, Jean-Claude Gaudin, Charles Gautier, Philippe Goujon, Mme Jacqueline Gourault, MM. Charles Guené, Jean-René Lecerf, Mme Josiane Mathon, MM. Hugues Portelli, Henri de Richemont, Jean-Pierre Sueur, Mme Catherine Troendle, MM. Alex Türk, Jean-Paul Virapoullé, Richard Yung.

(2) *Cette mission est composée de* : M. Charles Guené, *président ;* MM. Nicolas Alfonsi, Philippe Arnaud, Mme Eliane Assassi, MM. Alex Türk, Richard Yung, v*ice-président*s ; Mme Alima Boumediene-Thiery, M. Philippe Goujon, *secrétaire*s ; M. Jean-René Lecerf, *rapporteur*, MM. Christian Cointat, Jean-Patrick Courtois, Charles Gautier, Mme Jacqueline Gourault, MM. Jacques Mahéas, Henri de Richemont, Jean-Paul Virapoullé.

Papiers d'identité.

SOMMAIRE

Pages

LES RECOMMANDATIONS DE LA MISSION D'INFORMATION

Réunie le mardi 28 juin 2005 sous la présidence de M. Charles Guené, président, la mission d'information sur la nouvelle génération de documents d'identité et la fraude documentaire a adopté le rapport de M. Jean-René Lecerf.

Le Président a rappelé que la mission, constituée le 9 février 2005, avait procédé à de nombreuses auditions, afin de recueillir les points de vue de représentants de l'administration, de membres de la Commission nationale de l'informatique et des libertés, d'associations de défense des droits de l'homme, de chercheurs, d'industriels, d'avocats, d'universitaires, et effectué plusieurs déplacements, notamment à Washington, Bruxelles et Lyon.

Le rapporteur a indiqué que les travaux de la mission avaient essentiellement porté sur l'évaluation de la fraude à l'identité et les réponses classiques ou innovantes à y apporter. Il a souligné que le débat sur la création d'un titre d'identité électronique avec ou sans biométrie avait été envisagé sous trois aspects : la sécurisation de l'identité dans le monde réel et dans le monde virtuel de l'Internet, la modernisation de l'administration et la sauvegarde des libertés individuelles, au premier rang desquelles le respect de la vie privée.

La mission n'a pas souhaité proposer de solutions définitives. Au contraire, elle s'est efforcée d'envisager l'ensemble des scénarii possibles, sans a priori. Espérant alimenter les réflexions, elle a toutefois fait de nombreuses observations et recommandations.

I. Un constat : une fraude significative avérée en dépit de l'absence d'une évaluation globale

- aucun organisme ou ministère n'a réalisé une évaluation globale de la fraude à l'identité en France ;

- des données dispersées révèlent une fraude significative qui est le fait, pour une part importante, d'organisations criminelles ;

- la fraude concerne l'ensemble des documents mais plus particulièrement le passeport et le permis de conduire ;

- l'ensemble des pays développés est touché par ce phénomène ;

- les principaux points faibles de la chaîne de l'identité se situent au niveau de l'état civil et du vol de documents vierges.

II. Des solutions simples pour réduire la fraude

- il serait utile de confier à l'Observatoire national de la délinquance la mission d'élaborer un outil performant d'évaluation de la fraude à l'identité ;

- il convient de renforcer la formation et l'équipement des agents chargés du contrôle de premier degré ;

- la coopération internationale doit être intensifiée, en particulier avec Interpol ;

- le répertoire national d'identification des personnes physiques tenu par l'INSEE pourrait être utilisé pour vérifier l'exactitude des informations relatives à l'état civil fournies par les demandeurs de titre et pour éviter ainsi la délivrance indue de copies intégrales et extraits d'actes de l'état civil ;

- la délivrance de la carte nationale d'identité devrait être assujettie au paiement d'une somme même modeste, dont seraient toutefois exonérées les personnes défavorisées, et des pénalités devraient être instituées en cas de vols ou de pertes répétés d'un titre d'identité ;

- il convient de créer un fichier centralisé des titres d'identité délivrés précisant leur statut (valide, perdu ou volé) ;

- la production des passeports doit être centralisée sur un site unique ;

- la carte d'identité et le passeport devraient être retenus comme les seuls documents valant justificatif d'identité pour l'ensemble des démarches administratives tant que d'autres documents, notamment le permis de conduire, n'offrent pas un niveau de sécurité équivalent ;

- il ne faut pas renoncer sans examen approfondi à la possibilité de fusionner à terme la carte nationale d'identité et le passeport au bénéfice de ce dernier.

III. La biométrie : un surcroît de sécurité à plusieurs conditions

- la France n'a plus la liberté de refuser toute utilisation de la biométrie, ses engagements européens l'y obligeant d'ores et déjà pour les passeports ;

- la question du passeport biométrique ne se confond pas avec celle de la carte nationale d'identité électronique, le calendrier de mise en place du passeport étant prioritaire ;

- la biométrie est la seule technologie permettant l'identification de millions de personnes de façon sûre et pourrait constituer une réponse efficace aux usurpations d'identité, dès lors que serait constituée une base centrale des données biométriques ;

- la technologie permet de constituer un fichier central des données biométriques garantissant l'unicité de l'identité lors de la délivrance d'un titre sans rendre possible l'utilisation de ce fichier à d'autres fins telles que l'identification ;

- la biométrie ne doit pas être perçue comme une solution miraculeuse et le succès de sa mise en oeuvre requiert plusieurs précautions, notamment la réduction de la durée de validité des titres à cinq ans et le maintien d'une présence humaine lors des contrôles ;

- si un fichier central était utilisé à des fins d'identification, le passage à la biométrie plaiderait en faveur du caractère obligatoire des titres d'identité pour des raisons d'efficacité et de cohérence ;

- si un système biométrique était déployé, il devrait faire l'objet d'une introduction progressive ou être précédé d'une phase d'expérimentation.

IV. Développer les fonctions d'authentification à distance et de signature électronique grâce aux titres d'identité électronique

- un titre d'identité électronique pourrait permettre de sécuriser les échanges électroniques et de faciliter la vie quotidienne des citoyens ;

- ces nouvelles fonctions devraient être limitées dans un premier temps à la sphère publique et ne devraient servir de prétexte ni à des vérifications abusives de l'identité des personnes ni à une remise en cause de la possibilité d'échanges électroniques anonymes ;

- l'utilisation de ces fonctions devrait être ouverte à tous sur l'ensemble du territoire ;

- l'utilisation d'un titre électronique pour des transactions privées requiert à ce stade une grande prudence en raison du respect de la concurrence, de la protection de la vie privée et des risques de mise en jeu de la responsabilité de l'Etat au regard de la prestation de services de certification.

V. Protéger les libertés individuelles et le respect de la vie privée

- un système de titre d'identité électronique avec ou sans biométrie doit respecter le principe constitutionnel et conventionnel de proportionnalité entre les moyens déployés et les finalités assignées au système ;

- le débat devrait moins porter sur la création d'un fichier des Français que sur les conditions d'utilisation d'un tel fichier ;

- si l'utilisation d'une base centrale biométrique à des fins d'identification était retenue, elle ne devrait se faire que sous le contrôle d'un magistrat ou de la CNIL sans souffrir aucune exception ;

- grâce à l'authentification à distance, chaque personne devrait pouvoir accéder en permanence et immédiatement à l'ensemble de ses données personnelles ainsi qu'à l'historique des consultations de ces données ;

- les moyens de la CNIL doivent être renforcés dans des proportions importantes ;

- la technologie du « sans contact » ne présente pas à ce jour de garanties suffisantes au regard du respect des libertés individuelles et de la vie privée.

Mesdames, Messieurs,

Le 1er février dernier, le Bureau du Sénat autorisait votre commission des Lois à créer en son sein une mission d'information sur la nouvelle génération de documents d'identité et la fraude documentaire, c'est-à-dire la fraude aux documents valant pièce justificative d'identité.

A la suite des attentats du 11 septembre 2001, l'Organisation de l'aviation civile internationale, l'Union européenne et de nombreux Etats, au premier rang desquels les Etats Unis, ont en effet décidé d'insérer dans les passeports des puces électroniques sécurisées comportant des données biométriques numérisées, notamment la photographie, pour identifier avec certitude leurs détenteurs et lutter ainsi contre une fraude documentaire qui favorise l'immigration irrégulière, la criminalité organisée et les activités terroristes.

Dans le cadre du projet d'identité nationale électronique sécurisée, appelé « projet INES », le Gouvernement français envisage d'équiper également les cartes nationales d'identité de puces électroniques sécurisées qui, non seulement contiendraient des données biométriques numérisées -la photographie et les empreintes digitales- afin de réduire les risques de fraude, mais offriraient en outre à leurs titulaires de nouveaux services tels que l'authentification à distance, la signature électronique et la possibilité d'inscrire sur la puce des données personnelles communicables. Un fichier informatique national des empreintes digitales serait constitué. La carte nationale d'identité pourrait être rendue obligatoire et payante, alors qu'elle est facultative depuis sa création en 1955 et gratuite depuis 1998. A la suite d'un comité interministériel réuni le 11 avril 2005, M. Dominique de Villepin, alors ministre de l'intérieur, de la sécurité intérieure et des libertés locales, a annoncé que le Parlement serait prochainement saisi d'un projet de loi à cet effet.

Ce projet ambitieux n'est ni nouveau ni isolé. En 2001, le Gouvernement de M. Lionel Jospin envisageait déjà la création d'un « titre fondateur », c'est-à-dire une refonte du dispositif de délivrance des cartes nationales d'identité et des passeports permettant aux administrés d'obtenir, selon une procédure unique et simplifiée, des documents d'identité et de voyage sécurisés et d'effectuer des téléprocédures administratives. De nombreux Etats européens ont d'ores et déjà décidé ou envisagent eux aussi de mettre en place des cartes nationales d'identité électroniques remplissant cette double fonction.

La réforme projetée suscite tout à la fois l'intérêt et l'inquiétude. Ces sentiments mêlés se sont notamment exprimés, au cours des six premiers mois de l'année 2005, dans le cadre de plusieurs débats publics et d'un sondage organisés par le Forum des droits sur l'Internet à la demande du ministère de l'intérieur.

Le sondage réalisé par la société IPSOS au mois de mai 2005, montre que la lutte contre la fraude à l'identité semble constituer une préoccupation majeure des Français : 74 % des sondés se sont déclarés favorables à la création d'une carte nationale d'identité électronique comportant des données personnelles numérisées telles que les empreintes digitales, la photographie, ou l'iris de l'œil ; 75 % se sont déclarés favorables à la constitution d'un fichier informatique national des empreintes digitales ; 69 % ont estimé que la future carte d'identité électronique devrait être obligatoire pour garantir une réelle diminution des fraudes.

Les débats publics organisés par le Forum qui, de l'aveu même de sa présidente Mme Isabelle Falque-Pierrotin, ont réuni un public à la fois plus averti et plus critique, ont quant à eux mis en exergue les craintes d'atteintes à la vie privée suscitées par le programme INES.

Sans attendre le dépôt éventuel d'un projet de loi, votre commission des Lois a souhaité créer une mission d'information afin, d'une part, d'appréhender l'ampleur de la fraude documentaire, d'évaluer la sécurité des procédures de délivrance des titres d'identité et d'examiner les mesures susceptibles d'être prises pour l'améliorer, d'autre part, d'étudier les perspectives offertes par la biométrie, d'envisager les possibilités d'extension des usages de la carte nationale d'identité et de déterminer les garanties nécessaires pour protéger les libertés individuelles, au premier rang desquelles le respect de la vie privée.

La mission d'information a ainsi procédé à de nombreuses auditions[1] qui lui ont permis de recueillir les points de vue de représentants de l'administration, de membres de la Commission nationale de l'informatique et des libertés, d'associations de défense des droits de l'homme, de chercheurs, d'industriels, d'avocats, d'universitaires…

---

[1] *La liste des auditions et des déplacements de la mission figure en annexe du rapport.*

Elle a en outre effectué plusieurs déplacements. A Eragny, plusieurs de ses membres ont découvert le centre de recherche de la SAGEM, société spécialisée dans les technologies de reconnaissance biométrique. A Lyon, ils ont rencontré les responsables d'Interpol ainsi que le président et le procureur de la République du tribunal de grande instance. A Val Maubuée, ils se sont rendus dans l'une des deux unités de production des cartes nationales d'identité et des titres de séjour du Centre national de production des titres.

A Washington, ils ont visité l'aéroport international de Baltimore-Washington, rencontré M. James Sensenbrenner, président de la commission judiciaire de la Chambre des représentants, et Mme Maura Harty, « US assistant secretary » pour les affaires consulaires au département d'Etat. A Bruxelles, ils ont étudié la nouvelle carte d'identité électronique belge.

Enfin, après avoir suivi avec attention les débats organisés par le Forum des droits sur l'Internet, la mission a pris connaissance avec intérêt des recommandations qu'il a formulées le 16 juin dernier.

Ces travaux lui ont permis de proposer, d'une part, les mesures qu'elle juge nécessaires pour lutter contre une fraude aux titres d'identité difficile à quantifier mais réelle, d'autre part, les garanties devant entourer le développement d'une nouvelle génération de titres d'identité électroniques.

I. LES MESURES NÉCESSAIRES POUR LUTTER CONTRE UNE FRAUDE AUX TITRES D'IDENTITÉ DIFFICILE À QUANTIFIER MAIS RÉELLE

La fraude aux titres d'identité est difficile à évaluer en France. Elle n'en constitue pas moins une réalité préoccupante dont le développement est favorisé par les défaillances de la « *chaîne de l'identité* ». Plusieurs mesures ne nécessitant pas la mise en place de titres d'identité électroniques permettraient de l'enrayer.

A. DES CHIFFRES SIGNIFICATIFS MAIS PAS D'ÉVALUATION GLOBALE

Au cours de ses travaux, la mission d'information a pu recueillir des chiffres significatifs qui attestent de la réalité de la fraude documentaire et de sa progression sans toutefois pouvoir la quantifier précisément.

1. La fraude aux titres d'identité, support du crime et du terrorisme

a) Différents documents pour justifier de son identité

Il n'existe aucun texte législatif ou réglementaire énumérant les documents valant pièce justificative d'identité. En conséquence, chaque autorité administrative est libre de fixer les pièces d'identité qu'elle admet dans le cadre de l'accomplissement des procédures relevant de sa compétence. De même, les acteurs privés apprécient librement les titres qu'ils acceptent pour vérifier l'identité d'une personne. Les documents susceptibles d'être produits ne revêtent toutefois pas tous la même valeur probante.

- *La carte nationale d'identité*

La carte nationale d'identité, créée par un décret n° 55-1397 du 22 octobre 1955, est le **seul document officiel ayant pour objet exclusif de certifier son identité**.

En application d'un décret n° 2000-1277 du 26 décembre 2000 portant simplification de formalités administratives et suppression de la fiche d'état civil, elle vaut extrait d'acte de naissance et certificat de nationalité française pour l'accomplissement de démarches courantes. Elle est également reconnue comme document de voyage dans certains Etats, pour des séjours égaux ou inférieurs à trois mois.

Facultative et gratuite, la carte nationale d'identité peut être demandée par tout Français, quel que soit son âge.

Elle comprend un numéro à 12 chiffres[1], le nom patronymique, les prénoms dans l'ordre de l'état civil, le sexe, la date et le lieu de naissance, la taille, l'adresse, la signature et la photographie du titulaire, la durée de validité et la date de délivrance du document ainsi que la qualité et la signature de l'autorité qui s'en est chargée. **5,15 millions de titres ont été délivrés l'an passé.**

La durée de validité de la carte nationale d'identité est de **dix ans**. Toutefois, même périmée, elle continue à certifier de l'identité de son titulaire s'il est reconnaissable sur la photographie qui y figure.

---

[1] *Les quatre premiers correspondent à l'année et au mois de la délivrance, les trois suivants représentent le code géographique du lieu de délivrance (numéro INSEE) et les cinq derniers sont relatifs au numéro d'ordre.*

Histoire de la carte nationale d'identité

• 1921 : Emission des premières cartes, avec photographie et empreintes digitales, par la préfecture de police de Paris pour le département de la Seine

• Loi du 27 octobre 1940 : Obligation de détenir une carte d'identité à partir de 16 ans, comportant les empreintes digitales et la photographie, et de déclarer tout changement d'adresse. Institution d'un fichier central de la population et d'un numéro d'identification individuel, qui seront détruits à la Libération

• Décret du 22 octobre 1955 : Création d'une nouvelle carte nationale d'identité, facultative, sans numéro d'identification ni de déclaration de changement d'adresse. Apposition d'une empreinte digitale (supprimée en 1974)

• 1968-1969 : Projet de titre polyvalent, facultatif et gratuit

• 1975-1981 : Projet d'informatisation de la carte nationale d'identité (centralisation de la production, constitution d'une base de données centrale)

• 1986-1995 : Diffusion d'une carte sécurisée (production centralisée ; zone de lecture optique…), dite « carte Pasqua ». Relevé d'une empreinte digitale

• 1998 : Gratuité de la carte

- *Le passeport*

Le passeport, dont les conditions de délivrance et de renouvellement sont fixées par un décret n° 2001-185 du 26 février 2001, constitue un **document international de voyage**, obligatoire pour certains séjours. Il permet également, sauf règle particulière, de faire la preuve de son identité et de la nationalité française.

Il est délivré sans condition d'âge à tout Français qui en fait la demande, moyennant un **droit de timbre** d'un montant de 60 euros dont sont dispensées les personnes reconnues « indigentes ». Outre les mentions figurant sur la carte nationale d'identité, le passeport comporte un numéro et la couleur des yeux de son titulaire. Depuis le 1er mars 2001, sa durée de validité est passée de cinq à **dix ans**. Si la carte nationale d'identité est strictement personnelle, des mineurs de moins de 15 ans peuvent être inscrits sur le passeport d'une personne majeure ayant des liens avec eux. Le document a alors une durée de validité de cinq ans tout comme les passeports détenus en propre par des mineurs[1]. **2,7 millions de titres** ont été délivrés l'an passé.

Les passeports et les cartes nationales d'identité demeurent la propriété de l'Etat qui peut les retirer à leur titulaire.

[1] *Article 953 du code général des impôts.*

- *Les autres pièces administratives utilisées pour prouver son identité*

D'autres pièces administratives peuvent servir de mode de preuve de l'identité de leur titulaire.

L'article 78-2 du code de procédure pénale autorise ainsi, en cas de contrôle de police, à justifier de son identité par tout moyen c'est-à-dire, selon une circulaire d'application du 11 décembre 1995, par un document officiel comportant une photographie, toutes autres pièces probantes ou le témoignage de tiers.

Aux termes de l'article L. 131-15 du code monétaire et financier, toute personne « *doit justifier de son identité au moyen d'un document officiel portant sa photographie* » lors de la remise d'un chèque.

Le plus utilisé est le permis de conduire, obligatoire pour la conduite d'un véhicule[1] et **dont la durée de validité n'est pas limitée**. **2,3 millions de titres** ont été délivrés l'an passé. Toutefois, **bien d'autres documents** tels que le permis de chasser, les cartes d'identité professionnelles ou encore la carte du combattant peuvent être utilisés pour prouver son identité.

Le code électoral dispose ainsi que, pour exercer leur droit de vote dans les communes de plus de 5.000 habitants[2], les électeurs français peuvent produire au choix une des pièces suivantes : une carte nationale d'identité ou un passeport, même périmés (si la preuve de nationalité a été apportée par un certificat de nationalité), une carte du combattant, une carte d'invalidité civile ou militaire avec photographie, une carte d'identité de fonctionnaire avec photographie, une carte d'identité ou de circulation avec photographie délivrée par les autorités militaires, un permis de conduire, un permis de chasser avec photographie ou un titre de réduction de la SNCF avec photographie[3].

Cette diversité de pièces permet aux individus de justifier de leur identité avec **souplesse**, facilite leurs démarches quotidiennes et témoigne d'un principe de **confiance** entre administrations et citoyens. Toutefois, les pièces précitées ont été créées pour d'autres fonctions que la justification de l'identité de leur titulaire, fonction qu'elles remplissent à titre accessoire.

La grande hétérogénéité des niveaux de protection des pièces valant justificatif d'identité s'avère, selon le ministère de l'intérieur, « *particulièrement néfaste* » à une politique efficace de lutte contre la fraude documentaire à l'identité.

---

[1] *Articles L. 221-1 et suivants du code de la route.*

[2] *Dans les communes de 5.000 habitants ou moins, la production de la carte électorale par l'électeur est suffisante.*

[3] *Article R. 60 du code électoral et arrêté du 24 septembre 1998 fixant la liste des pièces d'identité exigées des électeurs au moment du vote dans les communes de plus de 5.000 habitants.*

b) Les techniques de fraude documentaire à l'identité

La fraude à l'identité est aussi ancienne que le besoin d'identification des hommes en société. En 1921, c'est le constat d'utilisations frauduleuses des multiples documents délivrés par les autorités locales ou certaines associations, facilement falsifiables, qui a conduit la préfecture de police à émettre les premières cartes d'identité pour les habitants du département de la Seine.

Cette fraude peut prendre **diverses formes** :

- l'identité fictive ;

- l'usurpation d'identité ;

- l'échange d'identité ;

- l'utilisation de l'identité d'une personne décédée.

Plusieurs techniques de fraude aux titres d'identité français ont été détectées ces dernières années :

- le vol de titres vierges ultérieurement falsifiés ;

- la falsification, qui consiste à modifier les données d'identité d'un titre délivré ou à personnaliser un titre vierge volé[1] ;

- la contrefaçon, c'est-à-dire une imitation d'un titre officiel ;

- l'obtention frauduleuse d'un titre authentique, c'est-à-dire d'un « vrai faux » document, par l'utilisation d'une identité créée ou usurpée au moyen d'une fraude à l'état civil ;

- l'usage frauduleux d'un titre authentique, emprunté ou dérobé à un tiers.

c) La fraude aux titres d'identité, une nécessité pour la criminalité

La fraude aux titres d'identité est généralement utilisée pour commettre d'autres infractions : ouvrir un compte bancaire, souscrire un emprunt, bénéficier de prestations sociales, quitter le territoire national, échapper aux recherches de la police…

---

[1] *Substitution de la photographie, découpe du film protecteur et modification des mentions, apposition d'une fausse vignette sur le passeport, démontage du document et remplacement de pages…*

Après son évasion de la prison de Fresnes en mars 2003, M. Antonio Ferrara, braqueur multirécidiviste finalement arrêté le 11 juillet de la même année à Paris, avait ainsi modifié son apparence à l'aide de la chirurgie esthétique et utilisé de faux papiers d'identité d'excellente qualité pour se déplacer librement.

Les liens entre la fraude documentaire et le crime organisé ou le terrorisme sont particulièrement étroits.

Selon le ministère de l'intérieur, une part importante des escroqueries ou des abus de confiance constatée dans l'état 4001 (145.174 infractions constatées en 2003), tableau statistique de la criminalité, donne lieu à l'utilisation de fausses identités.

Selon MM. Pierre de Bousquet de Florian, directeur de la surveillance du territoire (DST) au ministère de l'intérieur, et Philippe Lagauche, directeur adjoint des affaires criminelles et des grâces au ministère de la justice, **les réseaux terroristes utilisent systématiquement de faux documents d'identité, délivrés par des faussaires** qui fournissent également les criminels de droit commun.

A titre d'exemple, il est possible d'évoquer la condamnation par le tribunal correctionnel de Paris, le 9 juillet 2004, de MM. D….D.. et R… M…, respectivement à 5 ans et 8 ans d'emprisonnement, reconnus coupables des chefs d'association de malfaiteurs en relation avec une entreprise terroriste en récidive légale, recel de documents administratifs, détention de faux documents administratifs et recel de contrefaçon de timbres. Ils avaient été arrêtés le 30 octobre 2002 en provenance de Rotterdam, en possession de 30 passeports français, 60 timbres fiscaux et 60 films plastifiés portant la mention « RF » destinés aux passeports. L'enquête les concernant a établi que leur activité logistique était liée à la mouvance islamiste radicale et que les faux titres étaient destinés à des groupes ayant suivi une formation militaire dans la zone afghano-pakistanaise.

Selon le ministère de la justice, la falsification de documents administratifs, la détention de documents contrefaits, la contrefaçon, le transport et le recel de contrefaçon de timbres ou de passeports vierges ou volés en relation avec une entreprise terroriste sont parmi les infractions terroristes les plus fréquemment retenues dans les enquêtes judiciaires françaises.

Un marché des faux titres d'identité s'est développé. En France, le prix d'achat au marché noir d'un faux permis de conduire est de 500 euros, celui d'un faux passeport de 2.000 euros. Il existerait environ une dizaine d'officines assez actives, installées en région parisienne et à Marseille, les terroristes basques disposant quant à eux de leurs propres ateliers clandestins.

M. Marcel Faure, commissaire divisionnaire, chef de la division nationale de répression des atteintes aux personnes et aux biens à la direction centrale de la police judiciaire, a souligné que la production de faux titres d'identité était devenue une **activité criminelle lucrative** favorisant le développement d'une véritable industrie de production de faux papiers nécessitant de lourds investissements et bénéficiant d'outils de reproduction de haute qualité.

Polymorphe, la fraude aux titres d'identité est mal évaluée. Toutefois, la réalité du phénomène ne peut être contestée.

2. La quantification difficile d'un phénomène préoccupant

L'évaluation de l'importance de la fraude documentaire à l'identité en France est rendue difficile par l'absence de centralisation des informations et d'harmonisation des statistiques. Néanmoins, mêmes partielles, les données recueillies par votre mission d'information attestent son importance.

a) L'absence d'évaluation globale de la fraude aux titres d'identité en France

L'importance de la fraude documentaire à l'identité est mal connue pour plusieurs raisons. Par nature, cette fraude est difficile à déceler car son but est bien d'empêcher l'identification de celui qui y recourt. De plus, elle n'est pas toujours dénoncée par ceux qui en sont victimes.

Le nombre de documents volés, les saisies de titres contrefaits ou la détection de fausses pièces par les personnels compétents permettent de constater la réalité de ce phénomène mais les modalités de sa mesure en France sont peu satisfaisantes.

En effet, les sources d'information sont dispersées et incertaines.

Selon le ministère de l'intérieur, la véritable ampleur du phénomène est « *partiellement ignorée des chiffres officiels de la délinquance* », aucun organisme n'ayant en France la mission spécifique de l'évaluer.

M. Alain Bauer, président du conseil d'orientation de l'Observatoire national de la délinquance, dont le rôle est de développer une mesure statistique plus fine de la délinquance, a reconnu que la fraude documentaire n'était pas spécifiquement prise en considération par ce dernier.

M. Pierre Piazza, chargé de recherche à l'Institut national des hautes études de sécurité, a déploré le fait qu'aucune étude officielle ne semblait avoir été menée sur ce sujet.

Par ailleurs, les difficultés de collecte des informations relatives à la fraude aux titres d'identité résultent de **l'absence de centralisation de ces données par un organisme unique**.

Pas moins de trente directions ou sous-directions relevant de huit ministères paraissent pourtant concernées par la fraude documentaire à l'identité (ministères des affaires étrangères ; de la défense ; de l'économie, des finances et de l'industrie, de l'emploi, de la cohésion sociale et du logement ; des transports, de l'équipement ; du tourisme et de la mer ; de l'intérieur et de l'aménagement du territoire ; de la justice ; de la santé et des solidarités) mais elles conservent par devers elles les renseignements qu'elles ont recueillis sur cette délinquance.

En effet, leurs bases de données ne sont pas toujours accessibles aux autres autorités concernées par la fraude, ce qui fragilise leur actualisation régulière ainsi que les échanges d'informations. A titre d'exemple, certaines données détenues par la direction des libertés publiques et des affaires juridiques du ministère de l'intérieur ne sont pas prises en compte dans les bases de données opérationnelles du ministère.

Parfois, les autorités n'ont même pas développé d'outils de mesure : ainsi, le ministère des affaires étrangères a indiqué qu'il ne disposait pas de statistiques sur les passeports déclarés perdus ou volés et retrouvés pour les années antérieures à 2005.

Administrations sociales, entreprises (SNCF, la Poste, Air France…) et banques ne souhaitent pas nécessairement **communiquer sur l'ampleur et les modalités du phénomène constaté**, pour ne pas entraver des stratégies commerciales ou fragiliser la confiance de leurs clients ou actionnaires.

De plus, chaque acteur concerné développe ses propres instruments et définitions pour évaluer la fraude en fonction de ses priorités.

Ainsi, l'état 4001 n'en offre qu'une « *vision tronquée* » selon le ministère de l'intérieur. De plus, les données rassemblées ne font l'objet d'aucune analyse précise rendue publique par les services compétents.

S'il existe bien une rubrique relative aux faux documents d'identité et autres documents administratifs, elle ne reflète pas l'intégralité de la fraude puisque **cette dernière n'est pas systématiquement recensée** lorsqu'elle est connexe à une infraction principale (exemple d'une escroquerie avec usurpation d'identité).

Or, de nombreuses infractions peuvent être commises à l'aide de faux papiers d'identité, ce qui empêche une **appréhension exhaustive de la fraude**.

Malgré les faiblesses de ces outils d'évaluation, les informations collectées par votre mission soulignent le caractère préoccupant de la fraude aux titres d'identité.

b) Néanmoins, une fraude avérée

La fraude documentaire à l'identité en France peut être mesurée à travers les statistiques des divers ministères qui y sont confrontés et de l'état 4001 en particulier, qui demeure un outil précieux malgré ses faiblesses.

Pour M. Daniel Canepa, Secrétaire général du ministère de l'intérieur, comme pour M. François Barry-Delongchamps, directeur des Français à l'étranger et des étrangers en France au ministère des affaires étrangères, **la fraude aux titres d'identité est en pleine croissance**.

Toutes pièces confondues, le ministère de l'intérieur a relevé **le vol de 84.464 titres vierges** (passeports, permis de conduire, cartes grises, visas...) dans les préfectures et lors de leur transport entre 1999 et 2004. Le nombre de faux documents saisis par l'administration des douanes est passé de 675 en 2001 à 3.157 en 2003 (+ 67,7 %).

Quant aux porteurs de faux documents, 11.603 ont été interpellés en 2003 par les personnels de la direction centrale de la police aux frontières (DCPAF).

Concernant la carte nationale d'identité, alors que le volume des cartes délivrées chaque année a baissé de 11 % entre 2000 et 2003 (de 5.937.921 à 5.236.066), **le nombre d'inscriptions pour fraude au fichier des personnes recherchées**[1] **a augmenté de 476 % sur la même période** (de 138 à 816). **L'usurpation d'identité est à l'origine de 70 % des affaires ayant donné lieu à inscription.**

Par ailleurs, 2.835 fausses cartes nationales d'identité ont été interceptées par les agents de la police aux frontières en 2002.

Ces données traduisent certains comportements négligents mais également l'action de délinquants à la recherche de titres authentiques.

Les passeports semblent aussi touchés par la fraude. Ainsi, selon le ministère de l'intérieur, **plus de 90.000 documents ont été déclarés perdus ou volés par leur titulaire entre 1999 et 2004.** Les postes consulaires en recensaient déjà 1.000 au cours des cinq premiers mois de l'année 2005.

---

[1] *Recensant toutes les personnes faisant l'objet d'une mesure de recherche ou de vérification de leur situation juridique (450.000 au 1er janvier 2005), ce fichier est tenu conjointement par les ministères de l'intérieur et de la défense. Il peut être consulté par les autorités judiciaires, les services de police et de gendarmerie, les autorités administratives pour des recherches relevant de leurs attributions et les services de police d'Etats liés à la France par accord international.*

Par ailleurs, 14.700 passeports vierges ont été volés sur le territoire national entre 2003 et 2004. Certains d'entre eux ont été détectés par des postes consulaires à l'étranger (Maroc, Qatar, Comores, Royaume-Uni…).

9.000 permis de conduire ont été volés depuis 2001. Il s'agit d'un **document à la fois peu sécurisé** (livret cartonné avec une photographie) et **très intéressant pour diverses catégories de fraudeurs** : personnes souhaitant bénéficier des droits liés à la nationalité française, non titulaires du permis ou conducteurs à qui il a été retiré…

M. Xavier Richaud, procureur de la République près du tribunal de grande instance de Lyon, a constaté que les permis de conduire faisaient l'objet d'une fraude massive dans le ressort du tribunal, en particulier à cause du développement des demandes d'échange de permis étrangers frauduleux contre des permis français.

Selon les assureurs, environ 3 % des conducteurs, soit environ 1,2 million de personnes, conduiraient sans permis ou avec une fausse pièce. Le nombre des conducteurs verbalisés avec un faux permis de conduire a augmenté de 60 % entre 2002 et 2003.

Ces chiffres pourraient être sous-évalués. M. Christophe Naudin, chargé de recherche au département Menaces criminelles contemporaines de l'Institut de criminologie de l'Université de Paris-Panthéon-Assas, estime qu'il existe actuellement environ 3 millions de faux permis de conduire.

L'examen des infractions constatées par les policiers et les gendarmes souligne l'importance de l'utilisation de faux documents d'identité (+7,71 % entre 2001 et 2003).

Ces statistiques sont « *faussées* » à la baisse selon le ministère de l'intérieur car, lors du démantèlement d'une affaire, l'infraction est imputée aux faussaires, mais n'est pas retenue à l'encontre des centaines de clients apparaissant sur les documents contrefaits.

Faits constatés (et variation) – France métropolitaine – tous services (extrait de l'état 4001)

	2001	2002	Variation	2003	Variation	Variation 2001-2003
Index 81 Faux documents d'identité	9.275	10.712	+15,49 %	9.990	*-6,74 %*	**+ 7,71 %**
Index 82 Faux documents concernant la circulation des véhicules	1.959	2.342	+ 19,55 %	2.311	*-1,32 %*	**+ 17,97 %**
Index 83 Autres documents administratifs	2.476	3.083	+ 24,52 %	3.2258	**+ 5,68 %**	**+ 31,58 %**
Index 91 Escroquerie et abus de confiance	154.107	140.593	- 8,77 %	145.174	**+ 3,26 %**	*- 5.80 %*
Total des index	167.817	156.730	- 6,61 %	160.733	**+ 2,55 %**	*- 4,22 %*
Total des index dans le total des crimes et délits	4,13 %	3,81 %		4,04 %		

Source : ministère de l'intérieur

M. Philippe Lagauche, directeur adjoint des affaires criminelles et des grâces au ministère de la justice, a indiqué que **le casier judiciaire national ne recensait qu'une partie de la fraude tout en soulignant la fiabilité de ses chiffres, qui correspondent aux délits et crimes jugés**.

Ces chiffres révèlent **une relative stabilité de la fraude à un niveau élevé depuis 1994**. **Selon M. Philippe Lagauche, , entre 5.700 et 6.500 condamnations ont été prononcées chaque année en moyenne sur la période** (dix à quinze fois moins lorsque la fraude est la seule infraction). La détention frauduleuse de faux documents administratifs constatant une identité a sensiblement augmenté (+ 69% en neuf ans).

Infractions sanctionnées	Année	Condamnations prononcées comportant cette infraction	Condamnations principales	Condamnations infraction unique
Détention frauduleuse de faux documents administratifs constatant un droit, une identité ou une qualité	1994	108	38	6
	2002	1.213	526	126
	2003	1.155	460	114
Faux dans un document administratif constatant un droit, une identité ou une qualité	1994	2.550	885	185
	2002	1.456	589	64
	2003	1.467	586	57
Fourniture d'identité imaginaire pouvant provoquer des mentions erronées au casier judiciaire	1994	161	33	6
	2002	350	63	15
	2003	421	97	24
Usage de faux dans un document administratif constatant un droit, une identité ou une qualité	1994	3.521	690	220
	2002	2.848	550	191
	2003	2.691	547	180
Condamnations prononcées pour des délits relatifs à la fausse identité	1994	6.340	1.646	417
	2002	5.867	1.728	396
	2003	5.734	1.690	375

Source : ministère de la justice (DACG)

En résumé, la fraude documentaire concerne l'ensemble des titres d'identité, favorisant un développement des usages criminels des fausses identités constaté par l'ensemble des services compétents.

c) Un coût ignoré

En raison de la faiblesse des outils de mesure de la fraude aux titres d'identité et de la discrétion des organismes qui en sont victimes, **l'évaluation de son coût demeure elle aussi difficile** et vraisemblablement sous-estimée. **Votre mission dispose ainsi de peu de chiffres pertinents. Ils se révèlent cependant significatifs.**

La Régie autonome des transports parisiens (**RATP**) a indiqué que les **pertes dues aux infractions non recouvrées en raison d'une fausse adresse ou d'une usurpation d'identité s'élevaient en 2003 à 15 millions d'euros, pour un coût global de la fraude de 70 millions d'euros**.

Selon les informations transmises par le ministère de l'intérieur, le coût de la fraude à l'identité pour le versement des allocations et des prestations sociales représenterait 0,02 % des dépenses de santé en France, c'est-à-dire environ 30 millions d'euros par an.

Comme l'a rappelé M. Christian Noyer, gouverneur de la Banque de France, président de l'Observatoire de la sécurité des cartes de paiement, en **soulignant le nombre croissant d'ouvertures de comptes en banques sous de fausses identités, les entreprises et les banques subissent surtout des préjudices d'ordre financier en raison de la fraude**. Il en va **de même pour les organismes sociaux et les administrations** (fiscale notamment) qui peuvent délivrer des pièces ou ouvrir des droits à des personnes qui ne devraient pas en bénéficier.

Comme l'illustre l'exemple de Mme X, communiqué par le ministère des affaires étrangères, **l'usurpation d'identité est traumatisante pour ses victimes**. Leur vie quotidienne est bouleversée : elles doivent soudain justifier de leur identité et de leurs droits alors que les apparences sont contre elles et rétablir la vérité au prix de démarches longues et coûteuses.

Un exemple d'usurpation d'identité

Mme X, âgée de 34 ans, domiciliée en France, a saisi le ministère des affaires étrangères (bureau des élections) en mai 2005, d'une usurpation d'identité dont elle était victime. Elle venait ainsi de recevoir de la mairie de son lieu de résidence une lettre l'informant qu'elle ne pourrait pas participer au référendum du 29 mai 2005 car elle était inscrite sur une liste de centre de vote à l'étranger.

Son identité a été usurpée et sa bonne foi ne peut être mise en cause puisqu'elle vit avec sa mère, qui peut attester de l'identité de sa fille. L'usurpation d'identité a pu être détectée grâce au contrôle des listes électorales effectué par l'INSEE, l'usurpatrice ayant demandé son inscription sur la liste de centre de vote d'un poste consulaire. Mme X a été invitée à déposer plainte auprès du tribunal de grande instance de son lieu de résidence. La victime pense que son identité a été usurpée à la suite de la perte de son passeport au Royaume-Uni, en 1990.

La personne qui a usurpé son identité est inscrite au registre des Français établis hors de France d'un poste consulaire aux Etats-Unis depuis la fin de l'année 2004. Au moment de son inscription, elle a fourni un acte de naissance d'une commune en France, une carte nationale d'identité délivrée en 1993 par une préfecture et un passeport délivré par le poste consulaire en 1999 après consultation de l'autorité qui avait délivré le précédent passeport.

L'usurpatrice s'est mariée aux Etats-Unis sans demander la transcription à l'état civil français de son acte de mariage. La mention de ce mariage n'a donc pas été portée en marge de l'acte de naissance de la vraie titulaire de cette identité. Dans ces conditions, si la véritable Mme X avait demandé une copie de son acte de naissance, elle n'aurait pas su que son identité avait été « *empruntée* ».

3. Un problème mondial

La fraude aux titres d'identité fragilise l'ensemble des sociétés « ouvertes » aux échanges et aux communications.

a) Une fraude constatée dans tous les Etats

La France n'est pas le seul Etat où sont constatées des fraudes aux titres d'identité. En fait, **l'ensemble des pays développés semble touché par le phénomène**. Si les données étrangères doivent être évaluées avec prudence au regard de la situation française, elles constituent néanmoins un bon indice du caractère mondial de la fraude.

On dénombre ainsi chaque année environ 70.000 délits de falsifications de documents (faux en écriture...) **en Allemagne**[1], cette fraude concernant peu le passeport allemand (30 à 50 cas par an), qui serait l'un des plus sûrs du monde si l'on en croit la direction centrale de la police aux frontières.

En **Espagne**[2], selon le ministère de l'intérieur, « *les chiffres fournis sont comparables à ceux de la France* » : 8.614 documents (carte nationale d'identité ; passeport) saisis pour falsification en contrefaçon ; 1.954 documents vierges volés en 2003. Le nombre de documents perdus ou volés est supérieur : 963.951 documents, soit 15,18 % des titres délivrés en 2003.

Au Royaume Uni[3], le coût annuel de la fraude liée aux fausses identités serait de 2 milliards d'euros[4]. Le nombre de passeports perdus ou volés est passé de 184.301 en 2003 à 306.406 en 2004 (procédure déclarative).

---

[1] *2.487.377 passeports et 7.177.509 cartes d'identité y ont été délivrés en 2003.*
[2] *6.347.121 documents d'identité y ont été délivrés en 2003 (dont 1.427.387 passeports et 4.919.734 cartes d'identité). La carte nationale d'identité est obligatoire et payante.*
[3] *5.500.000 passeports délivrés en 2003.*
[4] *Enquête du Guardian.*

Selon les autorités britanniques, l'ampleur de la fraude documentaire liée aux fausses identités est très préoccupante. Les banques ont alerté le Gouvernement, faisant état de milliers de cas de fraudes. Il existe par ailleurs un trafic important de permis de conduire, utilisés comme seconde pièce d'identité. Les autorités du Home Office ont d'ailleurs décidé de se doter d'un service de lutte contre la fraude documentaire (NDFU).

Les Etats-Unis ne sont pas épargnés par cette délinquance. **Ainsi, 214.905 plaintes ont été déposées en 2003 (+ 28 % par rapport à 2002)** pour fraude à l'identité sur le territoire américain dont 2000 concernant des personnes ayant tenté de se faire délivrer indûment des passeports (sur 7.255.022 établis).

Le passeport est avec la « carte verte » (destinée aux résidents étrangers) le seul document d'identité délivré au niveau fédéral : comme au Royaume-Uni, il n'existe pas de carte nationale d'identité.

La fraude aux permis de conduire et aux actes d'état civil, délivrés par les Etats fédérés sans harmonisation fédérale sur le format et les sécurités des documents, mobilise également les autorités américaines. Le coût annuel de la fraude liée aux fausses identités a été évalué à 60,8 milliards d'euros[1].

Lors du déplacement aux Etats-Unis d'une délégation de votre mission, les entretiens menés à Washington avec M. James F. Sensenbrenner, président de la commission judiciaire de la Chambre des représentants, et Mme Maura Harty, secrétaire d'état adjoint en charge des affaires consulaires au département d'Etat, ont permis de constater que l'absence de document « national » permettant l'identification de la population américaine (seulement 20 % des citoyens américains possèdent un passeport) posait de réelles difficultés.

b) Un phénomène qui se joue des frontières

Par nature, la fraude aux titres d'identité est internationale.

En effet, elle a pour objet de permettre à ses bénéficiaires de commettre des actes délictueux ou criminels à travers le monde, en se déplaçant librement.

Les fraudeurs profitent même de la diversité des règles nationales pour exploiter les failles des dispositifs de contrôle et de détection.

A titre d'exemple, M. François Barry-Delongchamps, directeur des Français de l'étranger et des étrangers en France au ministère des affaires étrangères, a indiqué que **la notion de nom patronymique était de moins en moins pertinente pour s'assurer de l'identité des personnes**.

---

[1] *Etude du département* ***Retrait décisions d'Aberdeen Group****.*

Il a évoqué des différences notables de qualité des registres d'état civil et la coexistence de dizaines de personnes possédant le même nom dans certains Etats, cette situation étant mise à profit par les fraudeurs. Il a aussi signalé les problèmes fréquents de traduction en français d'identités patronymiques de ressortissants d'Etats où l'alphabet latin n'est pas utilisé, estimant qu'ils pouvaient favoriser la création de fausses identités.

Les spécialistes d'Interpol, qui ont une mission de coordination des politiques de lutte contre la fraude documentaire et de collecte des informations relatives à cette dernière, **estiment à environ 35 millions le nombre de faux documents en circulation dans le monde à l'heure actuelle (10 % de contrefaçons et 90 % de falsifications)**. **Ces fraudes, cela a été rappelé, sont utilisées par des réseaux criminels transnationaux d'immigration clandestine ou de trafics**, par exemple de voitures volées : le chiffre d'affaires de la revente de véhicules « maquillés » à l'aide de faux documents s'élève à environ 600 millions d'euros en France en 2003 selon Europol.

c) Des filières mondiales de contrefaçons

« L'industrie » de la contrefaçon au service de la criminalité dispose d'officines bien organisées et dotées de compétences techniques de pointe, installées notamment en Asie (Thaïlande, Laos, Sri Lanka) et en Bulgarie, qui peuvent répondre à des commandes venues du monde entier, parfois avec l'appui des autorités locales. A titre d'exemple, l'ambassade de France en Thaïlande a porté plainte, en décembre 2003, auprès des autorités thaïlandaises pour contrefaçon de documents français (849 cartes d'identité et 1.355 passeports répertoriées entre juin 2003 et avril 2004).

B. UNE CHAÎNE DE L'IDENTITÉ DÉFAILLANTE

La fraude documentaire profite de la faiblesse de certains maillons de la chaîne de l'identité. Il est ainsi possible d'obtenir de vrais titres d'identité au moyen de fausses pièces justificatives. Les conditions de délivrance des cartes nationales d'identité et des passeports n'offrent pas toutes les garanties de sécurité. Enfin, les moyens de détection des faux documents doivent être renforcés.

1. La possibilité de bénéficier de vrais titres d'identité au moyen de fausses pièces justificatives

La production de pièces justificatives de l'état civil et de la nationalité française est requise pour la première délivrance d'une carte nationale d'identité ou d'un passeport. Or, les conditions d'obtention de ces pièces ne sont pas assez sécurisées.

a) Les pièces demandées

- *Les justificatifs de l'état civil*

Pour obtenir une carte d'identité, le requérant doit produire un extrait d'acte de naissance comportant sa filiation. Le livret de famille est également admis dans la mesure où il a valeur d'extrait d'acte[1].

Pour le passeport, une carte nationale d'identité en cours de validité, un précédent passeport en cours de validité ou un passeport périmé depuis moins de deux ans sont suffisants. L'extrait avec filiation de l'acte de naissance ou le livret de famille n'est nécessaire que si le requérant n'est pas en mesure de produire l'un de ces documents.

Aux termes de l'article 47 du code civil, un acte de l'état civil établi à l'étranger doit être admis en France si rien ne permet de douter de sa régularité.

En l'absence d'acte de naissance ou de document admis en remplacement, il est nécessaire de s'adresser au tribunal de grande instance pour obtenir un jugement déclaratif ou supplétif d'acte de naissance. La transcription de ce jugement permettra de constituer un acte tenant lieu d'acte de naissance.

- *Les justificatifs de la nationalité*

Les modes de preuve de la nationalité française varient en fonction de la situation personnelle des demandeurs.

L'usager qui a bénéficié de l'effet collectif attaché à l'acquisition de la nationalité française par l'un de ses parents (naturalisation, réintégration dans la nationalité française, déclaration) doit produire cette décision, si elle n'est pas portée en marge de son acte de naissance ou, à défaut, un certificat de nationalité française.

Il peut en être dispensé s'il remplit les conditions requises pour bénéficier de l'application du concept de la possession d'état de Français. Cette mesure d'assouplissement des règles en matière de preuve de la nationalité française peut s'appliquer dans certains cas aux personnes qui sont soit nées en France de parents étrangers, soit nées à l'étranger ou dans des départements ou territoires précédemment sous administration française.

Le certificat de nationalité constitue le moyen de preuve le plus couramment utilisé. Depuis la loi n° 95-125 du 8 février 1995, il est délivré par le greffier en chef du tribunal d'instance.

---

[1] *Décret n° 74-449 du 15 mais 1974.*

b) Des conditions de délivrance insatisfaisantes

Les registres de l'état civil sont tenus par les communes depuis la création de celui-ci, en 1792, sauf pour les événements survenus à l'étranger ou dans les territoires anciennement sous administration française et qui concernent des ressortissants français. Ces derniers relèvent en effet de la compétence du service central de l'état civil du ministère des affaires étrangères[1]. Les officiers d'état civil sont placés sous l'autorité du procureur de la République[2].

Ces registres sont bien tenus, comme l'a souligné M. Xavier Richaud, procureur de la République près du tribunal de grande instance de Lyon, lors du déplacement d'une délégation de la mission dans cette ville le 17 mars 2005. Celui-ci a toutefois noté l'impossibilité pour les tribunaux de s'acquitter de leur obligation légale de conservation du double des registres communaux, ces derniers n'étant jamais actualisés, faute de temps et de moyens.

En revanche, la fraude est rendue possible par les conditions de délivrance d'un extrait d'acte de naissance et par les difficultés de vérifier l'authenticité des actes établis à l'étranger.

- *Les conditions de délivrance des extraits ou copies d'actes de l'état civil*

Les conditions posées par le décret n° 62-921 du 3 août 1962 pour la délivrance des actes d'état civil reposent sur un équilibre entre les exigences de publicité et les impératifs de confidentialité qu'impose la protection des éléments relatifs à la vie privée qu'ils contiennent.

L'extrait d'acte de naissance ou de mariage sans indication de filiation, qui comporte principalement l'identité, la date, l'heure et le lieu de naissance ainsi que le sexe de l'intéressé, peut être délivré à tout demandeur sans qu'il ait à justifier des motifs de sa demande.

La copie intégrale ou un extrait de ces mêmes actes comportant mention de la filiation ne peut l'être qu'à l'intéressé majeur ou émancipé, à ses ascendants, ses descendants, son conjoint, son représentant légal ou à un mandataire justifiant d'une procuration. Le requérant doit alors indiquer les nom et prénom usuels des parents de la personne que l'acte concerne. Si les héritiers autres que les ascendants, descendants, frères et soeurs ou conjoints sont dispensés de cette exigence, ils doivent néanmoins justifier de leur qualité

---

[1] Créé par le décret n°65-422 du 1er juin 1965, ce service est situé à Nantes. Il a délivré 1.503.871 copies et actes en 2004.

[2] Ils ont ainsi l'obligation de lui signaler, par écrit, tous renseignements relatifs à des crimes ou des délits dont ils ont eu connaissance dans l'exercice de leurs fonctions, au vu des pièces qui leur ont été présentées dans le cadre d'une procédure administrative (article 40 du code de procédure pénale).

d'héritier par la production d'un acte de notoriété établi par un notaire ou un juge d'instance.

En revanche, la délivrance à un tiers de la copie intégrale d'un acte ou d'un extrait d'acte de naissance, de reconnaissance ou de mariage avec mention de la filiation n'est accordée qu'en vertu d'une autorisation du procureur de la République reposant sur un intérêt légitime démontré.

Les demandes peuvent être effectuées auprès de l'officier de l'état civil mais aussi par correspondance, cette faculté permettant à tous ceux qui ne vivent plus dans leur commune de naissance d'effectuer leurs démarches avec souplesse.

Garantissant la protection de la vie privée des personnes, cette procédure ne paraît pas suffisante pour empêcher la remise de copies ou d'extraits à des individus usurpant une identité.

En effet, à condition de connaître la filiation d'une autre personne, le fraudeur peut se voir remettre des documents d'état civil. Or, pour le ministère de l'intérieur, cette délivrance indue favorise une fraude en « cascade », comprenant une fraude matérielle (altération de l'acte…) mais aussi **l'obtention ultérieure d'un titre authentique** légitimant une identité fictive ou usurpée (« vrai-faux »).

M. Daniel Labrosse, chef du service central de l'état civil, a également signalé la fragilité actuelle des livrets de famille, faciles à modifier ou à compléter pour établir une fausse identité.

Pour lutter contre cette fraude sans entraver les activités des citoyens, un décret n° 2004-1159 du 29 octobre 2004[1] a modifié le décret du 3 août 1962 afin de prévoir que : « *Les copies intégrales et extraits d'actes de l'état civil précisant en outre les noms, prénoms, dates et lieux de naissance des père et mère peuvent être demandés directement aux officiers de l'état civil dépositaires des actes par une administration, un service, un établissement public, un organisme ou une caisse contrôlé par l'Etat, en charge de l'instruction d'un dossier administratif, dès lors que celui-ci ou celle-ci est légalement fondé à requérir ces actes des usagers, sous réserve que ces derniers en aient été préalablement informés*. »

Il ne s'agit toutefois que d'une faculté et la personne qui sollicite un titre d'identité conserve la possibilité de produire elle-même les pièces justificatives demandées.

---

[1] *Décret n° 2004-1159 du 29 octobre 2004 portant application de la loi n° 2002-304 du 4 mars 2002 modifiée relative au nom de famille et modifiant diverses dispositions relatives à l'état-civil.*

- *La validité incertaine des actes de l'état civil établis à l'étranger*

Les relations internationales étant fondées sur la confiance et la réciprocité, l'article 47 du code civil pose le principe selon lequel **tout acte de l'état civil dressé dans un pays étranger**[1], concernant des Français ou des étrangers, **fait foi en France s'il a été rédigé dans les formes usitées dans ledit pays**.

Ces actes doivent remplir certaines conditions (nature d'acte de l'état civil, établissement par un officier de l'état civil conformément à la loi locale[2], traduction en français). La bonne foi du requérant doit être présumée.

Les actes dressés par des autorités étrangères sont transcrits lorsqu'ils concernent des Français, soit d'office, soit à la demande des intéressés, sur les registres consulaires français.

Or, les ministères des affaires étrangères et de l'intérieur ont noté la croissance du nombre des actes de l'état civil établis à l'étranger, irréguliers ou falsifiés.

En 2001 et 2002, le ministère des affaires étrangères a tenté d'évaluer la réalité du phénomène en consultant certains de ses postes consulaires, en particulier d'Afrique francophone. Le nombre d'actes irréguliers, falsifiés ou inexistants a été estimé à 11.000 par an. Or, ces actes représentaient une part importante de ceux présentés aux agents diplomatiques et consulaires (32 % au Nigéria, 60 % en Guinée, 90 % en République démocratique du Congo ou aux Comores).

Les actes de l'état civil frauduleux peuvent résulter d'un manque de rigueur ou de moyens dans la tenue des registres, parfois inexistants (détruits par un conflit …), **mais aussi de la corruption des officiers de l'état civil locaux.**

Des fraudes par falsification de copies et d'extraits d'actes délivrés régulièrement par des officiers de l'état civil français ont également été constatées (cas de substitution volontaire de l'identité de Français établis hors de France).

Ces comportements frauduleux ont, pour objectif essentiel de permettre à leur bénéficiaire de **contourner la législation en vigueur sur l'entrée et le séjour en France et d'obtenir un titre d'identité français**.

---

[1] Les actes établis avant l'indépendance de l'Algérie ou dans d'autres territoires dépendant antérieurement de la France sont considérés en droit comme des actes étrangers.

[2] La preuve du respect de la loi locale peut être apportée par la production d'un certificat de coutume, attestation délivrée par un juriste et mentionnant le contenu de la loi étrangère en cause.

Selon le ministère des affaires étrangères, plusieurs procédures semblent concernées par les fraudes. **Il s'agit tout d'abord de l'acquisition de la nationalité française** par déclaration[1] et de naturalisation par décret[2].

Les justificatifs à partir desquels le service central d'état civil doit établir les actes des postulants ne sont que des copies intégrales d'actes de l'état civil étrangers, qui peuvent s'avérer irréguliers ou frauduleux (il en va de même pour les actes soumis à transcription).

Il s'agit également de **la délivrance des certificats de nationalité française**, qui servent à prouver cette dernière, et peuvent être produits pour l'obtention d'une première carte nationale d'identité ou d'un passeport. Ces certificats doivent être demandés, éventuellement par correspondance, auprès du greffier en chef du tribunal d'instance du domicile ou du lieu de naissance du demandeur.

Or, des fraudes concernant des personnes nées ou résidant à l'étranger ont été relevées par le service central de l'état civil à l'occasion de l'établissement de leur acte de naissance, dont la production est nécessaire à l'obtention d'un certificat. Certains tribunaux d'instance, peu confrontés à des demandes de Français établis hors de France, ont pu délivrer indûment des certificats. Le ministère de la justice a alors engagé un contentieux judiciaire (70 affaires par an en moyenne).

Aussi, depuis le début de l'année, le greffier en chef du tribunal d'instance du premier arrondissement de Paris, qui bénéficie d'une bonne connaissance des actes et des méthodes de fraude utilisées en raison de sa spécialisation progressive dans le contentieux des Français établis hors de France, est seul compétent pour délivrer les certificats aux personnes nées et résidant à l'étranger[3].

Enfin, comme l'ont signalé M. Xavier Richaud, procureur de la République, et Mme Girard Zampino, vice-présidente du tribunal de grande instance de Lyon, **les fraudeurs détournent parfois les jugements déclaratifs ou supplétifs des tribunaux de grande instance pour faire reconnaître une fausse identité**. En effet, ces jugements, dont le dispositif pourra être transcrit sur les registres du service central, tendent à remplacer des actes d'état civil perdus ou inexistants.

---

[1] Articles 21-13 et 21-14 du code civil (enfants majeurs adoptés ou recueillis ; bénéficiaires de la possession d'état de Français depuis dix ans ...).

[2] Articles 21-15 à 21-25 du code civil (étrangers ayant leur résidence habituelle en France depuis cinq ans, bonnes mœurs, assimilation à la communauté française, connaissance de la langue, des droits et des devoirs conférés par la nationalité française...).

[3] Décret n°2005-460 du 13 mai 2005 relatif aux compétences des juridictions civiles, à la procédure civile et à l'organisation judiciaire.

Le Gouvernement français utilise plusieurs dispositifs pour détecter et mettre en échec la fraude :

- la **légalisation** d'un acte étranger (authentification d'une signature et de la qualité du signataire par l'apposition d'un contreseing officiel) est effectuée par le consul français dans la circonscription duquel agit le fonctionnaire étranger qui l'a délivré (l'apostille est un régime de légalisation simplifié). **Toutefois, de nombreuses conventions internationales ont prévu la dispense de cette formalité** ;

- dans le cadre de transcriptions qui leur sont soumises ou à la demande d'autorités françaises auxquelles les actes étrangers sont opposés (préfectures, greffier en chef compétent en matière de nationalité …), **les agents diplomatiques et consulaires peuvent procéder à des vérifications.** Cependant, **jusqu'à la modification de l'article 47 du code civil par la loi du 26 novembre 2003**[1], ces vérifications ne pouvaient remettre en cause la force probante de l'acte étranger.

Désormais, ce dernier fait foi sauf preuve du contraire, c'est-à-dire sauf « *si d'autres actes ou pièces détenus, des données extérieures ou des éléments tirés de l'acte lui-même établissent que cet acte est irrégulier, falsifié ou que les faits qui y sont déclarés ne correspondent pas à la réalité* ».

En cas de doute, l'administration saisie d'une demande d'établissement, de transcription ou de délivrance d'un acte ou d'un titre, surseoit à la demande et informe l'intéressé qu'il peut, dans un délai de deux mois, **saisir le procureur de la République de Nantes** pour qu'il soit procédé à la vérification de l'authenticité de l'acte.

En pratique, celle-ci peut se traduire par une demande de certificat de coutume à l'Etat concerné, par une « *levée d'acte* » (demande de renseignement formulée par lettre) ou par une consultation des registres étrangers par les autorités consulaires françaises.

S'il estime la demande de vérification sans fondement, le procureur en avise l'intéressé et l'administration dans le délai d'un mois.

En revanche, s'il partage les doutes de l'administration, il fait procéder dans un délai de six mois, renouvelable une fois, à toutes investigations utiles. Au vu des résultats de ces dernières, il peut saisir le tribunal de grande instance de Nantes pour qu'il statue sur la validité de l'acte.

---

[1] *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.*

Le décret nécessaire à l'application de la nouvelle procédure a été publié récemment[1] et les premiers éléments chiffrés (22 saisines auxquelles le parquet de Nantes n'a pas donné suite) sont peu significatifs. Il est encore trop tôt pour évaluer son impact sur la fraude.

2. Des modalités d'obtention des cartes d'identité et des passeports qui n'offrent pas toutes les garanties de sécurité

Lors du déplacement d'une délégation de la mission à Lyon, le 17 mars 2005, **M. Alain Barbier, sous-directeur à Interpol, a souligné la nécessité de sécuriser le processus de délivrance des titres d'identité pour lutter contre la fraude.**

a) De nombreux intervenants

Une demande de carte d'identité ou de passeport doit être déposée :

- auprès du maire de la commune du domicile, de résidence ou de rattachement du requérant, ou directement auprès du sous-préfet ou du préfet[2] ;

- à Paris, auprès des antennes de la préfecture de police situées dans les mairies d'arrondissement ;

- à l'étranger, auprès des agents diplomatiques et consulaires.

Dans un but de simplification administrative, elles peuvent faire l'objet d'un même formulaire.

Pour la carte d'identité, le requérant doit comparaître devant l'agent compétent à la fois pour permettre la vérification de son identité, **le recueil de sa signature et le relevé d'une empreinte digitale**, celle de l'index gauche. Pour le passeport, la demande peut être effectuée par un tiers ou par courrier.

Le dossier est ensuite transmis à la préfecture ou sous-préfecture compétente, qui en assure l'instruction et contrôle l'identité du demandeur.

---

[1] Décret n° 2005-170 du 23 février 2005 pris pour l'application des articles 47 et 170-1 du code civil.

[2] Le requérant ne peut s'adresser directement à la préfecture ou à la sous-préfecture qu'en cas d'impossibilité ou d'urgence pour une demande de passeport. Toutefois, le Conseil d'Etat (CE 5 janvier 2005, Commune de Versailles) a annulé le premier alinéa de l'article 7 du décret du 26 février 2001 confiant aux maires la tâche de recueillir les demandes de passeport. Selon l'article L. 1611-1 du code général des collectivités territoriales, aucune dépense de l'Etat ne peut être imposée directement ou indirectement aux collectivités territoriales qu'en vertu de la loi. Le même raisonnement s'applique à la délivrance des cartes d'identité. Une commune peut donc refuser si elle le souhaite de recevoir les demandes de passeport et de carte nationale d'identité.

La fabrication de la carte nationale d'identité est assurée par le Centre national de production des titres qui dispose de deux unités de production à Val Maubuée (Lognes) et Limoges. Celle des passeports est moins centralisée puisque les titres vierges sont fabriqués par l'Imprimerie nationale dans divers sites de production puis acheminés dans les sous-préfectures pour être personnalisés.

Une fois produit, le titre d'identité doit être retiré au lieu du dépôt de la demande. **La carte d'identité est remise en personne ou à un mandataire muni d'une procuration** et justifiant de son identité. **Pour le passeport, la présence du titulaire est requise** puisqu'il doit signer le document. La ressemblance entre la personne et la photographie peut alors être vérifiée.

La délivrance d'un titre donne lieu, en principe, à la restitution de l'ancien. Toutefois, un second passeport peut être délivré lorsque les visas du premier empêchent son titulaire d'effectuer un déplacement ou pour certains motifs professionnels.

Les délais de délivrance de ces documents varient entre huit jours et deux mois pour le passeport et autour de trois semaines en moyenne pour la carte nationale d'identité.

Il existe des procédures accélérées en cas d'urgence ou pour certaines catégories de citoyens, par exemple les personnes sans domicile fixe. Par ailleurs, les modalités de remplacement d'une carte ou d'un passeport sont plus rapides.

b) De meilleurs résultats pour la carte nationale d'identité que pour le passeport

Les conditions d'instruction des demandes et la centralisation de la fabrication des cartes nationales d'identité assurent à ces documents une plus grande sécurité qu'aux passeports.

L'exigence d'une comparution personnelle du requérant et le recueil de sa signature et d'une de ses empreintes digitales permettent une vérification plus poussée de son identité. En revanche, le titre n'est pas remis en personne, alors que cette obligation est prévue pour le passeport.

La centralisation de la production des cartes nationales d'identité permet de faire évoluer les documents en leur apportant des sécurités supplémentaires (papier fiduciaire plastifié, guilloches, encre optique variable, micro perforations et micro impressions, « *terre rare* » réfléchissant la lumière à une fréquence stable quelle que soit la source) et d'éviter le transport et le stockage de titres vierges.

Ainsi la carte nationale d'identité n'est guère falsifiée. Pour autant, la fraude à l'état civil permet d'obtenir indûment de vrais titres et les contrefaçons de qualité se développent.

A l'inverse, en dépit de l'intégration de sécurités nouvelles avec la création en 1999 puis la généralisation en 2002 du modèle DELPHINE[1], **le passeport fait encore l'objet**, comme on l'a vu, non seulement **de contrefaçons mais également de nombreuses falsifications.**

Selon les spécialistes de la police aux frontières, les risques de vols de titres vierges sont accrus par le choix de confier leur transport à des sociétés comme Chronopost, qui utilisent de nombreux sous-traitants, pas toujours bien identifiés par l'Etat.

Au total, le passeport français est très attractif pour les fraudeurs car sa protection contre les techniques de fraude est relative et sa délivrance permet à son titulaire de prouver sa nationalité française et son identité, de bénéficier des droits qui y sont attachés et de posséder un titre de voyage.

3. La détection imparfaite de la fraude documentaire

a) Une sensibilisation aux enjeux de la fraude perfectible

Difficile à détecter et souvent liée à d'autres infractions la fraude à l'identité n'est pas toujours considérée en France comme une infraction grave. Il en résulte parfois une insuffisante sensibilisation des acteurs qui peuvent y être confrontés.

- *La formation des personnels en question*

La détection et la lutte contre la fraude reposent en premier lieu sur les agents des mairies, des sous-préfectures et des préfectures ainsi que des postes consulaires à l'étranger chargés de la délivrance des titres d'identité.

Leur intégrité et leur motivation ne peuvent être mises en cause, sauf en de rares occasions. Ainsi, de 1999 à 2004, 31 agents seulement ont été accusés de fraude et des négligences ont récemment conduit à des vols de passeports dans plusieurs préfectures et sous-préfectures.

En revanche, Mme Elisabeth Rumi et M. Pierre Garcia, respectivement chef du bureau de la fraude documentaire et capitaine à la direction centrale de la police aux frontières, ont déploré tout à la fois :

- le **manque de formation** des personnels des mairies et des préfectures, qui permet parfois l'obtention indue d'actes de l'état civil ou de titres d'identité, notamment au moyen de photographies peu ressemblantes ;

---

[1] *DELivrance de Passeport à Haute INtégritE de sécurité.*

- l'emploi de stagiaires pour l'instruction des dossiers dans certaines préfectures ;

- la difficulté d'avoir des échanges rapides avec les services de police en cas de suspicion de fraude.

En aval de la délivrance des titres, la détection de la fraude relève de la compétence des agents chargés des contrôles d'identité.

Il n'existe pas d'unité spécialement chargée de la lutte contre la fraude documentaire, à l'exception de petites entités spécifiques telles que le bureau de la fraude documentaire à la direction centrale de la police aux frontières, car cette fraude est « *transversale* ».

- *Des moyens de détection qui pourraient être mieux utilisés*

Des moyens de détection de la fraude documentaire existent au long de la « chaîne de l'identité ».

En premier lieu, les demandes de titres d'identité sont recensées dans des fichiers informatiques spécifiques (fichier national de gestion des cartes d'identité créé en 1987 ; fichier des passeports DELPHINE ; fichier national des permis de conduire) gérés par le ministère de l'intérieur.

Ces fichiers de gestion peuvent permettre aux agents chargés de la délivrance des titres de procéder à des vérifications et de détecter les anomalies lors de la procédure de délivrance de titres (demandes réitérées…).

De leur côté, les personnels de la police aux frontières disposent du matériel de base pour opérer des contrôles de premier degré dans des postes fixes ou des unités mobiles ainsi que d'appareils plus sophistiqués pour révéler les documents frauduleux (lecteurs optiques…).

Les documents d'identité volés, qui donnent lieu à un dépôt de plainte auprès de la police ou de la gendarmerie, font l'objet d'une inscription sur la base de leur numéro de série dans les **fichiers de police**. Chaque service compétent a ainsi les moyens, à son niveau, de repérer et de neutraliser les titres frauduleux.

Simultanément, le dispositif comporte des insuffisances notables.

Tout d'abord, ainsi que l'a signalé M. Pierre Garcia, **certaines sécurités des titres d'identité sont inutiles** pour la vérification de leur régularité, **faute de matériel adapté pour les exploiter** dans les services de police et les préfectures (lecteurs pour les « *luminophores* » des cartes d'identité).

Par ailleurs, **l'informatisation des procédures et l'exploitation des fichiers existants pour la détection de la fraude pourraient être confortées**. Le bilan de l'interrogation systématique du fichier des personnes recherchées (FPR) par les agents chargés des dossiers de demandes de titres ou d'un contrôle d'identité « *apparaît mitigé* » selon le ministère de l'intérieur, en dépit de l'inscription d'un millier de personnes en 2004 pour tentative de fraude.

Les personnels qui assurent le contrôle de « *premier degré* » dans les aéroports ou les ports n'ont pas d'accès direct aux fichiers de gestion des titres et ceux-ci offrent de faibles capacités d'exploitation : ainsi, le fichier national de gestion des cartes d'identité ne permet pas de comparer deux photographies issues de demandes différentes établies sous un même état civil.

De plus, les **empreintes digitales** relevées lors des demandes de titres sont conservées « *sous forme papier* » dans les préfectures et sous-préfectures. **Les agents confrontés à un soupçon de fraude** et désireux de vérifier l'effectivité ou la régularité d'une délivrance de titre doivent obtenir communication (par courrier) des dossiers de demandes concernés ou interroger les administrations intéressées. Ainsi, en pratique, ils **opèrent peu ces contrôles** en raison de la nécessaire rapidité du traitement des demandes de titres.

Enfin, les pertes de titres d'identité sont mal recensées. Les particuliers effectuent parfois des démarches tardives (déclarations) pour signaler la perte de leur titre auprès des mairies ou des préfectures. En théorie, la transmission de ces déclarations ainsi que de messages de vigilance signalant des pertes répétées aux services de police devrait être immédiate. Les pertes ne font pas l'objet d'un suivi précis (les fichiers de gestion semblent ne pas le permettre).

En revanche, les sanctions pénales prévues pour punir la fraude documentaire à l'identité paraissent satisfaisantes.

b) Des sanctions pénales suffisantes

Les diverses modalités de la fraude à l'identité, qui n'est pas un phénomène nouveau, sont réprimées par le droit en vigueur.

Sont sanctionnés :

- la modification illicite du nom et de l'état-civil dans un acte public ou authentique (six mois d'emprisonnement et 7.500 euros d'amende)[1] ;

- le fait de prendre le nom d'un tiers, dans des circonstances qui ont déterminé ou auraient pu déterminer contre celui-ci des poursuites pénales (cinq ans d'emprisonnement et 75.000 euros d'amende)[2] ;

- la fabrication, l'usage et le recel d'un document administratif constatant une identité (même peine ou sept ans d'emprisonnement et 100.000 euros d'amende si l'infraction est habituelle ou commise par un agent public dans le cadre de ses fonctions)[3] ;

- le fait de détenir, de fournir ou d'obtenir frauduleusement un document administratif constatant une identité (de deux ans d'emprisonnement et 30.000 euros d'amende à sept ans d'emprisonnement et 100.000 euros d'amende)[4] ;

- l'escroquerie lorsqu'une fausse identité est utilisée pour obtenir indûment des prestations de la part des organismes de sécurité sociale ou de caisses d'allocations familiales (cinq ans d'emprisonnement et 375.000 euros d'amende, dix ans d'emprisonnement et un million d'euros d'amende si l'infraction a été commise en bande organisée)[5].

En outre, des peines complémentaires peuvent être prononcées à l'encontre des fraudeurs (interdiction des droits civiques ou d'exercer certaines activités…)[6].

Selon M. Philippe Lagauche, directeur adjoint des affaires criminelles et des grâces au ministère de la justice, l'échelle des peines existantes répond à l'ensemble des situations rencontrées.

Le quantum de ces peines semble en moyenne assez important pour réprimer la fraude à l'identité, d'autant que celle-ci est souvent sanctionnée comme infraction connexe à un délit ou à un crime plus graves.

---

[1] *Article 433-19 du code pénal.*
[2] *Articles 434-23 du code pénal et 781, alinéa 2, du code de procédure pénale.*
[3] *Articles 321-1 et 441-2 du code pénal.*
[4] *Articles 441-3, 441-5 et 441-6 du code pénal.*
[5] *Articles 313-1 et 313-2 du code pénal.*
[6] *Articles 441-10 et 441-11 du code pénal.*

C. DES PISTES DE RÉFORME

La lutte contre la fraude aux titres d'identité actuels implique de se doter des moyens d'en évaluer précisément l'ampleur, de mieux détecter les faux, de sécuriser les conditions de délivrance des documents et de s'interroger sur l'opportunité de réduire le nombre des documents valant titre d'identité.

1. L'harmonisation et la centralisation des statistiques relatives à la fraude documentaire

Les travaux conduits par la mission d'information lui ont permis de constater la réalité de la fraude documentaire mais pas de la quantifier. Une évaluation précise s'avère pourtant nécessaire pour déterminer les réponses idoines. Elle nécessite une harmonisation et une centralisation des statistiques actuelles.

a) Harmoniser les statistiques

L'état 4001 du ministère de l'intérieur constitue certainement l'un des outils statistiques les plus précis et les plus perfectionnés parmi les pays européens. Il **pourrait** cependant **être complété afin de mieux appréhender la fraude aux titres d'identité**.

Comme l'avaient déjà souligné MM. Robert Pandraud et Christophe Caresche dans un rapport établi en 2002 à la demande du Premier ministre, il conviendrait en outre de **remédier à l'absence de coordination et à l'éparpillement des différentes sources d'information**, **au cloisonnement des systèmes d'information d'un ministère à l'autre et à l'absence de croisement des différents instruments de mesure**[1].

A cet égard, il est intéressant de relever que les autorités allemandes ont décidé au mois de mai 2005 de réactiver un fichier fédéral créé en 1981 afin de recenser la fraude documentaire mais tombé en désuétude faute de mise à jour.

Le **recours aux enquêtes de victimation** permettant une meilleure connaissance des infractions non déclarées aux services de police et de gendarmerie ou ignorés des policiers et gendarmes constituerait par ailleurs une approche complémentaire au dispositif 4001.

---

[1] *« Sur la création d'un Observatoire de la délinquance » - rapport de MM. Christophe Caresche et Robert Pandraud au Premier ministre - la Documentation française - 2002.*

b) Centraliser les informations

La direction générale de la police nationale avait émis le souhait, en 2003, de créer un office central de la fraude documentaire. Cette proposition n'a pas eu de suite tant il est vrai que le nombre des offices, observatoires et autres commissions est pléthorique en France.

Plutôt que de créer un nouvel organisme, sans doute serait-il judicieux de **confier cette mission à l'Observatoire national de la délinquance**, ainsi que l'ont suggéré le président de son conseil d'orientation, M. Alain Bauer, mais également M. Philippe Lagauche, directeur adjoint des affaires criminelles et des grâces au ministère de la justice.

Installé le 4 novembre 2003, rattaché à l'Institut national des hautes études de sécurité, l'Observatoire a déjà pour missions de recueillir les données statistiques relatives à la délinquance auprès de tous les départements ministériels et organismes publics ou privés ayant à connaître directement ou indirectement de faits ou de situations d'atteinte aux personnes ou aux biens, d'exploiter les données recueillies, de communiquer les conclusions qu'inspirent ces analyses aux ministres intéressés et à ses partenaires, d'assurer la mise en cohérence des indicateurs, de la collecte et de l'analyse des données, de faciliter les échanges avec d'autres observatoires, en particulier l'Observatoire des zones urbaines sensibles, d'animer un réseau de correspondants et d'organiser la communication au public de ces données.

Il semble le mieux à même de réunir des données consolidées sur la fraude à l'identité, d'apprécier ses usages par les réseaux terroristes et mafieux et d'évaluer ses conséquences financières.

2. L'amélioration de la détection des faux documents d'identité

L'amélioration de la détection de faux documents d'identité suppose, d'une part, de développer la formation et l'équipement des agents qui en sont chargés, d'autre part, de renforcer les coopérations internationales.

a) Développer la formation et l'équipement des agents

Selon le ministère de l'intérieur, **des efforts très significatifs ont été consentis au cours des dernières années pour améliorer la détection des faux documents**.

S'agissant de la police aux frontières, **tous les services disposeraient du matériel de détection de base permettant d'effectuer des contrôles de premier niveau**, tant au sein des postes fixes des ports et aéroports que des unités mobiles : trousses d'inspection contenant des lampes et des loupes

spécialisées ainsi que des compte-fils[1]. Des appareils plus sophistiqués combinant différentes techniques (« Retrocheck ») seraient également disponibles. Enfin, un **plan d'acquisition de lecteurs optiques des documents de voyage** serait en cours de réalisation depuis 2003, 509 appareils d'un coût total de 1,1 million d'euros devant être installés dans un délai de trois ans.

La fraude documentaire est abordée au cours de la **formation initiale** des gardiens de la paix (un module de deux heures de cours), des officiers de police (un module de dix-huit heures de cours) et des commissaires (divers modules théoriques et pratiques). La direction centrale de la police aux frontières a mis en place un logiciel d'aide à la reconnaissance de la fraude documentaire (SINBAD) recensant les différents modèles de titres, français et étrangers, les types de sécurisation et les modalités connues de falsification. Une centaine de personnes bénéficiant de formations spécialisées a été affectée dans les principaux aéroports. Enfin, de nombreux agents suivent des stages dans le cadre de **la formation continue**, comme en témoigne le tableau ci-après.

Stages de formation continue à la fraude documentaire

	Formations centrales		**Formations locales**	
	stagiaires	**heures/fonctionnaires**	**stagiaires**	**heures/fonctionnaires**
2002	870	10.842	306	1.517
2003	760	9.621	315	2.657
2004	1.166	14.448	197	1.900

Source : ministère de l'intérieur.

Ces efforts doivent être poursuivis. Comme le soulignaient Mme Elisabeth Rumi et M. Pierre Garcia, respectivement chef du bureau de la fraude documentaire et capitaine à la direction centrale de la police aux frontières, **il importe surtout de développer la formation des agents de terrain, c'est-à-dire des gardiens de la paix**.

b) Approfondir les coopérations internationales

M. François Barry-Delongchamps, directeur des Français à l'étranger et des étrangers en France, indiquait à juste titre, lors de son audition par la mission, que le caractère mondial de la fraude documentaire nécessite de renforcer les coopérations internationales.

---

[1] *Le compte-fils est une loupe à fort grossissement munie le plus souvent d'un gabarit assurant la distance optimale de l'optique à ce qui est examiné, ainsi qu'une échelle de mesure.*

Si la collaboration entre Etats est fructueuse au sein de l'Organisation de l'aviation civile internationale (OACI) et de l'Union européenne pour fixer des normes standardisées de protection des titres de voyage, la coopération internationale en matière de détection de la fraude semble perfectible.

La France joue un rôle essentiel dans les travaux de la Commission internationale de l'état-civil[1], qui constitue un lieu d'échange privilégié entre les services de ses Etats membres. La Commission dispose d'un groupe de travail spécialisé sur la fraude et a adopté, au mois de mars 2005, une « *recommandation relative à la lutte contre la fraude documentaire en matière d'état-civil* », précisant les indices susceptibles de révéler le caractère frauduleux d'actes de l'état-civil. Son secrétaire général, M. Paul Lagarde, a toutefois indiqué devant la mission que la faiblesse des moyens de cet organisme limitait sa capacité d'initiative.

Le contrôle des actes de l'état civil étrangers demeure difficile car les procédures (levées d'actes, consultations des registres étrangers…) **nécessitent l'accord des Etats concernés**. Le ministère des affaires étrangères a indiqué que ces derniers se montraient plus ou moins coopératifs : dans certains pays, la vérification des actes nécessite un délai de dix-huit mois à deux ans ; dans d'autres, les demandes des autorités françaises n'aboutissent jamais.

La **coopération en matière de détection des faux titres d'identité** permet aux experts français de partager leur expérience avec leurs collègues étrangers et de s'adapter aux nouveaux type de fraude au sein de plusieurs structures internationales : groupes de travail de l'OACI et du G8[2] ; groupe « frontières » de l'Union européenne ; coopération policière technique bilatérale.

La France participe par ailleurs aux actions et aux échanges d'information du système Schengen, d'Europol et d'Interpol.

Les **accords de Schengen** du 14 juin 1985 et du 19 juin 1990 ont pour objet la suppression des contrôles de personnes aux frontières communes entre les Etats signataires et le renforcement de la coopération policière, douanière et judiciaire.

Ils ont été signés par quinze Etats européens : la France, l'Allemagne, la Belgique, le Luxembourg, les Pays-Bas, l'Italie, la Grèce, l'Espagne, le Portugal, le Danemark, l'Autriche, la Suède, la Finlande, la Norvège et

---

[1] La CIEC est composée de 16 membres : Allemagne, Autriche, Belgique, Croatie, Espagne, France, Grèce, Hongrie, Italie, Luxembourg, Pays-Bas, Pologne, Portugal, Royaume-Uni, Suisse, Turquie. Six autres pays ont un statut d'observateur.

[2] Le G8 est la réunion régulière des chefs d'Etat de l'Allemagne, du Canada, des Etats-Unis, de la France, de l'Italie, du Japon, du Royaume-Uni et de la Russie. Au cours de ses sommets, les dossiers de l'actualité mondiale y sont examinés dans un cadre informel.

l'Islande. Les cinq pays de l'Union nordique des passeports (Danemark, Suède, Finlande, Norvège et Islande) sont rentrés dans l'espace Schengen le 25 mars 2001. Conformément au protocole joint au traité d'Amsterdam, l'Irlande et le Royaume-Uni ont été autorisés, respectivement en 2000 et en 2002, à participer à une partie seulement des dispositions de l'acquis de Schengen. En outre, cet acquis a été intégré dans l'Union européenne. A la suite d'une votation organisée le 5 juin, la Suisse devrait également prochainement entrer dans l'espace Schengen.

Au sein de cet espace, un réseau automatisé appelé « Système d'information Schengen » (SIS) a été élaboré, non sans difficultés au niveau technique, pour permettre à tous les postes de police et les agents consulaires des États ayant adhéré à l'espace Schengen de disposer de données sur les personnes signalées, les documents volés, les objets ou véhicules recherchés. La base de données est alimentée par les Etats membres grâce à des réseaux nationaux (N-SIS) connectés à un système central (C-SIS). Au 26 avril 2005, elle contenait 10.590.701 documents volés, vierges ou personnalisés, dont 2.204.141 inscrits par la France. Cette construction informatique est complétée par un réseau nommé SIRENE (Supplément d'information requis à l'entrée nationale), composé de représentants de la police, de la gendarmerie, des douanes et de la justice. Une refonte du système (SIS II) est en cours pour lui permettre de fonctionner avec les nouveaux Etats membres de l'Union européenne.

De son côté, l'**Office européen de police** « Europol », dont le mandat a été étendu le 1er janvier 2002 aux formes graves de la criminalité internationale, a pour objet d'améliorer l'efficacité des services compétents des Etats membres et leur coopération dans le cadre de la prévention et de la lutte contre ces activités. Il intervient en facilitant l'échange d'informations entre les officiers de liaison détachés auprès de lui par les Etats membres. Toutefois, l'office ne dispose pas de fichier d'analyse traitant spécifiquement de la falsification de documents. Il pourrait se voir conférer un accès direct au système d'information Schengen.

Créée en 1923, l'Organisation internationale de police criminelle **Interpol** a pour objet de favoriser la coopération et les échanges d'information entre les polices nationales de ses 182 Etats membres. Elle dispose aujourd'hui de bases de données importantes sur les empreintes digitales, les profils ADN ou encore les véhicules volés, qui sont alimentées et peuvent être consultées en permanence par les forces de police nationales.

La base de données relative aux documents de voyage volés ou perdus, alimentée par 60 pays environ, recense ainsi 6 millions de documents. Elle est d'un accès facile et rapide, comme ont pu le constater les membres de la mission qui se sont rendus au siège de l'organisation le 17 mars 2005.

M. Jean-Michel Louboutin, directeur exécutif d'Interpol, a toutefois indiqué que les autorités françaises semblaient réticentes au partage des informations relatives aux documents volés et en assuraient une transmission partielle. Expliquant que ces réticences étaient motivées par le souci légitime de protection de la vie privée de nos ressortissants, il a précisé que chaque Etat pouvait toutefois choisir avec quel autre Etat membre il souhaite partager ses données. Il a en outre regretté une sous-utilisation des moyens mis à la disposition des agents français chargés des contrôles d'identité, observant à titre d'exemple que ces derniers n'avaient pas d'accès direct à la base de données d'Interpol.

Aussi le Conseil de l'Union européenne a-t-il adopté, le 20 janvier 2005, une **position commune relative à l'échange de certaines données avec Interpol** qui « *contraint les Etats membres à faire en sorte que leurs autorités compétentes échangent les données susmentionnées en utilisant la base de données d'Interpol sur les documents de voyage volés et les saisissent parallèlement dans une base de données nationale appropriée et dans le SIS pour les Etats membres qui y participent*. »

La mission d'information souscrit à cette démarche. En matière de documents de voyage faux ou volés, la coopération au niveau international est l'échelon le plus pertinent. Il est contre-productif de multiplier les fichiers de documents volés, comme les membres du G5[1] ont pu le suggérer en proposant au début de l'année de créer un fichier de ce type entre eux.

3. La sécurisation des conditions de délivrance des titres d'identité

La sécurité des conditions de délivrance des titres d'identité peut encore être renforcée. Elle suppose d'empêcher la délivrance indue de vrais documents d'identité au moyen d'une fraude à l'état civil, de prévenir l'usage frauduleux de titres authentiques et de revoir les conditions de délivrance des permis de conduire et des titres de séjour.

a) Empêcher l'obtention indue de vrais documents d'identité au moyen d'une fraude à l'état civil

Nonobstant les progrès induits par la publication du décret n° 2004-1159 du 29 octobre 2004, qui permet à une administration, un service, un établissement public, un organisme ou une caisse contrôlé par l'Etat en charge de l'instruction d'un dossier administratif de demander les copies intégrales et extraits d'actes de l'état civil directement aux officiers de l'état civil qui en sont dépositaires, la réflexion doit se poursuivre sur la **dématérialisation de l'état civil**.

---

[1] *Le G5 est un groupe informel réunissant régulièrement les ministres de l'intérieur de l'Allemagne, de l'Espagne, de la France, de l'Italie et du Royaume-Uni.*

A la différence d'autres pays européens, **la France ne dispose pas d'un fichier national de l'état civil**.

Depuis la parution du décret n° 97-852 du 16 septembre 1997, les communes ont la possibilité de recourir à des systèmes informatisés pour la tenue de leurs registres. L'article 1317 du code civil, inséré par la loi nº 2000-230 du 13 mars 2000, dispose qu'un acte authentique peut être dressé sur support électronique. Le 24 juin 2004, la Commission nationale de l'informatique et des libertés a adopté une norme simplifiée sur la gestion de l'état civil par les communes afin de leur permettre de déclarer de façon plus simple et plus rapide les traitements courants.

Une partie importante du fonds d'actes dont le service central d'état civil de Nantes est dépositaire est d'ores et déjà informatisée. Tel n'est pas le cas de l'ensemble des 36.000 communes de France, dont les équipements ne sont au surplus pas homogènes.

Selon le ministère de la justice : « ***il n'est envisagé ni de créer un fichier national de l'état civil, ni de contraindre les communes à dématérialiser leurs registres*** *mais de permettre à celles qui le souhaitent de ne plus tenir de registre sur support papier dès lors que leur support informatique répond à des conditions d'authenticité, de sécurité et de conservation adaptées à la nature juridique des actes authentiques*. »

L'une des pistes étudiées pour améliorer la lutte contre la fraude consisterait à **utiliser le répertoire national d'identification des personnes physiques (RNIPP) tenu par l'Institut national de la statistique et des études économiques (INSEE) pour vérifier les informations communiquées par les demandeurs de titres d'identité**, le rôle de l'Institut se limitant à confirmer ou infirmer leur exactitude sans possibilité de communiquer ses propres données. Sa mise en œuvre suppose de compléter le répertoire en y intégrant les données relatives à la filiation des individus. La télétransmission des actes serait ainsi généralisée puisque toutes les données détenues par l'INSEE sont dématérialisées.

La **création d'un fichier centralisé des données relatives à la nationalité** est également à l'étude. Y seraient recensés : les demandes de délivrance de certificats de nationalité, les certificats délivrés, les refus de délivrance notifiés par les tribunaux d'instance et les données relatives aux contentieux. MM. Daniel Labrosse, chef du service central d'état-civil au ministère des affaires étrangères, et Marcel Faure, commissaire divisionnaire, chef de la division nationale de répression des atteintes aux personnes et aux biens de la direction centrale de la police judiciaire, ont indiqué à la mission qu'un tel fichier faciliterait la tâche des tribunaux d'instance et dissuaderait les demandeurs de se présenter successivement ou concomitamment auprès de différents greffes : sur les 161.248 demandes de certificat examinées par les tribunaux d'instance en 2003, 147.377 avaient été acceptées et 8.935 rejetées.

b) Prévenir l'usage frauduleux d'un titre authentique

L'augmentation sensible du nombre des cartes nationales d'identité perdues ou volées depuis que leur délivrance est devenue gratuite, c'est-à-dire le 1er septembre 1998, conduit à s'interroger sur le bien fondé de cette mesure.

Le nombre des déclarations de perte ou vol de cartes nationales d'identité a été multiplié par 14, passant de 37.000 en 1997 à 527.000 en 2003.

La gratuité de ces documents n'incite pas leurs titulaires à la vigilance, grève les finances publiques et favorise la fraude. Mme Elisabeth Rumi, chef du bureau de la fraude documentaire à la direction centrale de la police aux frontières, a ainsi indiqué à la mission qu'une même identité avait pu être utilisée par sept personnes différentes pour obtenir, selon les cas, une carte nationale d'identité, un passeport ou un permis de conduire au moyen d'une déclaration de perte ou de vol. Par ailleurs, selon les chiffres communiqués par le ministère de l'intérieur, le nombre des personnes inscrites au fichier des personnes recherchées pour fraude à la carte nationale d'identité reste faible mais a été multiplié par 6 entre 2000 et 2003, passant de 138 à 816.

En l'état actuel du droit, les pertes répétées de titres d'identité ne peuvent fonder un refus de renouvellement, dans la mesure où ces documents permettent l'exercice effectif de la liberté d'aller et venir garantie aussi bien par la Constitution[1] que par les engagements internationaux de la France[2]. Le Conseil d'Etat a ainsi indiqué que la délivrance et le renouvellement d'un passeport ne pouvaient être refusés que si les déplacements de l'intéressé risquaient de compromettre la sécurité nationale ou la sécurité publique[3]. Les agents de l'Etat ne peuvent qu'avertir les intéressés qu'ils s'exposent à des poursuites pénales en cas de fraude.

Il conviendrait donc, afin de lui restituer sa valeur, de rendre à nouveau payante la délivrance de la carte nationale d'identité, fût-ce pour une somme modeste, et d'instituer des pénalités en cas de pertes ou de vols répétés d'un titre d'identité. Les personnes défavorisées pourraient bénéficier d'exonération.

Sans doute serait-il également utile de **créer un fichier centralisé des titres d'identité délivrés précisant leur statut** : valide, perdu ou volé. Le suivi des documents s'en trouverait amélioré et la lutte contre les filières de la fraude renforcée.

---

[1] Décision n°79-107 DC du 12 juillet 1979 du Conseil constitutionnel sur la loi relative à certains ouvrages reliant les voies nationales ou départementales.
[2] Article 2 du protocole n°4 additionnel à la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales.
[3] Conseil d'Etat, 8 avril 1987, ministère de l'intérieur contre Peltier.

Si les documents volés, qu'ils soient vierges ou personnalisés, font en effet actuellement l'objet d'une inscription sur la base de leur numéro de série dans les fichiers de police (le système de traitement des infractions constatées), avec extraction au profit de la base de données de l'espace Schengen et du fichier Interpol, les mairies et les préfectures sont en revanche directement responsables de l'enregistrement des déclarations de perte effectuées par les particuliers.

c) Centraliser la production des passeports et sécuriser les permis de conduire et les titres de séjour

La carte nationale d'identité est très peu falsifiée car sa production est centralisée, ce qui permet d'utiliser des techniques très sophistiquées et d'éviter le transport de titres vierges. Il apparaît indispensable **de centraliser la production des passeports, aujourd'hui éparpillée dans l'ensemble des préfectures.**

De la même manière, les conditions de délivrance des permis de conduire et des titres de séjour pourraient être sécurisées en centralisant leur production et en évitant le transport de documents vierges.

S'agissant des **permis de conduire**, la directive 91/439/CEE du 29 juillet 1991 a déjà harmonisé profondément leur régime, posé le principe de la reconnaissance mutuelle des permis délivrés par les Etats membres et instauré un modèle communautaire de permis en papier, son utilisation demeurant facultative. Une refonte de ce document est en cours[1]. Les nouveaux permis devraient obligatoirement être délivrés sous le format d'une carte plastique aux dimensions d'une carte de crédit, les Etats ayant en outre la possibilité d'y insérer une puce. Ils seraient soumis à un renouvellement administratif périodique et harmonisé : les permis A et B seraient renouvelés tous les dix ans et, pour les plus de 65 ans, tous les cinq ans. En France, en Belgique, en Allemagne et en Autriche, leur durée de validité est actuellement illimitée.

Tout en approuvant ce projet de refonte, **votre commission des Lois** s'est opposée, **par une résolution** adoptée le 16 juin 2004 sur le rapport de notre ancien collègue M. Lucien Lanier, à l'harmonisation de la durée de validité des permis de conduire des véhicules des catégories A et B dans les différents Etats membres, qu'elle a jugé contraire aux principes de subsidiarité et de proportionnalité. Elle **a** en outre **invité la Commission européenne à accélérer ses réflexions sur la création d'une interface informatique commune** permettant à chaque Etat de consulter rapidement le fichier des permis de conduire des autres Etats membres[2]. De telles solutions techniques

---

[1] Proposition de directive CE du Parlement européen et du Conseil relative au permis de conduire (refonte) - document COM (2003) 621.

[2] La Commission a lancé une étude dénommée RESPER relative à la mise en place d'un réseau d'échange entre les fichiers nationaux des permis de conduire.

devraient notamment faciliter l'exécution des décisions de retrait, d'annulation ou de suspension du droit de conduire prises par un Etat membre différent de l'Etat de résidence. Cette proposition de résolution est devenue résolution du Sénat le 29 juin 2004.

Les **titres de séjour** donnent actuellement lieu à la délivrance de deux types de documents : une vignette autocollante, éditée par les préfectures et insérée dans le passeport de l'étranger pour les autorisations de séjour inférieures ou égales à un an ; une carte plastifiée de même format que la carte nationale d'identité, fabriquée par le Centre de production des titres à Val Maubuée et délivrée par la préfecture pour les autres autorisations de séjour.

Le Conseil de l'Union européenne a adopté une action commune le 16 décembre 1996 puis, le 13 juin 2002, un **règlement** (CE) n° 1030/2002 **établissant un modèle uniforme européen de titre de séjour pour les ressortissants des pays tiers**, afin de faciliter l'authentification par les autorités nationales de ces documents tout en mettant en place des standards élevés pour leur sécurisation. Ce processus devrait conduire à la centralisation de l'impression des titres de séjour.

4. La réduction du nombre des documents valant titre d'identité

Une piste pour améliorer la protection de l'identité de nos concitoyens consisterait à ne retenir comme documents valant titre d'identité que ceux dont les conditions de délivrance sont les plus sûres : la carte d'identité et le passeport. La question de la fusion de ces deux documents mérite également d'être étudiée même si elle soulève des difficultés juridiques et pratiques.

a) Retenir la carte d'identité et le passeport comme seuls documents valant titre d'identité pour l'ensemble des relations avec l'administration

La carte nationale d'identité et le passeport devraient être retenus comme les seuls documents valant justificatif d'identité pour l'ensemble des relations avec l'administration tant que d'autres documents, notamment le permis de conduire, n'offrent pas un niveau de sécurité équivalent. Ceci ne remettrait pas en cause la règle, posée notamment par l'article 78-2 du code de procédure pénale, selon laquelle il est possible de justifier de son identité par tout moyen à l'occasion d'un contrôle d'identité. Dans cette hypothèse, le passeport devrait acquérir la même valeur probante que la carte nationale d'identité.

Les habitudes de nos concitoyens ne s'en trouveraient guère bouleversées. La présentation d'une carte nationale d'identité est en effet

exigée pour l'accomplissement de nombreuses démarches administratives, ce qui rend de fait sa possession quasiment obligatoire. Ainsi, aux termes du décret n° 2000-1277 du 26 décembre 2000 portant simplification de formalités administratives et suppression de la fiche d'état civil, une photocopie lisible de la carte nationale d'identité en cours de validité vaut justificatif de l'identité, de l'état civil ou de la nationalité française de l'usager dans le cadre des démarches administratives dites courantes. En outre, dans la mesure où environ 5 millions de cartes d'identité et 2,7 millions de passeports sont délivrés chaque année, on peut légitimement penser que la plupart des Français possède l'un au moins de ces deux documents.

Une telle obligation, bien que n'imposant pas la possession d'une carte d'identité ou d'un passeport, pourrait soulever en revanche une question de principe en raison de notre histoire. Ce fut en effet une loi du 27 octobre 1940 qui, dans un but de contrôle de la population, imposa aux personnes âgées de plus de 16 ans d'être titulaires d'une carte d'identité comportant leurs empreintes digitales et leur photographie et de déclarer leurs changements d'adresse. Toutefois, les réticences de la population et les pénuries de papier, de matériel et de personnel entravèrent considérablement la distribution de la carte. Après la Libération, elle fut supprimée et les fichiers détruits.

Pour autant, les dérives du passé, si elles ne doivent pas être oubliées, ne suffisent à justifier le refus de toute réforme, dès lors que des garanties appropriées sont apportées à la protection des libertés individuelles.

Une étude réalisée par le service des Affaires européennes du Sénat en février 2003 montre que la détention de la carte d'identité est obligatoire dans un grand nombre d'Etats européens - l'Allemagne, la Belgique, le Danemark, l'Espagne, les Pays-Bas et le Portugal - sans que cette obligation soit ressentie par leurs citoyens comme une atteinte à leurs droits[1].

b) Etudier la possibilité de fusionner la carte nationale d'identité et le passeport

La question de la fusion de la carte nationale d'identité et du passeport mérite également d'être étudiée même si elle soulève des difficultés juridiques et pratiques.

Ces deux documents constituent en effet à la fois des titres d'identité et, au sein l'Union européenne et de la plupart des Etats membres du Conseil de l'Europe, des documents de voyage. Leur délivrance peut faire l'objet d'une même demande et être soumise à une procédure unifiée.

---

[1] *Document n° LC-118 – février 2003.*

Leur fusion simplifierait la vie de nos concitoyens et diminuerait leurs coûts de production. Elle s'avère toutefois difficile à réaliser dans la mesure où le passeport est soumis à de nombreuses normes internationales, édictées par l'OACI et l'Union européenne, qui devraient alors s'appliquer à la carte nationale d'identité et en contraindre à la fois le format, le contenu et les usages.

Ainsi, le format actuel de la carte nationale d'identité ne permet pas de recueillir les visas et les tampons imposés par certains Etats pour accéder à leur territoire et en sortir. En application du règlement n° 2252/2004 (CE) du Conseil du 13 décembre 2004, le passeport devra comporter une puce électronique intégrant des données biométriques -la photographie et les empreintes digitales- qui ne pourront être utilisées que pour vérifier l'authenticité du document et l'identité de son titulaire. La désignation des autorités et des organismes habilités à consulter les données sur le support de stockage des documents est en revanche régie par la législation nationale. En cas de fusion, la carte nationale d'identité devrait nécessairement intégrer de telles données et ne pourrait être utilisée à d'autres fins, par exemple d'authentification à distance et de signature électronique.

En l'état actuel du droit, la fusion de la carte nationale d'identité et du passeport reviendrait à supprimer la première au bénéfice du second, donc à retenir comme titre d'identité national un document de voyage soumis à des règles internationales sur lesquelles l'Etat a peu de maîtrise. C'est donc du choix des usages de la carte nationale d'identité que dépend cette piste de réforme.

II. LES GARANTIES DEVANT ENTOURER LE DÉVELOPPEMENT D'UNE NOUVELLE GÉNÉRATION DE TITRES D'IDENTITÉ ÉLECTRONIQUES

Une nouvelle génération de titres d'identité électroniques émerge dans les pays occidentaux. Certains comportent des données biométriques afin d'assurer un meilleur contrôle de l'identité de leurs titulaires. D'autres intègrent des fonctions d'authentification et de signature électroniques afin de promouvoir le développement de l'administration et du commerce électroniques. Dans la mesure où ils sont susceptibles de donner lieu à des traitements automatisés de données à caractère personnel, leur développement éventuel doit être entouré de garanties préservant les libertés individuelles.

A. UN TITRE D'IDENTITÉ BIOMÉTRIQUE : QUELS AVANTAGES POUR LA SÉCURITÉ ?

Les technologies biométriques ouvrent de nouvelles possibilités. Sujet de controverse, la biométrie est pourtant déjà une réalité. Elle s'impose d'ores et déjà comme un instrument fort de sécurisation des documents. Toutefois, la plus-value en terme de sécurité reste mal évaluée. La biométrie n'est pas une solution miracle ; son efficacité dépend de nombreux facteurs.

1. La biométrie : définition et intérêt

a) Définition

La biométrie est, au sens étymologique, la mesure des choses vivantes. Appliquée à l'homme, elle constitue l'anthropométrie[1]. Toutefois, par un abus de langage, **la biométrie désigne l'ensemble des technologies de reconnaissance physique ou biologique des individus.**

En effet, chaque être humain se distingue de ses « semblables » par un ensemble de caractéristiques morphologiques et biologiques qui rendent son identification possible. Le cerveau humain effectue en permanence des opérations de reconnaissance biométrique, notamment de reconnaissance faciale. Lorsque nous croisons un individu, nous mesurons inconsciemment l'écartement des yeux, la taille du nez, la position des oreilles. Ces informations sont comparées à notre mémoire afin d'y associer un nom.

Les technologies biométriques fonctionnent d'une façon similaire. Couplée à des traitements informatisés de plus en plus puissants, la biométrie peut permettre l'identification d'un individu parmi plusieurs millions avec certitude. La précision du système varie selon le type et le nombre d'éléments biométriques utilisés.

En effet, ces données biométriques sont de plusieurs types, chacune présentant des avantages et des inconvénients en fonction de l'usage qui en est fait. Les principales sont la morphologie du visage, les empreintes digitales ou palmaires, la forme de la main, la reconnaissance de l'iris et les empreintes génétiques. D'autres sont plus confidentielles ou expérimentales comme le dessin du réseau veineux de la main. M. Emmanuel-Alain Cabanis, président de la Société de biométrie humaine, a évoqué la cartographie intracorporelle, notamment celle des circonvolutions du cerveau.

---

[1] *Née au milieu du XIXème siècle, l'anthropologie est la science de l'homme. L'une de ses branches, l'anthropologie physique ou anthropométrie, étudie les caractères anatomiques et biologiques de l'homme.*

b) Des utilisations anciennes

A l'origine, l'anthropométrie s'est efforcée d'établir des corrélations physiques précises distinguant l'homme des autres espèces animales. Un des développements[1] de cette discipline fut l'anthropométrie judiciaire également appelé bertillonnage[2]. Cette méthode d'identification des criminels par leurs mensurations prit un essor particulier avec la découverte des empreintes digitales dans les premières années du XXème siècle.

Aujourd'hui, **la police scientifique** reste le principal champ d'application de la biométrie. Ainsi, au 1er janvier 2005, le fichier automatisé des empreintes digitales (FAED) comptait 1.981.615 empreintes digitales enregistrées et 151.992 traces non identifiées. Ce fichier ne cesse d'être enrichi, puisqu'un décret du 27 mai 2005[3] permet désormais d'y archiver des clichés anthropométriques ainsi que des empreintes et traces palmaires.

Un autre fichier créé en 1998, le fichier automatisé des empreintes génétiques (FAEG), tend à se développer très rapidement. Au 31 décembre 2002, il ne contenait que 2.824 profils génétiques de personnes définitivement condamnées et 179 traces non identifiées. Au 26 mai 2005, 50.000 profils génétiques étaient enregistrés. Ce nombre devrait atteindre plusieurs centaines de milliers d'ici quelques années.

Toutes les polices du monde disposent de fichiers similaires.

Depuis plus de vingt ans, ces technologies se sont étendues au secteur de la sécurité **aux fins de surveillance des sites sensibles et de contrôle des accès.**

c) Un intérêt renouvelé

Le développement et la mondialisation de la fraude à l'identité posent des difficultés inédites. **Les modes traditionnels de preuve de l'identité sont affaiblis.** Comme il a été vu[4], la notion de nom patronymique est de moins en moins pertinente pour s'assurer de l'identité des personnes.

---

[1] *Les théories raciales en furent un autre...*

[2] *Alphonse Bertillon fonda en 1870 le premier laboratoire de police scientifique d'identification criminelle et inventa l'anthropométrie judiciaire. Ce système d'identification reposait sur le relevé d'une vingtaine de mensurations du squelette et de la photographie de face et de côté.*

[3] *Décret n° 2005-585 du 27 mai 2005 modifiant le décret n° 87-249 du 8 avril 1987 relatif au fichier automatisé des empreintes digitales géré par le ministère de l'intérieur.*

[4] *voir supra page 23.*

La biométrie offre a priori des réponses à ce défi :

- d'une part, elle est universelle et immuable, chaque être humain pouvant être identifié de la sorte quelle que soit sa culture et quel que soit son âge[1] ;

- d'autre part, elle garantit l'unicité de la personne en établissant un lien unique entre la donnée biométrique et son porteur, la robustesse de ce lien pouvant résister, à certaines conditions, à la comparaison de plusieurs centaines de millions d'individus entre eux ;

- surtout, les progrès de l'informatique ouvrent de nouvelles possibilités pour son utilisation.

Les qualités précitées de la biométrie sont connues depuis longtemps. C'est ainsi que l'on relève l'empreinte de l'index gauche lors de la délivrance de la carte nationale d'identité sécurisée. Lorsqu'une vérification est nécessaire, l'empreinte est consultable dans le dossier en préfecture. Mais, il ne s'agit alors que d'une sécurité supplémentaire très difficilement exploitable[2].

Le traitement informatisé de la biométrie ouvre la voie à la notion **d'identité biométrique**. Cette identité ne se substituerait pas à l'identité au sens classique. L'état civil resterait la base de l'identité. Mais la biométrie rendrait l'identité indissociable d'un processus technique d'identification.

Toutefois, il ne faut pas confondre identité numérique et identité biométrique. L'identité numérique, c'est-à-dire la numérisation des données relatives à l'identité d'une personne, notamment sur un support comme une puce, peut se concevoir sans biométrie. La biométrie présente des enjeux spécifiques.

2. Des développements nouveaux que la France ne peut ignorer

a) Les exigences internationales et européennes

- *Des contraintes fortes en matière de passeport*

À la suite des attentats du 11 septembre 2001, trois contraintes convergentes imposent désormais à la France la mise en place rapide d'un **passeport biométrique**.

---

[1] *Les éléments biométriques ne sont pas tous parfaitement immuables. Les empreintes digitales peuvent, par exemple, être altérées par l'usage de certains produits ou avec l'âge.*

[2] *voir supra page 35.*

En premier lieu, en application d'un règlement du 13 décembre 2004[1], les Etats membres de l'Union européenne devront, à partir du 28 août 2006, délivrer des passeports incluant une donnée biométrique sur une puce : la photographie faciale. L'introduction d'une seconde donnée biométrique, les empreintes digitales, interviendra dans un délai de 36 mois à compter de l'adoption de spécifications techniques qui ne sont pas encore arrêtées.

En deuxième lieu, la recommandation adoptée le 9 mai 2003 par l'OACI prévoit l'intégration avant 2015 d'au moins une donnée biométrique dans les documents de voyages : la photo numérisée serait obligatoire, mais des données biométriques supplémentaires resteraient optionnelles (empreintes digitales, iris de l'œil).

En dernier lieu, et c'est sans doute la contrainte la plus importante, les États-Unis imposent aux vingt-sept pays[2] qui bénéficient du programme américain d'exemption de visa[3], une échéance précise pour la mise aux normes de l'OACI des passeports. Fixée au 26 octobre 2006, cette échéance est sanctionnée par le rétablissement des visas à l'encontre des ressortissants détenteurs d'un passeport, délivré après cette date, ne comportant pas au minimum une donnée biométrique (la photographie faciale)[4]. **Toutefois, les passeports lisibles en machine délivrés avant cette date continueront d'exempter de la présentation d'un visa.**

L'échéance initiale était le 26 octobre 2004. Le Congrès avait accepté de repousser d'une année ce délai à la demande de l'administration américaine. Lors du déplacement d'une délégation de la mission d'information à Washington, il est apparu qu'un nouveau report de l'échéance devait être demandé au Congrès par le Département d'État et le nouveau ministère de la sécurité du territoire (Department of Homeland Security). L'administration américaine a concédé ne pas être prête pour le 26 octobre 2005 à mettre en œuvre le contrôle aux frontières des passeports biométriques étrangers, ni à faire face à une recrudescence massive des demandes de visas. Toutefois, le Congrès, et en particulier M. James Sensenbrenner, président de la commission judiciaire de la Chambre des représentants, s'était déclaré opposé à un tel report.

---

[1] 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. Publié au JOUE du 29 décembre 2004.

[2] Le Patriot Act du 26 octobre 2001 impose l'introduction d'éléments biométriques dans le passeport des personnes désireuses de se rendre aux Etats-Unis.

[3] Le « visa waiver program », dont l'ensemble des Etats de l'Union européenne à l'exception de la Grèce est membre, dispense de visas les citoyens de ces vingt-sept pays pour les séjours d'une durée inférieure à trois mois. D'ores et déjà, pour en bénéficier, un passeport lisible optiquement en machine (passeport Delphine en France) est impératif.

[4] Les Etats-Unis n'ont décidé que récemment de doter leurs compatriotes de passeports biométriques et de s'imposer de la sorte ce qu'il impose aux autres. Les premières expérimentations devraient être lancées au second semestre 2005 avec les passeports diplomatiques ou de service. Au cours du déplacement d'une délégation de la mission à Washington, il est apparu que cette décision était guidée par un souci de courtoisie et de réciprocité, plus que par des craintes sur la sécurité des passeports américains.

Le 6 juin, le gouvernement américain a annoncé, comme il était pressenti, qu'il acceptait de repousser au 26 octobre 2006 la date butoir. Toutefois, il réclame qu'au 26 octobre 2005, les voyageurs des vingt-sept pays concernés présentent des passeports avec des photographies numérisées et que les autorités de ces pays présentent un plan acceptable pour commencer à émettre les passeports biométriques à puce dans un an.

À l'heure actuelle, seules l'Autriche, la Slovénie et la Belgique délivrent des passeports répondant à ces normes.

In fine, la France devra se doter :

- d'un passeport comportant la photographie faciale numérisée au plus tard le 28 août 2006 ;

- d'un passeport incluant une seconde donnée biométrique (les empreintes digitales) à moyen terme.

Toutefois, aucune autre obligation ne s'impose. Les règles de consultation des données stockées sur le passeport ainsi que l'opportunité de la création d'un fichier central des données biométriques relèvent de l'appréciation de chaque Etat.

- *Des solutions harmonisées au niveau européen*

Le Conseil européen de Thessalonique de juin 2003 a affirmé la nécessité de dégager au sein de l'Union une approche cohérente en ce qui concerne les identificateurs ou les données biométriques utilisés. Une telle approche doit également prévaloir pour la détermination des spécifications techniques des systèmes de manière à assurer leur interopérabilité. Cette approche a été appliquée aux passeports, aux titres de séjour des ressortissants de pays tiers et aux visas.

Concernant les titres de séjour, le Conseil « justice et affaires intérieures »est parvenu à un accord sur la proposition de règlement du Conseil modifiant le règlement du 13 juin 2002 établissant un modèle uniforme de titre de séjour pour les ressortissants de pays tiers. Il prévoit le stockage obligatoire de la photographie de face et de deux empreintes digitales[1].

Concernant les visas, le déploiement du nouveau système d'information sur les visas (SIV II ou VIS II) en remplacement du système actuel a pour objet l'intégration des éléments biométriques sur les visas et la constitution d'un fichier central des demandes de visas Schengen. A nouveau,

---

[1] *La proposition de règlement (document COM (2003)558 final) doit encore être soumise à la consultation du Parlement européen.*

le choix s'est porté sur la photographie de face et deux empreintes digitales[1]. A cet égard, la France expérimente pour l'Union européenne ce nouveau modèle de visa avant qu'il ne soit généralisé à l'ensemble de l'espace Schengen.

Enfin, en vigueur depuis le 15 janvier 2003, **Eurodac** est un système européen de contrôle et de comparaison des empreintes digitales des demandeurs d'asile et des étrangers susceptibles de le devenir un jour. Les Etats membres prennent en effet les empreintes digitales des étrangers de plus de quatorze ans ayant déposé une demande d'asile, franchi irrégulièrement une frontière de l'Union ou se trouvant illégalement sur le territoire de l'un des Etats membres. Il s'agit d'éviter qu'un demandeur d'asile ne présente des demandes multiples dans plusieurs Etats parties. Ce système prévu par le règlement (CE) n° 2725/2000 du Conseil du 11 décembre 2000 concernant la création du système « Eurodac » doit en effet permettre l'application efficace de la convention relative à la détermination de l'Etat responsable de l'examen d'une demande d'asile présentée dans l'un des Etats membres par un ressortissant d'un pays tiers signée à Dublin le 15 juin 1990 (dite « Convention de Dublin »). Cette convention a été récemment remplacée par le règlement (CE) n° 343/2003 du Conseil du 18 février 2003 dénommé aussi « règlement Dublin II ».

Par ailleurs, la prochaine version du système d'information Schengen appelée SIS II intègrera des données biométriques et en premier lieu des empreintes digitales[2]. Ce projet est développé conjointement avec le projet VIS II.

b) Un foisonnement d'expériences et de projets à l'étranger

Outre la mise aux normes des passeports et la préparation du passage à des titres de séjour et des visas biométriques, plusieurs de nos partenaires européens travaillent à des projets strictement nationaux relatifs à une carte d'identité biométrique[3]. En effet, beaucoup développent une nouvelle génération de titres d'identité électroniques ou envisagent de le faire comme l'illustre le tableau ci-après. Chaque pays conserve ses spécificités selon son histoire et les objectifs qu'il assigne à cette carte.

---

[1] Voir la proposition de règlement du Conseil modifiant le règlement (CE) n° 1683/95 établissant un modèle type de visa.

[2] Proposition de règlement du Parlement européen et du Conseil sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen de deuxième génération (SIS II). Document COM (2005) 236 final présentée par la Commission européenne le 31 mai 2005.

[3] L'Union européenne n'a pas encore proposé l'harmonisation des cartes d'identité. Un groupe de travail a toutefois été constitué. À moyen terme, la carte d'identité valant titre de voyage dans l'Union européenne, une harmonisation semble probable.

Les projets de carte d'identité biométrique en Europe

	Etat d'avancement du projet	Éléments biométriques insérés dans la puce	Existence d'un fichier central
Italie	En cours de délivrance depuis juillet 2002	Empreintes digitales	Non
Espagne	Loi de 2004 Délivrance dès 2006	Empreintes digitales + photographie	
Pays-Bas	A l'étude[1] Objectif : 2007	- photographie faciale - empreintes digitales	Projet de création d'un numéro d'identification unique
Royaume-Uni	Projet de loi en cours d'examen à la Chambre des communes	- empreintes digitales - photographie - peut-être l'iris	Création d'un registre national d'identité intégrant les données numériques
Allemagne	Loi fédérale du 2 janvier 2002 autorise l'insertion de données biométriques	À définir[2]	Non
Suède	A l'étude		
Autriche	A l'étude[3]		
Estonie	A l'étude[4] Objectif : second semestre 2006	- empreintes digitales - autres	

[1] Depuis octobre 2002, tous les documents d'identité émis par les Pays-Bas ont un emplacement prévu pour de futures données biométriques stockées sur une puce.

[2] A ce jour, aucun projet de loi n'a été déposé pour définir les éléments biométriques utilisés. La loi du 9 janvier 2002 prévoit que ces données ne pourraient être utilisées que pour contrôler l'authenticité du document et prouver l'identité du titulaire.

[3] La carte en vigueur a été conçue pour intégrer ultérieurement une puce électronique supportant des données biométriques.

[4] Depuis janvier 2002, une carte d'identité électronique et non biométrique est délivrée aux Estoniens et aux étrangers qui en font la demande.

L'exemple britannique est le plus significatif. La carte nationale d'identité n'y a été introduite qu'à deux reprises au cours de l'histoire du pays lors des deux guerres mondiales. Traditionnellement perçue comme une atteinte aux libertés individuelles, elle pourrait cependant être prochainement rendue obligatoire, payante et biométrique. En outre, un registre national d'identité contenant de nombreuses informations sur toutes les personnes

résidant au Royaume-Uni âgées de plus de seize ans et incluant des données biométriques serait constitué. Un projet de loi a été redéposé devant le parlement britannique après les élections législatives de mai 2005.

Cette véritable révolution témoigne de la nouvelle sensibilité des gouvernements européens au problème de la fraude à l'identité et de ses conséquences sur le fonctionnement sur nos sociétés.

c) Un enjeu incontournable pour la France

Ce contexte international et européen contraint la France à réfléchir à la place de la biométrie et à son utilisation.

En premier lieu, il lui faut satisfaire à ses engagements internationaux et aux demandes américaines qui valent de fait normes communes.

Le passeport biométrique devra être délivré dans un an environ. Toutefois, le débat a encore sa place, chaque État étant libre par exemple de créer ou non un fichier central des données biométriques.

En deuxième lieu, la France a anticipé le recours à la biométrie en matière de visa et de titre de séjour au niveau européen. En effet, **la loi du 26 novembre 2003 relative à la maîtrise de l'immigration prévoit que les empreintes digitales et la photographie des demandeurs de visa peuvent être relevées et faire l'objet d'un traitement automatisé. Lorsque le visa est accordé, le relevé est obligatoire**. Cette disposition s'ajoute à une autre, plus ancienne, introduite par la **loi du 24 avril 1997** dite « loi Debré » et qui **permet le relevé des empreintes digitales des ressortissants étrangers** qui **sollicitent** la **délivrance d'un titre de séjour**, **sont en situation irrégulière** en France ou **font l'objet d'une mesure d'éloignement** du territoire français[1]. La loi du 11 mai 1998 dite « loi Chevènement » ne l'a pas remise en cause.

Toutefois, ces dispositions, bien que discutées au Parlement, n'ont pas été précédées d'un débat général sur la biométrie et les conditions de son utilisation. Il est significatif que la loi du 24 avril 1997 précitée n'ait toujours pas été mise en oeuvre et que le relevé des empreintes digitales des demandeurs de visas voté en novembre 2003 fasse l'objet d'une expérimentation[2] lancée au début de l'année 2005 seulement. L'utilisation de la biométrie est complexe et ne peut s'improviser.

---

[1] Ces dispositions ont été codifiées aux articles L. 611-3 à L. 611-7 du code de l'entrée et du séjour des étrangers et du droit d'asile.

[2] 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 des données à caractère personnel relatives aux ressortissants étrangers sollicitant la délivrance d'un visa

En outre, ces dispositions doivent être coordonnées avec le projet européen VIS II en cours de discussion. C'est la raison pour laquelle l'expérimentation en matière de visa a été mise en place en coopération avec la Commission européenne et d'autres Etats membres[1]. Financée sur des fonds communautaires, la mission BIODEV (BIOmétrie des DEmandeurs de Visas) a débuté la production de visas biométriques le 22 mars 2005 au consulat général de France à Bamako. Au total, une dizaine de consulats devraient délivrer progressivement 50.000 visas biométriques. Les données biométriques (la photographie et les dix empreintes digitales) sont enregistrées dans un fichier central et dans une carte à puce insérée dans une pochette plastique collée en page de couverture du passeport. Cela permet un double contrôle aux frontières en confrontant les empreintes du porteur du visa aux empreintes insérées dans la puce et au fichier central. Cette expérimentation doit permettre de mieux cerner les difficultés technologiques, administratives, économiques et sociologiques qu'implique le déploiement d'un système biométrique visant des dizaines de millions de personnes réparties sur l'ensemble de la planète.

Votre mission remarque incidemment que l'application de la biométrie aux étrangers ne soulève pas les mêmes débats et oppositions que ceux de ces derniers mois lorsqu'il s'agit d'appliquer la biométrie à des citoyens français. Pourtant, les enjeux éthiques ou moraux sont similaires, en dépit de notre tradition juridique qui permet d'assujettir les étrangers à une législation spécifique pour des raisons de police.

En troisième lieu, **les nombreux projets nationaux de carte d'identité biométrique en Europe ne peuvent manquer d'avoir un impact sur les réflexions françaises.** D'une part, la Commission européenne a reçu mandat, dans le cadre du programme de La Haye[2], de contribuer à l'élaboration d'une norme minimale en terme de sécurisation des titres d'identité délivrés par les Etats membres par référence aux normes de l'OACI. Cette position, défendue par la France, le Royaume-Uni, l'Espagne et l'Allemagne, se justifie par le fait que la carte d'identité est reconnue comme document de voyage au sein de l'Union européenne. Dès lors, il ne peut y avoir un pays « maillon faible ». D'autre part, la biométrie étant déjà utilisée ou étant sur le point de l'être comme élément d'identification des demandeurs d'asile ainsi que sur tous les documents de voyage (passeport, visa) ou de séjour, pourquoi l'exclure complètement pour la seule carte nationale d'identité ? Plus que tout autre document, la carte nationale d'identité atteste de l'identité d'une personne. En outre, un déploiement coordonné de la biométrie permettrait de mutualiser les coûts.

---

[1] *Etats participants : la France (chef de file), la Belgique (elle co-expérimente en délivrant des visas biométriques dans plusieurs de ses consulats), l'Allemagne, la Hongrie, l'Italie, les Pays-Bas et la Pologne.*

[2] *Réunion du Conseil européen du 4 novembre 2004.*

En dernier lieu, **l'enjeu industriel pèse sur ce débat.** Plusieurs entreprises françaises détiennent ensemble plus de la moitié du marché mondial de la biométrie qui est en pleine expansion. Mais cette domination est menacée par l'émergence de nouveaux concurrents en Asie et aux États-Unis. Aux yeux des industriels, il pourrait sembler paradoxal que la France ne se dote pas d'un système performant d'identification biométrique. Le parallèle peut être fait avec la carte bancaire à puce. Nos entreprises sont les premières sur ce marché et la France est le pays où le paiement par carte bancaire est le plus développé et le plus sûr.

d) Le projet INES

Le projet INES fait le choix d'un usage intensif de la biométrie pour garantir l'identité des personnes.

Au mois de mars 2005, le ministère de l'intérieur envisageait :

- de **fusionner les procédures de délivrance du passeport et de la carte nationale d'identité**, afin de réduire les coûts de production de ces documents et de simplifier les démarches administratives des citoyens ;

- d'**équiper la carte nationale d'identité et le passeport d'une puce électronique** contenant des **données relatives à l'état civil** et des **identifiants biométriques**, la photographie et les empreintes digitales[1].

La même démarche de sécurisation du titre en recourant à la biométrie pourrait être étendue par la suite au permis de conduire.

L'ensemble de ce système reposerait sur la **création d'une base centrale constituée de plusieurs fichiers**. Cette segmentation doit garantir un accès proportionné aux données contenues dans la base. Tous les usages de cette base ne nécessiteraient pas d'accéder aux mêmes types de données personnelles et, a fortiori, à l'ensemble des données.

Celle-ci contiendrait :

- un **fichier des six empreintes digitales** recueillies lors de la demande initiale de titre, destinée à éviter la délivrance de titres sous plusieurs identités à une même personne ou sous une même identité à plusieurs personnes ;

- un **fichier des photographies** ;

- un **fichier de gestion** des titres avec l'identité, proche du fichier de gestion existant pour la carte nationale d'identité sécurisée ;

---

[1] *Pour le passeport, seule la photographie serait dans un premier temps insérée, puis les empreintes digitales en application du règlement du Conseil du 13 décembre 2004.*

- le **fichier des archives** contenant les justificatifs scannés présentés lors du dépôt de la demande de titre.

Ces fichiers seraient reliés par un numéro de liaison technique.

3. Des systèmes biométriques différents selon le niveau de sécurité recherché

Un double constat s'impose : la biométrie s'étend rapidement ; il existe une multitude de systèmes biométriques différents répondant à autant de problématiques et d'objectifs.

La technologie permet à peu près tout, comme l'a affirmé M. Bernard Didier, directeur du développement de la SAGEM. Le panel proposé par les industriels offre une gamme très large de solutions techniques.

Du point de vue de la sécurité, les **questions essentielles avant de créer un titre d'identité biométrique** sont : quel degré de sécurité veut-on atteindre ? Quel type de fraude faut-il éliminer ? Quels autres usages de la biométrie veut-on permettre ou ne pas permettre ? Quelle est la taille de la population concernée ?

En fonction des réponses apportées à ces questions, il est possible de construire un système d'identité biométrique dont l'architecture réponde précisément au cahier des charges.

Toutefois, **quelques grands modèles**[1] peuvent être distingués selon le niveau de sécurisation de l'identité qu'ils garantissent. Ils sont présentés ci-après selon le niveau de sécurité croissant qu'ils sont censés apporter.

Les difficultés que ces modèles peuvent poser au regard des libertés seront présentées séparément.

Les modèles utilisant un fichier central, c'est-à-dire tous à l'exception du premier, sont supposés conçus de la façon suivante. L'approche technique qui permet une très grande flexibilité et un contrôle des usages consiste à répartir les données en deux bases distinctes : une base d'identité qui décrit pour chaque numéro d'identité l'ensemble des attributs retenus (nom, prénom...), une base de données biométriques dont chaque enregistrement est composé d'un numéro biométrique unique suivi des données biométriques proprement dites. Les numéros d'identité et les numéros biométriques permettent d'établir des liens entre l'identité d'une personne et ses données biométriques. Afin d'assurer le contrôle de l'usage, ces liens sont cryptés, les liens de décryptage pouvant être bidirectionnels, unidirectionnels, faibles ou inexistants.

---

[1] *M. Bernard Didier, directeur du développement à la SAGEM, a présenté à la mission plusieurs systèmes biométriques. Certains d'entre eux, et notamment le modèle dit à « lien faible » présenté ci-après, ont été brevetés par cette société.*

L'existence d'un fichier central présente un intérêt majeur pour la sécurisation de l'identité : elle assure **l'unicité de l'identité**. Cela signifie qu'un individu n'a qu'une seule identité et qu'une identité n'est utilisée que par un individu. Les usurpations et vols d'identité sont théoriquement impossibles.

a) La biométrie pour authentifier

Traditionnellement, un titre d'identité associe une photographie et un nom. Il permet au porteur du titre de **prouver son identité**. On parle alors d'« **authentification** », c'est-à-dire d'une **recherche dite « un contre un »**.

Avec un titre classique ou un titre électronique sans biométrie, il existe deux niveaux de vérifications : examen visuel et contrôle des sécurités du titre puis, si nécessaire, consultation du fichier de gestion de la carte nationale d'identité pour s'assurer que ce titre a bien été délivré par les autorités habilitées.

Trois solutions intégrant la biométrie permettent d'améliorer la qualité de l'authentification.

- *Une carte à puce biométrique sans fichier central*

Les données biométriques ne figurent que sur la puce. Cela permet un troisième niveau de sécurité en authentifiant le porteur par comparaison avec les données biométriques contenues dans la puce.

Si seule la photographie est dans la puce, le gain en sécurité est assez faible par rapport à ce que permet un titre classique ou un titre électronique sans biométrie sur lequel figure déjà la photographie.

Si les empreintes digitales ou une autre donnée biométrique performante **figurent sur la puce**, le **gain en sécurité est meilleur**. A la différence de la photographie, le « look like » c'est-à-dire l'utilisation de la carte d'un tiers, complice ou non, ressemblant physiquement à la personne usurpant l'identité, devient impossible.

Toutefois, **cette utilisation de la biométrie ne permet pas d'assurer l'unicité de l'identité lors de la délivrance du titre**.

- *Une carte à puce biométrique avec un fichier central unidirectionnel dans le sens identité vers biométrie*

Avec ce modèle, **il est possible, à partir de l'identité d'une personne, de retrouver ses données biométriques. Toutefois, l'inverse n'est pas possible**. Ainsi, la connaissance de l'identité d'une personne permet d'accéder à sa donnée biométrique et de procéder, si nécessaire, à son authentification.

Par rapport au modèle précédent sans fichier, ce modèle présente un **triple avantage** :

- **si la carte à puce est muette** (titre imité ou altéré), **on peut vérifier l'identité du porteur** en sélectionnant son identité dans la base, puis en comparant ses données biométriques avec celles contenues dans la base biométrique correspondant à l'identité affichée ;

- le **renouvellement d'une carte est simplifié et sécurisé**. On sélectionne par l'identité pour obtenir une caractéristique biométrique que l'on compare à celle du porteur ;

- l'**unicité de l'identité est assurée** à l'occasion de la délivrance du titre. En effet, si l'individu a un titre sous une autre identité, ses données biométriques auront déjà été enregistrées dans la base de données et le système s'en apercevra. Certes, il n'est pas possible de savoir quelle est cette autre identité. Mais, cela suffit à détecter une tentative d'usurpation d'identité.

- *Une carte à puce biométrique avec un fichier central dit à « liens faibles »*

Dans la situation précédente, les liens entre les deux bases étaient construits de telle sorte qu'à chaque enregistrement d'identité ne correspondait qu'une seule donnée biométrique. Le nombre de liens est équivalent au nombre de personnes que l'on souhaite gérer. Par exemple, si le système gère dix millions de personnes, il faut dix millions de liens de valeurs différentes, composés de huit chiffres, entre la biométrie et l'identité.

Supposons, maintenant que l'on réduise, pour cette même population, les valeurs de lien de huit chiffres à deux chiffres en gardant par exemple les deux derniers chiffres. Il y a alors cent mille entrées correspondant à chaque valeur de lien. **Il n'est alors plus possible de connaître la donnée biométrique d'une personne à partir de son identité**[1] **; de même, l'identification d'une personne à partir d'une donnée biométrique n'est pas possible**.

Toutefois, ce système original breveté par la SAGEM permet d'assurer **l'unicité de l'identité tout en garantissant l'anonymat**. En effet, la vérification biométrique est possible de la façon suivante : il faut sélectionner par l'identité et obtenir une première valeur du lien, puis sélectionner par la biométrie pour obtenir une seconde valeur du lien. Si les deux valeurs sont identiques, la probabilité que l'association identité-biométrie soit correcte est de 99 %. Ce chiffre de 99 % est donné à titre d'exemple. La probabilité pourrait être de 99,9 %, si les valeurs de lien comportaient trois chiffres au lieu de deux. Dans tous les cas, la probabilité est suffisamment grande pour

---

[1] *Dans cet exemple, si l'on souhaite comparer une empreinte digitale avec celles contenues dans la base, 100.000 empreintes correspondant à 100.000 individus seront sélectionnées.*

offrir une assurance quasi-complète sur l'unicité de l'identité et pour dissuader les fraudeurs. En effet, un fraudeur qui tenterait d'usurper une identité aurait une chance sur cent ou sur mille que ses données biométriques se soient vues attribuer la même valeur de lien que celle attribuée aux données biométriques de la personne dont il tente d'usurper l'identité[1].

b) La biométrie pour identifier

Les deux modèles précédents empêchent ou rendent très difficile l'utilisation des données pour d'autres fins que celles pour lesquelles elles ont été collectées.

Les exemples de modèle suivants ne présentent pas la même garantie. Ils permettent d'**identifier et non plus seulement d'authentifier**. A la différence de l'authentification qui consiste à comparer les données biométriques de la personne avec celles contenues sur la puce ou dans la base et supposées être les siennes (recherche dite « un contre un »), **l'identification consiste à comparer des données biométriques anonymes avec celles contenues dans la base afin de retrouver l'identité de la personne (recherche dite « un contre n »)**.

Les systèmes d'identification assurent l'**unicité de l'identité** comme les deux précédents systèmes d'authentification. Mais ils permettent d'**autres utilisations**, **étrangères à la simple gestion de la délivrance d'un titre d'identité.**

Un exemple de système de ce type est un **système où le lien est bidirectionnel** entre la base des données d'identité et la base des données biométriques. **On peut retrouver l'identité à partir de la biométrie et inversement. Un système d'identification encore plus abouti consiste en une seule base regroupant toutes les données sans lien crypté entre les différentes données**.

Cette fonctionnalité d'identification peut permettre :

- d'identifier un amnésique, un enfant fugueur ou retrouvé, des personnes désorientées (fous, maladie d'Alzheimer), des cadavres, notamment en cas de catastrophe naturelle majeure ;

- d'identifier une personne ayant commis une infraction et refusant de donner son identité ;

- d'identifier une personne à partir de traces retrouvées sur une scène de crime[2].

---

[1] Une technique de fraude pourrait consister à usurper l'identité d'une personne dont on connaît la valeur de lien. Si le fraudeur a la même valeur de lien, il peut passer le test. Ce système requiert donc que la valeur des liens reste secrète.

[2] Cela exige que les données biométriques utilisées dans la base soient des données qui laissent des traces, comme les empreintes digitales ou l'ADN. En revanche, l'iris ou la photographie ne permet pas une telle utilisation du fichier.

c) Une sécurisation de l'identité accrue

Tous ces systèmes biométriques, à l'exception du système sans fichier central, procurent une sécurité importante. Ils éliminent l'usurpation d'identité et peuvent justifier a priori le coût supplémentaire lié à la biométrie.

En effet, au regard des seuls critères de la protection de l'identité des personnes et du coût de la fraude à l'identité, un système biométrique ne vaut la peine que s'il représente un réel saut qualitatif et quantitatif.

Le tableau ci-après récapitule les possibilités offertes par ces différents systèmes. Rappelons qu'il ne s'agit que de modèles types, des perfectionnements ou tempéraments pouvant être apportés à chacun d'eux.

Le **seul point faible** de ces systèmes biométriques se situe **au moment de la délivrance du premier titre biométrique.**

A ce stade, les données biométriques du fraudeur ne sont pas encore dans le fichier. Il pourrait alors usurper l'identité d'une personne qui ne se serait pas vu délivrer, elle aussi, un premier titre biométrique ou créer une identité fictive. Le fraudeur usurperait de la sorte l'identité de la personne et substituerait ses données biométriques.

Toutefois, il apparaît à votre rapporteur qu'un tel **risque** est **limité**.

En effet, le **fraudeur en usurpant cette identité l'usurpe définitivement**. Il ne peut plus en changer. L'intérêt d'une telle manoeuvre est donc réduit. En outre, elle **risque d'attirer l'attention sur lui**.

Lorsque la personne dont l'identité a été usurpée désirera se faire délivrer un titre, le système détectera la fraude. Après enquête approfondie, il apparaîtra que le premier titre délivré l'a été indûment et l'identité usurpée sera restituée à son titulaire légitime.

Ces arguments peuvent suffire à dissuader les tentatives de fraude.

	Modèle 1 Lien unidirectionnel ID[68] vers BIO[69]	**Modèle 2 Lien faible**	**Modèle 3 Lien bidirectionnel ID vers BIO**	**Pour mémoire : absence de lien**
Association ID-Bio	ID vers BIO	Oui, à 99 %	Oui	Non
Gestion de l'association	Fonction cryptographique à sens unique	Lien faible	Fonction cryptographique sous contrôle	Aucune
Entrée = ID Sortie = Bio	Oui	Non (100.000 candidats proposés)	Oui	Non
Entrée = Bio Sortie = ID	Non	Non (100.000 candidats proposés)	Oui	Non
Unicité	Oui	Oui	Oui	Oui
Renouvellement	Facile par authentification	Plus lourde par identification	Facile	Non sûr
Suppression (Décès)	Facile par l'identité	Seulement si l'on détient les données biométriques et l'identité	Oui	Seulement si l'on détient les données biométriques et l'identité
Authentification sur carte illisible	Oui	Par identification sur une base restreinte	Oui	Non
Identification (victimes, amnésiques, criminels)	Non	Non	Oui	Non
Destruction de l'ensemble des liens invasion	Oui (par destruction des fonctions cryptographiques)	Par suppression des liens faibles	Oui (par destruction des fonctions cryptographiques)	N'existe pas
Contrôle possible par une autorité	Oui	Sans objet	Oui	Non
Possibilité de rétablir les liens en clair	Oui	Non Choix irrévocable	Oui	Non Choix irrévocable
Maturité industrielle	Prouvée	Inexistante	Prouvée	Non pertinent

Source : M. Bernard Didier, directeur du développement de la SAGEM

[68] *ID : identité.*
[69] *BIO : données biométriques.*

4. Les précautions nécessaires à une mise en place réussie d'un titre d'identité biométrique

Quel que soit le système biométrique retenu, certaines conditions sont indispensables à une mise en œuvre efficace et réussie d'un titre biométrique.

a) Ne pas surestimer la fiabilité de la biométrie

Nos sociétés ont depuis quelques années un fort besoin d'identification. Or, la biométrie est la seule technologie permettant l'identification de personnes parmi des masses humaines de plusieurs dizaines, voire centaines de millions d'individu.

Ce constat ne doit pas faire oublier que cet outil puissant et unique a également ses limites comme l'a indiqué Mme Bernadette Dorizzi, chercheur à l'Institut national des télécommunications, devant les membres de la mission.

Il ne s'agit pas là de remettre en cause la fiabilité de la biométrie. M. Christian Cabal, député, constatait et mettait en garde contre les excès de confiance et de défiance à l'égard de la biométrie dans un rapport[70] de juin 2003 sur les méthodes d'identification par la biométrie : « *Une analyse objective des performances techniques des systèmes biométriques et de leurs faiblesses éventuelles se heurte à diverses difficultés. D'une part, il est malaisé d'isoler dans les systèmes biométriques les défaillances imputables aux dispositifs eux-mêmes de celles liées à l'environnement technique, physique, voire juridique dans lequel ils sont implantés. D'autre part, la diversité des techniques biométriques [...] rend les analyses plus compliquées encore.* »

Toutefois, ce rapport estimait que certaines techniques biométriques, notamment les empreintes digitales, avaient acquis ou étaient sur le point d'acquérir une maturité satisfaisante et pouvaient servir d'identifiant pour des populations de plusieurs millions de personnes.

M. Christian Cabal, lors de son audition par la mission, a fait état des **progrès importants de ces technologies** depuis deux ans. Concédant, comme il le faisait déjà dans son rapport, qu'aucune technique ne pouvait se prétendre infaillible et apporter la preuve d'une performance à 100 %, il a, néanmoins, déclaré que l'utilisation de la biométrie à des fins d'authentification ou d'identification de groupes humains de plusieurs dizaines de millions d'individus était fiable.

---

[70] *Rapport n° 355(Sénat) ou n° 938 (Assemblée nationale)(2002-2003) de l'Office parlementaire d'évaluation des choix scientifiques et technologiques.*

M. Philippe Wolf, responsable du centre de formation de la direction centrale de la sécurité des systèmes d'information qui est placée sous l'autorité directe du Premier ministre, a toutefois douté de la maturité des technologies biométriques, soulignant le et d'études sérieuses et indépendantes. En outre, il a estimé que la meilleure sécurité informatique restait l'utilisation d'un code secret révocable. Or, les données biométriques ne sont ni secrètes, ni révocables. Il a conclu son propos en soulignant qu'il ne fallait pas abandonner complètement des systèmes traditionnels ayant fait leur preuve au profit de systèmes nouveaux encore mal connus.

Les premières expériences à grande échelle de la biométrie, notamment le programme US-Visit aux États-Unis, **semblent devoir valider la fiabilité de ces technologies**.

- *Ne pas abandonner les sécurités traditionnelles*

La sécurité ne doit pas reposer sur la seule biométrie. Selon M. Pierre Garcia, capitaine à la direction centrale de la police aux frontières, un système d'identité doit prévoir plusieurs degrés de contrôles : examen visuel (premier niveau), utilisation d'appareils pour tester les sécurités cachées ou lire la puce (deuxième niveau), consultation du fichier de gestion (troisième niveau).

Un titre biométrique doit donc **conserver les sécurités traditionnelles permettant une première authentification du titre en l'absence de l'équipement nécessaire à l'exploitation de la biométrie**. Comme on l'a vu, l'expérience de la carte nationale d'identité sécurisée nous enseigne que les lecteurs de certains éléments de sécurité, comme le luminophore, n'ont jamais été distribués à la police et à la gendarmerie

Ces sécurités forment aussi un filet indispensable en cas de panne du système biométrique.

- *Utiliser au moins deux éléments biométriques*

Appliqué à des populations de plusieurs dizaines de millions d'individus, **un système biométrique** doit prendre en compte ses propres faiblesses dès sa conception. Il **doit être souple et capable de traiter la différence**.

En effet, les études scientifiques et les premiers retours d'expérience à grande échelle évaluent à 2-3 % la fraction d'une population inadaptée à l'utilisation d'un type de données biométriques. Dans le cas des empreintes digitales, il peut s'agir de personnes aux mains coupées, ayant travaillé le ciment ou ayant eu les doigts attaqués par des acides. Dans le cas de l'iris, certaines maladies en troublent la lecture.

En outre, **sur de grandes populations**, les **risques d'erreur sont statistiquement accrus**. La probabilité que deux signatures biométriques soient identiques ou soient si proches que le traitement informatique les confonde est plus importante. En théorie, ce risque met à mal le principe d'unicité qui relie un individu à une donnée biométrique. En pratique, ce problème peut être réglé, la probabilité variant selon la technique utilisée. Ainsi, pour dix points de comparaison, la probabilité de trouver les mêmes points disposés de façon identique sur les empreintes digitales de deux personnes différentes serait d'une chance sur un million et, pour quatorze à dix-sept points, d'une chance sur dix-sept milliards.

Pour ces différentes raisons, **l'utilisation d'au moins deux données biométriques semble nécessaire,** le visage et les empreintes digitales, constituent un bon compromis. Ce choix permet de couvrir l'ensemble de la population et de réduire considérablement les erreurs du système (fausse reconnaissance ou faux rejet). Il convient également d'enrôler les empreintes digitales de plusieurs doigts afin de réduire la probabilité que deux personnes présentent des signatures biométriques très proches.

Lors de son déplacement à Washington, la délégation de la mission a constaté que les autorités américaines, dans le cadre du programme US-Visit, envisageaient d'accroître prochainement le nombre d'empreintes digitales relevées au moment de l'entrée sur le territoire américain. A l'heure actuelle, seuls les index droit et gauche sont enrôlés. Or, la population enregistrée dans la base de données croît très rapidement et comptera à terme plusieurs dizaines ou centaines de millions de personnes. Le Department of Homeland Security devrait rapidement passer à six empreintes.

- *Maintenir une présence humaine*

Pour un système biométrique, le maintien d'une présence humaine est indispensable même s'il est aussi une source de dysfonctionnement.

Il est indispensable car **un système biométrique ne peut pas bien fonctionner s'il est abandonné à lui-même**. Le tout technologique n'est pas fiable.

Ainsi, **lors de la phase cruciale[71] d'enrôlement des données** biométriques, une présence humaine est nécessaire afin de s'assurer, par exemple, que ce sont les bons doigts qui sont enregistrés. Elle permet également de lutter contre les tentatives de fraude. Bien que les capteurs les plus récents détectent les faux doigts ou les doigts morts, il faut rester prudent face à l'imagination des fraudeurs. Une présence humaine avertie doit détecter et dissuader les tentatives de contournement du système.

---

[71] De la qualité de l'enrôlement dépend la performance du processus d'authentification et d'identification. A défaut, les risques d'erreur se multiplient.

Une présence humaine est encore nécessaire **pour gérer la différence**, notamment pour traiter le cas des personnes dont les caractéristiques ne peuvent être relevées (doigts coupés, maladie de l'œil, borgnes...).

Enfin, elle doit servir **à réguler le système en cas d'erreur** (faux rejets, non reconnaissance).

Cet aspect humain est **fondamental pour l'acceptabilité de la biométrie**. **Les usagers ne doivent pas se trouver seuls face à une machine**. Selon Mme Bernadette Dorizzi, chercheur à l'Institut national des télécommunications, les premières études sociologiques et psychologiques réalisées sur des populations en situation réelle démontrent la bonne perception a priori de ces systèmes. Toutefois, des réactions de panique peuvent naître lorsqu'une personne se trouve seule face à une machine qui lui refuse un accès ou un droit. Le rejet doit donc toujours être décidé par une personne et non par la machine seule.

Indispensable, la présence humaine est aussi source de dysfonctionnement. Cela implique **d'apporter un soin particulier à la formation des agents**. Seuls des personnels spécialement formés doivent manipuler et surveiller les appareils biométriques. Ce principe est lourd en terme de gestion administrative et des ressources humaines, mais il ne doit pas souffrir d'exception.

Enfin, pour bien fonctionner, un système biométrique doit être favorablement perçu par les personnes qui s'y soumettent. D'une part, **un effort d'information et de transparence doit être entrepris** afin de dissiper les craintes infondées. D'autre part, le système doit être le plus simple et le moins intrusif possible pour l'usager.

b) Une durée de validité des titres d'identité réduite à cinq ans

Les titres en vigueur (carte nationale d'identité et passeport) ont une durée de validité de dix ans. Cette durée, déjà très longue pour des titres traditionnels, ne convient pas pour des titres d'identité électroniques et biométriques.

Les experts rencontrés lors des déplacements de la mission au Centre national de production des titres et en Belgique ont souligné **la fragilité de la cryptographie au delà d'une période de cinq ans.** La résistance aux attaques extérieures ne peut pas être assurée au delà. Ceci a encore été confirmé par M. Jean-Pierre Buthion, responsable « produits et services » du Groupement des cartes bancaires, et les industriels du secteur. L'exemple des cartes bancaires en témoigne, puisqu'elles sont renouvelées tous les deux ans afin de maintenir un niveau optimal de sécurité.

De plus, **l'usure de la puce** (rayure, décollement, oxydation...) exige également un renouvellement régulier.

Enfin, **les données biométriques des individus peuvent exceptionnellement évoluer** en raison de l'âge, de maladies ou d'accident. Un renouvellement tous les cinq ans permettrait de mieux prendre en compte ces évolutions.

c) Un titre obligatoire ?

Cette question déjà abordée à propos des titres classiques se pose de manière différente pour les titres biométriques.

Lorsque le système biométrique retenu est un système d'identification permettant d'autres usages que la simple sécurisation de la délivrance des titres (police judiciaire, contrôle d'identité...), la performance de ces systèmes repose essentiellement sur l'existence d'un fichier central et la possibilité de comparer une donnée biométrique avec l'ensemble des données de la base. En conséquence, **la performance est réduite si une grande partie de la population reste en dehors de la base**. Le rapport coût-avantage n'est plus aussi favorable.

Toutefois, il n'y a pas d'automaticité entre un **titre** biométrique et un titre obligatoire.

Ainsi, les **systèmes dits d'authentification avec ou sans fichier central n'impliquent pas un titre obligatoire**. Le libre choix peut être laissé à chaque individu de se prémunir ou non contre une usurpation d'identité.

d) Une nouvelle répartition des compétences entre les communes

A ce jour, les quelque 36.000 communes de France sont le lieu de dépôt et de retrait des demandes de titres. Les agents vérifient que le dossier papier est complet avant de la transmettre à la sous-préfecture qui assure le contrôle qualitatif des dossiers.

Avec le passage à un titre biométrique, le maintien de la possibilité de déposer une demande dans chacune des 36.000 communes poserait des difficultés techniques et financières. En effet, lors de cette phase, il est nécessaire de relever les données biométriques de la personne.

Financièrement, le coût serait élevé : achat des capteurs, équipement informatique, déploiement du réseau...

Techniquement, l'efficacité et la sécurité du système seraient moins fortes. La formation des agents en charge du système doit être irréprochable afin que la qualité des données biométriques enregistrées soit la meilleure. Des

agents formés spécialement seraient également plus aptes à détecter les tentatives de fraude. La production d'un titre d'identité est d'autant plus sûre qu'elle est relativement centralisée.

Dans le cadre du projet INES, il est envisagé d'équiper au moins 340 sites, soit un par arrondissement, le nombre de sites pouvant évidemment être supérieur dans les agglomérations importantes[72].

Les communes choisies[73] pourraient être les communes chefs-lieux d'arrondissement ou les communes sièges des établissements publics de coopération intercommunale à fiscalité propre d'une taille suffisante. Toutefois, une autre possibilité serait de rendre l'ensemble de cette compétence à l'État en la confiant aux sous-préfectures[74]. Consulté sur le projet INES, M. Jacques Pélissard, président de l'Association des maires de France (AMF) a indiqué que le Bureau de l'AMF unanime, sur la base des éléments dont il avait connaissance sur le projet INES, s'était déclaré favorable à cette dernière solution, estimant que la délivrance d'un titre d'identité biométrique relevait des missions régaliennes de l'État.

Compte tenu des **enjeux liés à l'aménagement du territoire et au maintien de la continuité des services publics**, votre mission d'information juge **nécessaire de procéder à une large concertation avec les élus et leurs représentants avant de privilégier une option**. Il pourrait être laissé aux communes membres d'un établissement public de coopération intercommunale à fiscalité propre le choix de désigner la commune responsable de la délivrance des titres. Des **solutions innovantes** doivent être imaginées, notamment la mise en place de stations mobiles d'enrôlement des données biométriques financées par l'Etat pour accéder aux régions isolées. Rappelons toutefois que les communes garderaient toutes leurs compétences en matière d'état civil.

En conclusion, la biométrie offre des solutions nouvelles pour mieux sécuriser les titres d'identité. Elle est toutefois complexe à mettre en oeuvre et nécessite au préalable une réflexion globale pour être performante. Elle ne doit pas non plus être considérée comme une solution miraculeuse. En tout état de cause, sa mise en oeuvre exige de la prudence. Telles sont les raisons pour lesquelles, un éventuel recours intensif à la biométrie pourrait faire l'objet d'une introduction progressive ou être précédé d'une phase d'expérimentation.

---

[72] Le coût d'une station de base serait évalué à 10.000 euros, un site pouvant disposer de plusieurs stations. Une station nécessite 1,5 agent à temps plein.

[73] Selon le projet INES, un site doit délivrer 2500 titres par an au minimum pour être efficace.

[74] Dans son discours de politique générale du mercredi 8 juin, M. Dominique de Villepin, Premier ministre, a souhaité rapprocher l'État des citoyens en donnant de nouvelles responsabilités aux sous-préfectures.

En outre, les priorités diffèrent selon qu'il s'agit du passeport ou de la carte nationale d'identité. Si des synergies évidentes sont possibles, ne serait-ce que pour mutualiser les coûts de production, il s'agit toutefois de documents distincts n'appelant pas nécessairement un traitement uniforme. A cet égard, le Forum des droits sur l'internet recommande de découpler le projet INES du projet passeport.

B. VERS DE NOUVEAUX USAGES DES TITRES D'IDENTITÉ AFIN DE SÉCURISER LES ÉCHANGES ÉLECTRONIQUES ?

Les pouvoirs publics français se sont attachés à élaborer un cadre juridique destiné à promouvoir les échanges électroniques. Pour les sécuriser, ils envisagent depuis plusieurs années de doter les cartes d'identité de puces offrant des possibilités d'authentification et de signature électroniques. Les solutions retenues dans plusieurs Etats européens les y encouragent. Toutefois, la mise en œuvre de ce projet suscite des objections de principe et des difficultés pratiques.

1. La définition d'un cadre juridique destiné à promouvoir les échanges électroniques

Le développement des technologies de l'information et de la communication suppose de sécuriser les échanges électroniques. Tel est l'objet des plans « RE/SO 2007 » (Pour une République numérique dans la société de l'information), présenté le 12 novembre 2002 par M. Jean-Pierre Raffarin, alors Premier ministre, et « eEurope 2005 », élaboré par l'Union européenne, qui tendent à promouvoir des services publics en ligne modernes, un environnement dynamique pour les affaires électroniques, une infrastructure d'information sécurisée, un accès au haut débit à des prix concurrentiels, une évaluation comparative et la diffusion des bonnes pratiques.

a) Un recours croissant aux technologies de l'information et de la communication

Les technologies de l'information et de la communication sont de plus en plus utilisées aussi bien dans les transactions privées que dans les relations entre l'administration et ses usagers.

Selon le tableau de bord du **commerce électronique** établi en décembre 2004 par la mission pour l'économie numérique, 31 % des ménages français étaient connectés à l'internet à domicile, en début d'année 2004, cette proportion ayant quadruplé depuis 1999. En septembre 2004, la moitié d'entre eux, soit environ 3,8 millions de ménages, disposait d'une connexion à haut débit.

Toutefois, au sein de l'Union européenne, la France figure en douzième position en matière de connexion à l'internet. Cette situation résulte notamment d'un **équipement des ménages français en micro-ordinateurs inférieur à celui de la majorité des autres pays européens** : 45 % début 2004 selon l'INSEE contre 62 % en Allemagne et 58 % au Royaume-Uni.

La pratique des **achats en ligne**, confidentielle au départ, devient de plus en plus un phénomène de société. Ainsi, sur 21,8 millions d'internautes à la fin 2003, environ 8,3 millions avaient effectué des achats en ligne, soit 38 % contre seulement 30 % un an plus tôt. En septembre 2004, plus de 47 % des internautes affirmaient leur confiance dans ce type d'achats.

Selon la Fédération des entreprises de ventes à distance, **le chiffre d'affaires des ventes en ligne de biens et services a atteint 3,6 milliards d'euros** (hors réservation voyages et produits financiers) **en 2003**, contre 2,2 milliards en 2002. Néanmoins, le nombre d'acheteurs réguliers reste encore limité.

Si elles appellent moins l'attention du public, les transactions commerciales interentreprises représentent plus de 90 % du chiffre d'affaires du commerce électronique total.

Plus de 90 % des entreprises françaises sont équipées en micro-ordinateurs, près de 83 % d'entre elles sont connectées à l'Internet, dont 53 % en haut débit (ADSL), et 83 % utilisent le courrier électronique.

La **vente par Internet** reste encore **limitée à un faible nombre d'entreprises** : moins d'une entreprise française sur dix avait franchi le pas à la fin de l'année 2002. En revanche, les achats se sont nettement développés. Plus de 31 % des entreprises françaises déclaraient y recourir en 2002, contre 25 % en 2001, cette part étant supérieure à la moitié pour les entreprises de plus de 250 salariés. Au total, les **achats** par Internet représentaient **3,7 % de l'ensemble des achats des entreprises** à la fin de l'année 2001.

L'**administration électronique** constitue **l'un des leviers essentiels de la réforme de l'Etat**. Elle permet en effet, d'une part, de réaliser d'importants gains de productivité ou de développer, à coût constant, de nouveaux services, d'autre part, de simplifier l'ensemble des démarches que doivent effectuer les citoyens et les entreprises. Aussi son développement a-t-il été encouragé par les gouvernements successifs.

Dans le cadre du plan RE/SO 2007, le **programme ADELE** (administration électronique) recense **140 mesures** destinées à moderniser l'administration entre 2004 et 2007. La coordination de ces projets a été confiée à l'Agence pour le développement de l'administration électronique, service interministériel placé auprès du Premier ministre et mis à la disposition du ministre chargé de la réforme de l'Etat.

Le **premier bilan** est **positif**. 7.000 sites Internet publics ont d'ores et déjà été créés. Neuf formulaires sur dix sont disponibles en ligne. Une feuille de maladie sur deux est traitée sous forme dématérialisée, contre une sur quatre il y a deux ans. 3,7 millions de citoyens, soit 11 % des foyers fiscaux, ont déclaré leurs revenus à l'administration fiscale par voie électronique en 2005, contre 119.000 en 2002, 600.000 en 2003 et 1,25 million en 2004.

Depuis le 1er janvier 2005, les acheteurs publics sont tenus, en application du second alinéa de l'article 56 du code des marchés publics, de recevoir les candidatures et les offres relatives aux marchés passés selon une procédure formalisée qui leur sont transmises par la voie électronique. Conformément aux dispositions d'un décret n° 2002-692 du 30 avril 2002, les candidats doivent revêtir leur envoi d'une signature électronique.

Depuis le mois de mai 2005, en application d'une ordonnance n° 2005-395 du 28 avril 2005 et d'un décret n° 2005-469 du 16 mai 2005, le service public du changement d'adresse permet aux quelque 6 millions de Français qui déménagent chaque année de déclarer en ligne leur nouvelle adresse aux caisses d'allocations familiales, aux caisses primaires d'assurance maladie, aux caisses d'assurance chômage, aux services des impôts et aux bureaux du service national. Il devrait être progressivement élargi aux autres services publics, caisses d'assurance vieillesse et services de renouvellement de cartes grises des véhicules notamment. A terme, les changements d'adresse devraient pourvoir être notifiés aux entreprises fournissant des services postaux, aux opérateurs de télécommunications et aux distributeurs d'électricité, de gaz et d'eau.

Cette croissance est liée à la progression du nombre d'internautes, au développement des connexions à haut débit mais également à la définition d'un cadre juridique protecteur.

b) L'élaboration d'un cadre juridique protecteur

Comme le soulignait le Conseil d'Etat dans une étude réalisée en 1998, **le développement des échanges électroniques suppose l'élaboration d'un cadre juridique garantissant leur valeur juridique et leur confidentialité**, la réglementation étatique devant par ailleurs se combiner avec l'autorégulation des acteurs[75].

De nombreux textes européens ont tracé ce cadre :

- la 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

---

[75] *« Internet et les réseaux numériques » - Etude adoptée par l'Assemblée générale du Conseil d'Etat le 2 juillet 1998 – M. Jean-François Thery, Mme Isabelle Falque-Pierrotin – La Documentation française.*

données, s'est attachée à établir un équilibre entre un niveau élevé de protection de la vie privée des personnes et la libre circulation des données à caractère personnel au sein de l'Union européenne, en fixant des limites strictes à la collecte et à l'utilisation des données à caractère personnel, et en demandant la création d'un organisme de contrôle dans chaque Etat membre ;

- la directive 1999/93/CE du 13 décembre 1999 portant sur un cadre communautaire pour les signatures électroniques a consacré la reconnaissance légale de la signature électronique et la libre circulation des services de certification électronique en Europe ;

- la directive 2000/31/CE du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur s'est attachée à renforcer la sécurité juridique du commerce électronique afin d'améliorer la confiance des internautes en soumettant les services de la société de l'information aux principes du marché intérieur (libre circulation et liberté d'établissement) et en instaurant un nombre limité de mesures harmonisées ;

- la directive cadre 2002/21/CE du Parlement européen et du Conseil du 7 mars 2002, complétée par six autres directives ou décisions formant ce qui est communément appelé le « paquet télécoms », a établi un cadre réglementaire commun pour les réseaux et les services de communications électroniques.

Ces textes ont été progressivement transposés en droit interne.

La loi n° 2000-719 du 1er août 2000 modifiant la loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication a mis en place un régime de responsabilité pour les fournisseurs d'hébergement76.

La loi n° 2000-1230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique a reconnu la validité juridique de la signature électronique au même titre que la signature manuscrite, instauré une présomption de fiabilité en faveur des signatures électroniques répondant à des conditions définies par décret en Conseil d'Etat et établi les règles applicables à la cryptologie.

---

[76] *Les fournisseurs d'hébergement ont pour fonction de gérer techniquement les ressources connectées au réseau Internet et de mettre ces ressources à la disposition de leurs abonnés. Ils assurent, en quelque sorte, une activité de loueur d'emplacement : techniquement, leur rôle se résume à stocker sur leur propre serveur l'ensemble des informations qu'ils sont conduits à recueillir et qui, par la suite, seront consultées par les utilisateurs du service de communication publique en ligne.*

En application du décret n° 2001-272 du 30 mars 2001, pour être présumée fiable, une signature doit être :

- sécurisée, c'est-à-dire propre au signataire, créée par des moyens que le signataire puisse garder sous son contrôle exclusif, et garantissant avec l'acte auquel elle s'attache un lien tel que toute modification ultérieure de cet acte soit détectable ;

- établie au moyen de dispositifs sécurisés de création, certifiés par un service du Premier ministre, la direction centrale de la sécurité des systèmes d'information, ou tout organisme désigné à cet effet par un Etat membre de la Communauté européenne ;

- vérifiée au moyen de certificats électroniques délivrés par des prestataires de services de certification électronique qualifiés selon une procédure précisée par un arrêté du 26 juillet 2004.

La signature électronique

Le développement du commerce électronique est subordonné à l'existence de garanties sur la sécurité des transmissions de données et des paiements en ligne. Grâce à un système de chiffrement appliqué au message transmis, sans que ce dernier soit nécessairement lui-même chiffré, la signature électronique constitue une réponse au problème, car elle garantit l'authenticité et l'intégrité des données, ainsi que l'identité du signataire. Si la confidentialité est requise, il faut chiffrer le contenu du message.

De façon générale, le chiffrement consiste à rendre le texte d'un message illisible pour qui ne détient pas la clé de déchiffrement. Dans les systèmes de chiffrement symétriques, une seule clé sert à la fois à chiffrer et à déchiffrer les données. Elle doit être gardée secrète par les parties intéressées pour que la sécurité de l'information soit garantie. L'inconvénient principal réside dans le fait que l'expéditeur et le destinataire doivent convenir à l'avance de la clé et disposer d'un canal sûr pour l'échanger.

Telle est la raison pour laquelle se développent depuis quelques années des systèmes de signature électronique reposant sur des algorithmes de chiffrement asymétriques où chaque utilisateur dispose de deux clés, une clé publique et une clé privée. Ces deux clés sont elles-mêmes créées à l'aide d'algorithmes mathématiques. Elles sont associées l'une à l'autre de façon unique et sont propres à un utilisateur donné. Un message chiffré à l'aide d'un algorithme asymétrique et d'une clé privée, qui constitue l'un des paramètres de l'algorithme, ne peut être déchiffré qu'avec la clé publique correspondante, et inversement. La clé publique doit donc être connue de tous, tandis que la clé privée reste secrète, la carte à puce semblant être le meilleur support de stockage des clés privées. Lorsque l'algorithme de chiffrement asymétrique est utilisé seulement pour créer la signature électronique, les mêmes clés, privée et publique, sont utilisées, mais seulement pour vérifier l'authenticité et l'intégrité du message.

Contrairement à la signature manuscrite, la signature numérique, composée de chiffres, de lettres et d'autres signes, ne comporte aucun élément permettant de l'attribuer à une personne donnée. Chaque utilisateur doit donc établir avec certitude l'identité de ses correspondants. Telle est la raison pour laquelle on recourt à des services de certification, souvent désignés comme « tiers de certification », qui disposent de la confiance de chacun et qui garantissent l'appartenance d'une signature à une personne. Comme le destinataire utilise la clé publique de l'expéditeur pour vérifier la signature électronique de ce dernier, la vérification suppose que le tiers certifie au destinataire que la clé publique qu'il utilise correspond bien à la clé privée de l'expéditeur signataire et que ce dernier est bien celui qu'il prétend être. Les tiers de certification délivrent donc des certificats d'authentification contenant, d'une part, divers renseignements sur la personne dont on souhaite vérifier l'identité (nom, prénom, date de naissance...), d'autre part, sa clé publique. Ces certificats sont généralement réunis dans des bases de données mises en ligne sur le réseau Internet, ce qui permet à chacun d'y accéder facilement.

La signature numérique constitue donc un bloc de données créé à l'aide d'une clé privée ; la clé publique correspondante et le certificat permettent de vérifier que la signature provient réellement de la clé privée associée, qu'elle est bien celle de l'expéditeur et que le message n'a pas été altéré.

La loi n° 2004-575 du 21 juin 2004 sur la confiance dans l'économie numérique a parachevé cette évolution. Elle a complété le régime de la responsabilité des prestataires contribuant à la mise à disposition du public de services de communication en ligne, établi des règles spécifiques applicables en matière de commerce électronique, précisé les conditions de la reconnaissance de la validité de l'écrit électronique, créé un nouveau régime applicable à la cryptologie et renforcé les dispositions permettant de lutter contre la cybercriminalité.

Peu après, la loi n° 2004-669 du 9 juillet 2004 relative aux communications électroniques et aux services de communication audiovisuelle a tiré les conséquences en droit interne des directives formant le « paquet télécoms ».

La directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 a quant à elle été transposée par la loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

2. Le choix de cartes à puce offrant un accès sécurisé aux échanges électroniques

Les pouvoirs publics ont également exprimé la volonté de créer des cartes équipées de puces électroniques afin d'offrir un accès sécurisé aux échanges électroniques. Des cartes de vie quotidienne sont d'ores et déjà expérimentées au niveau local. Le projet consistant à doter la carte nationale d'identité de fonctions d'authentification et de signature électroniques se précise.

a) La création de cartes de vie quotidienne au niveau local

De nombreux projets de « **cartes de vie quotidienne** » se sont développés depuis quelques années. Ils permettent de simplifier les relations entre les usagers et les services de proximité offerts par les collectivités territoriales.

L'Etat a élaboré un **plan de soutien national à ces projets locaux** afin de promouvoir les initiatives innovantes, la mutualisation des ressources et la standardisation des technologies. Lancé le 12 mars 2003, l'« appel à projets CVQ » s'est traduit par la sélection de **quatorze projets** bénéficiant d'un soutien financier, d'un apport méthodologique et d'un suivi régulier.

A titre d'exemple, les communes de Bondues, Comines, Faches-Thumesnil, La Madeleine, Lambersart, Lille, Lomme, Marcq-en-Baroeul, Marquette-lez-Lille, Mouvaux, Tourcoing, Villeneuve d'Ascq, Wattrelos et la communauté urbaine « Lille Métropole » ont créé une carte de vie quotidienne dotée d'une application d'identification et d'authentification pouvant être utilisée dans les domaines scolaires, périscolaires (restauration scolaire, gestion des crèches,…), culturels et sportifs (inscription en bibliothèque, médiathèque, accès aux piscines publiques,…) et d'un porte-monnaie électronique pour le paiement des droits d'accès à certains événements.

Un autre projet original, porté par le conseil général des Yvelines en partenariat avec le GIE SESAM-Vitale ainsi qu'avec les centres communaux d'action sociale et les établissements médico-sociaux, consiste à permettre l'utilisation de la carte Vitale dans le cadre d'un procédé de dématérialisation des traitements administratifs de l'allocation personnalisée à l'autonomie. Un second volet, appelé « carte jeune », associe l'ensemble des collèges du département afin de mettre à la disposition des collégiens une carte multi-services compatible avec le porte-monnaie électronique Moneo.

En réponse à une question écrite posée par M. Cinieri Dino, député, le Gouvernement a indiqué qu'il était « *aussi prévu de définir un **label** « carte de vie quotidienne » à deux niveaux : un premier niveau déclaratif sera attribué à tout projet dont l'élu se portera garant du respect du référentiel commun.*

Ce référentiel est actuellement en cours d'élaboration et il prendra en compte les projets les plus avancés, comme base de travail et devrait être diffusé à l'automne prochain. Le second niveau vise à assurer une ***interopérabilité*** *nationale entre les CVQ de manière à leur permettre de servir d'outil d'accès à l'ensemble des applications de l'administration.* (…) *Ce label sera défini et géré par l'agence pour le développement de l'administration électronique et il correspondra au respect d'un triple référentiel technique, juridique et organisationnel*[77]. »

b) Un projet de carte nationale d'identité dotée de fonctions d'authentification et de signature électroniques

Le programme INES est d'une toute autre ampleur. Il repose sur l'idée selon laquelle il incombe à l'Etat de garantir l'identité des citoyens quels qu'en soient ses usages.

Dans une note de présentation rendue publique au mois de mars 2005, le ministère de l'intérieur soulignait ainsi que : « *Le développement de l'administration électronique et la multiplication des données personnelles en ligne rendent patent le besoin de disposer d'outils permettant de garantir son identité sur Internet et de signer électroniquement ses transactions. Afin d'éviter que chaque administration mette en place ses propres modes de signature, ou achète au prix fort des certificats aux entreprises privées spécialisées, il est prévu de doter la carte INES de ces fonctionnalités qui seront valables pour toutes les administrations et tous les services financiers ou commerciaux sur Internet*. »

Il faisait écho aux réflexions formulées en ces termes par MM. Pierre Truche, Jean-Paul Faugère et Patrice Flichy, dans un rapport sur l'administration électronique et la protection des données personnelles publié en 2002 : « *Alors que les identités numériques prolifèrent, et que se développent à une échelle accrue des formes d'identité privées, semant le trouble sur la notion même d'identité, on va peut-être redécouvrir la valeur de l'identité publique, originelle et originale, unique, stable et permanente, attestée et garantie par l'État. L'identité publique, en un sens, sert déjà de socle et de référent pour certaines identités numériques. La carte d'identité n'est-elle pas demandée, dans bien des magasins, à l'appui d'un chèque* ?[78] »

Aussi était-il envisagé, selon les indications communiquées par ce même ministère, de permettre à la carte nationale d'identité électronique de remplir une **double fonction d'authentification et de signature électroniques** « *pour des usages d'abord orientés vers l'administration électronique mais potentiellement extensibles au commerce électronique lorsqu'il est nécessaire de prouver son identité ou de signer un contrat*. »

---

[77] *Réponse à la question écrite n° 59578 publiée au Journal officiel de l'Assemblée nationale du 7 juin 2005, page 5990.*

[78] *Administration électronique et protection des données personnelles : livre blanc – La Documentation française – février 2002 – page 39.*

La fonction d'authentification permettrait au titulaire de la carte d'avoir accès, en utilisant un code secret, à des sites d'administration électronique gérant des données personnelles : fiscales, médicales…

La fonction de signature lui permettrait, également au moyen d'un code secret, de signer par voie électronique des documents, par exemple une déclaration de revenus, avec la même valeur qu'une signature manuscrite.

Ces deux fonctions seraient assurées au moyen de certificats électroniques émis par l'Etat, garantissant l'identité du titulaire de la carte et permettant à son interlocuteur de s'en assurer.

Enfin, un **portfolio personnel** permettrait **à celui qui le souhaite** de stocker des informations complémentaires dans la carte soit pour faciliter ses transactions électroniques (par exemple ses nom, prénoms et adresse qu'il pourrait extraire afin de remplir des formulaires), soit pour remplacer d'autres documents (numéro du permis de conduire, numéro fiscal…). Ainsi, lors d'un contrôle routier, les forces de l'ordre pourraient consulter la base des permis de conduire et vérifier que l'individu en est bien titulaire.

En revanche, la carte ne comprendrait aucune donnée sanitaire ou sociale, serait dépourvue de tout lien avec la carte vitale et ne pourrait servir de carte de paiement.

Ces différentes applications seraient cloisonnées entre elles ainsi qu'avec les données d'identification contenues dans la puce électronique.

Un **centre d'appel** serait créé pour recevoir, nuit et jour, les demandes de mise en opposition d'une carte perdue ou volée. En cas d'utilisation de la carte sur Internet, il serait possible de vérifier, sur une liste tenue par le ministère de l'intérieur, si elle est mise en opposition.

Dans la mesure où elle offrirait de nouveaux services, la carte nationale d'identité électronique pourrait redevenir payante. **On peut également se demander si la nécessité d'assurer sa sécurité, notamment en renouvelant les certificats, ne rendrait pas elle aussi nécessaire de réduire sa durée de validité.**

c) Les avantages attendus de la carte nationale d'identité électronique

Un sondage réalisé en septembre 2002 par la SOFRES à la demande du Forum des droits sur l'Internet montrait que les trois-quarts des Français étaient favorables à une carte d'identité électronique permettant notamment d'effectuer ses démarches administratives par l'Internet.

Une telle carte présenterait en effet le double avantage de **sécuriser les échanges électroniques** et de **faciliter la vie quotidienne des citoyens** en leur évitant de se munir en permanence de divers documents administratifs.

Le besoin de sécurité est réel. La Commission nationale de l'informatique et des libertés a souligné ainsi à maintes reprises que certains échanges électroniques devaient être subordonnés à une authentification préalable. Encore récemment, dans une délibération n° 2005-054 du 30 mars 2005 sur le service public du changement d'adresse, constatant que l'authentification de l'usager serait assurée par la saisie d'un numéro de dossier et d'un mot de passe, elle a souligné « *les risques forts d'utilisation détournée du service inhérents à ce procédé d'authentification de faible niveau* » et jugé nécessaire de mettre en place un dispositif d'authentification renforcé, par exemple, par un système de certificat électronique ou de signature électronique.

Selon MM. Pierre Truche, Jean-Paul Faugère et Patrice Flichy : « *Dès lors que la version électronique de la carte nationale d'identité disposerait d'une puce, elle pourrait être dotée d'une fonction de signature électronique : celle-ci pourrait alors être utilisée pour donner accès à des téléservices en ligne pour lesquels serait exigée l'authentification. Cette fonctionnalité pourrait être utile dans certaines fonctions spécifiques à la gestion de l'identité par le ministère de l'intérieur (changement d'adresse, renouvellement de carte, par exemple). Elle pourrait également servir, au-delà, de système d'authentification générique pour l'accès et l'utilisation des téléservices publics. En d'autres termes, une carte nationale d'identité électronique pourrait être un candidat à la fourniture d'un « service public » de la signature électronique*[79]. »

Dans une recommandation sur le développement de l'administration électronique rendue publique le 3 février 2003, le Forum des droits sur l'Internet a admis l'utilisation d'une carte à puce délivrée aux usagers à des fins d'administration électronique, en indiquant que : « *Les administrations ne doivent pas a priori s'interdire de fournir elles mêmes aux usagers les outils de la signature électronique lorsque celle-ci apparaît nécessaire compte tenu des caractéristiques du téléservice en cause.* »

Enfin, lors de son audition devant la mission, M. Christian Noyer, gouverneur de la Banque de France, président de l'Observatoire de la sécurité des cartes de paiement, a indiqué que le renforcement des méthodes d'authentification des clients constituait un axe majeur d'amélioration de la sécurité des paiements sur lequel la profession bancaire avait engagé des efforts. Après avoir rappelé que la Banque de France avait, dès 2002, préconisé le recours à des méthodes d'authentification forte et la

---

[79] *Administration électronique et protection des données personnelles : livre blanc – La Documentation française – février 2002 – page 87.*

généralisation de l'identité et de la signature électroniques pour les paiements sur Internet, il a estimé que l'utilisation de la carte nationale d'identité électronique à des fins de contrôle pour des opérations bancaires, répondrait naturellement à ces préconisations. Il a précisé en revanche, qu'après avoir étudié en 2003 les apports éventuels de la biométrie dans l'environnement des cartes de paiement, l'Observatoire de la sécurité des cartes de paiement avait recommandé que les techniques d'authentification biométrique ne remplacent pas les mécanismes fondés sur la saisie d'un code confidentiel, compte tenu de la fiabilité encore insuffisante des dispositifs de contrôle des caractéristiques biométriques.

Notons enfin qu'**une carte d'identité électronique serait plus difficile à contrefaire que les documents actuels**. Les données stockées dans la puce, qui reproduiraient les données figurant sur le document (état civil, lieu et date de délivrance du titre), seraient en effet protégées par un blocage en écriture des zones non réinscriptibles de la puce à l'issue de la fabrication, notamment les zones d'identité, et l'utilisation des procédés cryptographiques de signature électronique, permettant par la lecture des données de s'assurer que celles-ci sont authentiques et intègres.

Toutefois, dans le cas de la France, le problème de la fraude n'est pas lié à la sécurisation de la carte nationale d'identité elle-même. Le principal problème se situe en amont du fait des fraudes à l'état civil qui conduisent à la délivrance de titres authentiques aux mauvaises personnes. Telles sont les raisons pour lesquelles le ministère de l'intérieur souligne que seul le recours à la biométrie permettrait d'éliminer la quasi-totalité de ces fraudes.

3. Une solution retenue dans plusieurs pays européens

De nombreux pays européens ont déjà créé ou envisagent de créer une carte nationale d'identité électronique comportant des fonctionnalités d'authentification et de signature électroniques.

a) Les pays où la carte d'identité électronique est déjà distribuée

En **Italie**, la mise en circulation d'une carte d'identité électronique a commencé en 2004. Cette carte permet l'authentification sur Internet, fonction à laquelle de nombreux services ont été associés : paiement des impôts, taxes et amendes, inscription aux services municipaux, rendez-vous hospitaliers, demandes d'aides sociales…

En **Estonie**, près de 40 % de la population, soit 700.000 Estoniens et résidents étrangers, dispose d'une carte d'identité électronique, dont la distribution a commencé en 2002. Celle-ci ne comporte pas de données biométriques mais peut être utilisée à des fins d'authentification et de

signature électroniques. Elle intègre le permis de conduire, la carte de sécurité sociale et permet le vote électronique. Son coût est légèrement inférieur à 10 euros.

En **Finlande**, 45.000 cartes électroniques avaient été distribuées en 2004, comportant des données d'assurance et de sécurité sociale et permettant à leurs titulaires de s'authentifier et de signer par voie électronique. Le coût d'acquisition de la carte s'élève à 40 euros.

En **Belgique**, après une phase d'expérimentation, la carte d'identité électronique est distribuée par les communes depuis le mois de juillet 2004. Un million de citoyens belges devrait en disposer au mois d'août 2005, environ 160.000 documents étant produits chaque mois. Pour permettre aux communes de faire face à cette charge supplémentaire, l'Etat a mis à leur disposition 722 emplois équivalents temps plein.

La carte est obligatoire dès l'âge de 15 ans et payante, son coût de base de 10 euros pouvant être majoré d'une taxe perçue par la commune. Elle ne comporte pas de données biométriques mais peut être utilisée à des fins d'authentification et de signature électroniques permettant à son titulaire, sans se déplacer :

- au niveau national, d'avoir accès aux données du Registre de la population qui le concernent, d'obtenir leur rectification ainsi que leur communication à des administrations ou des entreprises privées, de connaître l'identité des personnes qui y ont eu accès, de déclarer et payer ses impôts ou encore de se présenter à un examen au permis de conduire ;

- au niveau communal, de suivre l'état d'avancement d'un dossier, par exemple une demande de permis de construire, d'inscrire ses enfants à l'école, de réserver des spectacles ou des équipements sportifs, d'obtenir des extraits d'actes de l'état civil, des cartes de stationnement.

L'usage de la carte à des fins privées n'est pas interdit ; il nécessite simplement l'acquisition d'un lecteur. A terme, elle pourrait être fusionnée avec la carte de sécurité sociale. Microsoft a récemment annoncé que son service de messagerie MSN serait compatible avec elle.

Deux sociétés belges, ZETES et STERIA, ont été retenues par l'Etat au terme de deux appels d'offres européens, respectivement pour la production des cartes et l'exploitation de l'application informatique.

Une délégation de la mission d'information s'est rendue en Belgique le 12 mai 2005 afin d'observer la mise en place de ces cartes d'identité électroniques.

Elle y a été reçue par M. Luc Vanneste, directeur général de la direction des institutions et de la population, qui a mis en exergue les **avantages de ce document en termes de protection des données personnelles et de simplification des démarches des citoyens** à l'aide d'un exemple emprunté au monde bancaire :

« *Un banquier va m'accorder un prêt pour l'acquisition d'une voiture mais, avant de l'accorder, il veut apprendre quels sont mes revenus et quelles sont mes charges de famille. Mes revenus sont vérifiables de façon électronique dans mon dossier près du service des contributions ; mes charges familiales résultent de la rubrique « composition du ménage » du dossier de population*.

« *En tant que titulaire de la carte d'identité électronique, je peux vérifier les deux dossiers. Je peux extraire ces données de ces dossiers respectifs, les faire signer par les maîtres de ces fichiers (le service des contributions et le Registre national) et les transmettre sous format standardisé à mon banquier qui doit accorder le prêt et qui enregistre ces données dans mon dossier de prêt électronique. Le prêt est confirmé par une signature électronique du banquier et par celle du client*.

« *La protection de la vie privée est mieux assurée parce que le titulaire de la carte peut avoir accès à ses propres données enregistrées en toutes sortes de fichiers et vérifier qui a consulté ou mis à jour son dossier du registre national. La transparence des fichiers contenant des données personnelles devient une transparence véritable et non pas une transparence papier comme c'était le cas dans le passé*. »

En se rendant dans la commune de Woluwe-Saint-Pierre, collectivité pilote lors de la phase d'expérimentation, les membres de la délégation ont toutefois pu relever un certain nombre de **difficultés d'application, inhérentes aux prémisses de toute réforme**.

Ont ainsi été déplorés tout à la fois : les défaillances de la coordination générale du projet, les difficultés de connexion au fichier des cartes d'identité, le coût élevé des adaptations de l'application informatique demandées à la société STERIA, le manque de fiabilité des lecteurs de carte ainsi que les difficultés d'installation sur les ordinateurs personnels des logiciels d'exploitation des cartes. Les agents de la commune ont par ailleurs regretté de devoir utiliser leur propre carte d'identité pour travailler, jugeant préférable de disposer de cartes de service.

La carte d'identité électronique semble cependant bien acceptée par la population et offre des perspectives prometteuses, dès lors que les difficultés techniques seront résolues. Le déplacement de la délégation de la mission lui a également permis de constater la nécessité de développer les services en ligne avant de diffuser la carte, afin que les citoyens en perçoivent immédiatement l'utilité.

b) Les pays où la carte d'identité électronique reste en projet

En **Autriche**, la détention d'une carte d'identité n'est pas obligatoire et coûte 56 euros. Sa durée de validité est de dix ans ; elle varie en fonction de l'âge pour les enfants de moins de 12 ans. Réalisé au format d'une carte bancaire, le document a été conçu dans la perspective d'intégrer ultérieurement une puce électronique comportant des données biométriques et pouvant être utilisée à des fins d'authentification et de signature électroniques. Cette intégration n'a pas encore été décidée. Elle présente un faible intérêt dans la mesure où la carte bancaire la plus répandue dans le pays et la carte de sécurité sociale sont d'ores et déjà équipées d'un tel dispositif.

De même, en **Allemagne** et aux **Pays-Bas**, il est question d'intégrer dans les cartes nationales d'identité une puce électronique comportant non seulement des données biométriques, ainsi qu'il l'a été indiqué, mais pouvant également être utilisée à des fins d'authentification et de signature électroniques. La décision n'a cependant pas encore été prise.

4. Des objections de principe et des interrogations pratiques qui doivent être prises en compte

La création d'une carte nationale d'identité dotée de fonctions d'authentification et de signature électroniques suscite des objections de principe et des interrogations pratiques qui doivent être prises en compte.

a) Des objections de principe

D'aucuns considèrent que la carte nationale d'identité doit exclusivement servir à prouver son identité dans les cas prévus par la loi. Ils s'opposent ainsi, pour des raisons de principe, à ce que ce document puisse être utilisé pour sécuriser les échanges électroniques.

Telle a été notamment la position défendue aussi bien par MM. Thierry Wickers, président de la Conférence des bâtonniers, que par Mme Monique Herold et M. Alain Weber, respectivement vice-présidente et responsable de la commission Libertés et informatique de la Ligue des droits de l'homme, lors de leur audition par la mission.

M. François Giquel, vice-président de la Commission nationale de l'informatique et des libertés, a également exprimé des réserves en soulignant qu'une telle extension des fonctions de la carte nationale d'identité, en lui conférant davantage de valeur, pourrait accroître les risques d'atteinte aux personnes.

D'autres admettent l'intégration des fonctions d'authentification et de signature électroniques au sein de la carte nationale d'identité à la stricte condition d'en limiter l'utilisation à la sphère publique, c'est-à-dire à l'administration électronique.

M. Alain Bauer, président de l'Observatoire national de la délinquance, a ainsi considéré que la nouvelle carte d'identité n'avait pas vocation à servir dans toutes les circonstances de la vie et à devenir un outil commercial.

Dans sa recommandation sur le projet de carte nationale d'identité électronique du 16 juin 2005, le Forum des droits sur l'internet observe cependant que seule la possibilité d'utiliser la carte nationale d'identité électronique dans des transactions privées a suscité les réticences des participants au débat public, la possibilité de l'utiliser dans les téléprocédures administratives ne suscitant quant à elle guère d'intérêt.

b) Des interrogations pratiques

La création d'une carte nationale d'identité dotée de fonctions d'authentification et de signature électroniques ne doit pas entraîner une aggravation des inégalités.

Dans cette hypothèse, il conviendrait :

- de créer un document doté de fonctionnalités équivalentes au bénéfice des étrangers ;

- de permettre à l'ensemble du territoire national d'avoir accès au haut débit ;

- de favoriser l'équipement en micro-ordinateurs et en lecteurs de cartes à puce de l'ensemble de la population, les personnes âgées et celles disposant de faibles ressources étant actuellement nettement sous-équipées ;

- de permettre un accès à l'administration électronique sans recourir à un micro-ordinateur, soit par téléphone soit au moyen de bornes installées dans les communes.

La création d'une telle carte ne doit pas non plus conduire à une remise en cause de la possibilité d'échanges électroniques anonymes.

La totalité des démarches administratives ne nécessite pas d'identification formelle. Il en va de même de nombreuses transactions privées.

Dans sa recommandation sur le développement de l'administration électronique, le Forum des droits sur l'Internet estimait ainsi qu' : « *Il ne faut pas faire de l'usage de la signature électronique un préalable systématique au déploiement des services en ligne. Il est de nombreux services, comme la simulation d'impôts, dont l'usage doit pouvoir rester anonyme. Même quand l'identification ou l'authentification des usagers est nécessaire, elle peut très souvent fonctionner sur la base de simples identifiants et mots de passe. Quant au besoin de signature à proprement parler, il ne doit pas être surestimé : ce n'est pas parce que les formulaires papier comportent une case destinée à la signature du demandeur que leur équivalent électronique devrait être revêtu d'une signature électronique, car bien souvent la signature est demandée sur le formulaire papier sans avoir de réelle portée juridique*. »

Les exigences de sécurité techniques peuvent être modulées en fonction de la nature des échanges : le dispositif d'authentification prévu pour la carte nationale d'identité, très sécurisé, ne doit pas devenir un standard obligé pour tous les échanges électroniques.

Le ministère de l'économie, des finances et de l'industrie a ainsi prévu une gradation des mesures de sécurité en fonction de la nature des services proposés et du niveau de confidentialité ou de valeur juridique probante exigé : anonymat (simulations, actualité fiscale, téléchargements), simple adresse électronique de correspondance (réponses en ligne), authentification par mot de passe, authentification par l'usage de certificat électronique.

Dans son étude précitée sur Internet et les réseaux numériques, le Conseil d'Etat soulignait que : « *l'anonymat est une question complexe, au carrefour d'intérêts éthiques, économiques et politiques : l'individu veut se promener et agir librement comme dans sa vie quotidienne réelle, les entreprises veulent l'identifier pour mieux le servir, les autorités répressives ont besoin de retrouver les coupables d'infractions et donc de les identifier. L'équation est facile à poser moins facile à résoudre. L'individu doit pouvoir rester anonyme sur le réseau pour aller et venir, effectuer des paiements, envoyer des lettres… Cet anonymat peut se faire au moyen de la pseudonymisation. Il ne saurait cependant interdire de retrouver l'identité des personnes si nécessaire*. »

L'anonymat des échanges électroniques s'avère en effet relatif, dans la mesure où un fournisseur d'accès peut conserver toutes les données de connexion correspondant à une adresse IP, c'est-à-dire « l'adresse réseau » de la machine d'un utilisateur connecté au réseau Internet, et associer à chaque adresse IP, même dynamique, l'ensemble des données personnelles relatives à l'internaute, qui est son client.

La directive 1999/93/CE du 13 décembre 1999 portant sur un cadre communautaire pour les signatures électroniques reconnaît ainsi la légitimité de l'utilisation d'un pseudonyme tout en indiquant, dans son considérant n° 25, qu'« *il convient que les dispositions relatives à l'utilisation de pseudonymes dans des certificats n'empêchent pas les États membres de réclamer l'identification des personnes conformément au droit communautaire ou national*. » Son annexe I relative aux exigences concernant les certificats qualifiés prévoit ainsi que tout certificat qualifié doit comporter le nom du signataire ou un pseudonyme qui est identifié comme tel.

La création d'une carte d'identité dotée de fonctions d'authentification et de signature électroniques ne doit pas conduire les administrations à mettre en place un identifiant unique, comme l'a souligné le Forum des droits sur l'internet dans sa recommandation du 16 juin 2005.

Elle ne doit pas conduire non plus à une éviction des entreprises privées du marché de la certification.

Lors de son audition par la mission, M. Jacques Sauret, directeur de l'Agence pour le développement de l'administration électronique a estimé que, loin d'aboutir à un tel résultat, elle permettrait de structurer un marché de la certification qui peine à se développer.

Enfin, les risques afférents à la possibilité d'utiliser la carte électronique pour des transactions privées doivent être pris en compte. Elle ne doit :

- ni inciter les commerçants à imposer la justification de son identité pour tout paiement alors qu'en l'état actuel du droit, seul l'article L. 131-15 du code monétaire et financier oblige à présenter « un document officiel portant sa photographie » lors d'un paiement par chèque ;

- ni leur permettre d'établir des fichiers des habitudes de vie et de consommation de leurs clients ;

- ni rendre l'Etat, en sa qualité de prestataire de services de certification, destinataire d'informations relatives aux engagements privés souscrits par les particuliers,

- ni conduire à une mise en jeu de sa responsabilité pour les préjudices subis en cas de fraude.

Telles sont sans doute les raisons pour lesquelles la perspective d'une utilisation de la carte d'identité électronique pour des transactions privées est accueillie avec de réelles réticences.

Ces considérations montrent que l'enjeu essentiel de la création de titres d'identité électroniques tient à la nécessité d'assurer la protection des données personnelles qu'ils contiennent, au nom du droit constitutionnel au respect de la vie privée.

C. LES GARANTIES NÉCESSAIRES À LA PRÉSERVATION DES LIBERTÉS INDIVIDUELLES ET AU RESPECT DE LA VIE PRIVÉE

La mise en place d'un titre d'identité électronique avec ou sans biométrie pour lutter contre la fraude à l'identité génère des craintes quant au respect des libertés individuelles, en particulier de la vie privée. L'équilibre entre sécurité et liberté n'est pas aisé à trouver.

Il faut tout d'abord rappeler que **la sécurisation de l'identité n'est pas antinomique de la sauvegarde des libertés**. Protéger l'identité d'un individu, c'est protéger les droits attachés à sa personne, qu'il s'agisse du droit de propriété ou de la liberté d'aller et venir par exemple. Ainsi, comme l'a noté M. Gérard Tcholakian, membre de la commission « Libertés et droits de l'homme » du Conseil national des Barreaux, **la libre circulation et le droit au séjour des étrangers en situation régulière pourraient être mieux garantis avec un titre de séjour biométrique prouvant sans doute possible l'identité et les droits du porteur du titre**.

Protéger l'identité, c'est aussi sécuriser les relations contractuelles. Les sociétés modernes consacrent les droits et la responsabilité individuels. La confiance est donc indispensable aux relations individuelles et aux relations entre les citoyens et l'État. Si le système d'identité est altéré et dégradé, les conditions de la confiance ne sont plus réunies. Un parallèle peut être établi avec la fausse monnaie qui porte atteinte à la confiance dans le système monétaire.

Cet enjeu, ainsi que les questions de sécurité internationales, poussent les Etats à vouloir mettre en place de nouveaux systèmes d'identité extrêmement sûrs. **Cet objectif est légitime. Toutefois, il ne doit pas aboutir à sacrifier la liberté au nom de la sécurité**. Pour éviter cet écueil, il faut garder à l'esprit que **la fraude ne sera jamais éliminée** et qu'un système parfait n'existe pas. L'objectif raisonnable que les autorités publiques doivent se fixer est de contenir la fraude dans des proportions acceptables. Cette ligne de conduite est fondamentale pour **prévenir des solutions excessives**, solutions qui pourraient conduire notamment à transformer un système d'identité en un système de contrôle et de police.

1. Les règles régissant les traitements automatisés de données à caractère personnel

Avec ou sans biométrie, un titre d'identité électronique est soumis aux règles relatives à la protection des données à caractère personnel dès lors qu'il est adossé à un traitement automatisé ou qu'il permet d'échanger des données à distance.

a) Les exigences constitutionnelles

La jurisprudence du Conseil constitutionnel en matière de traitement des données à caractère personnel laisse au législateur une grande liberté d'appréciation tout en protégeant les libertés individuelles.

Aux termes de l'article 2 de la Déclaration des droits de l'homme et du citoyen : « *Le but de toute association politique est la conservation des droits naturels et imprescriptibles de l'homme. Ces droits sont la liberté, la propriété, la sûreté et la résistance à l'oppression* ».

En vertu de l'article 34 de la Constitution, il **appartient au législateur de fixer les règles générales applicables aux fichiers nominatifs et aux traitements de données personnelles**. **Celles-ci doivent s'attacher à respecter la vie privée** qui constitue un droit constitutionnel[80]. Ce droit requiert que soit observée une particulière vigilance dans la collecte et le traitement de données à caractère personnel de nature médicale[81].

Mais il incombe également au législateur de **concilier ce principe avec d'autres exigences, comme la sauvegarde de l'ordre public, la recherche des auteurs d'infractions et la préservation du bien-être économique et social**[82].

Le Conseil constitutionnel admet, sous certaines réserves, les **utilisations multiples d'un fichier**. Ainsi, dans sa décision n° 2003-467 DC du 13 mars 2003 sur la loi pour la sécurité intérieure, il a considéré qu'aucune norme constitutionnelle ne s'opposait par principe à l'utilisation à des fins administratives de données nominatives automatisées recueillies dans le cadre d'activités de police judiciaire. Toutefois, elle « *méconnaîtrait les exigences résultant des articles 2, 4, 9 et 16 de la Déclaration de 1789 si, par son caractère excessif, elle portait atteinte aux droits ou aux intérêts légitimes des personnes concernées* ». C'est aux conditions dans lesquelles il est procédé à la double utilisation d'un fichier que le Conseil constitutionnel et, par voie de conséquence, le législateur ou le pouvoir réglementaire doivent être attentifs.

Par ailleurs, le Conseil n'admet l'interconnexion de fichiers ayant à l'origine des finalités distinctes que dans un but de bonne administration et de contrôle.

---

80 Voir par exemple la décision n° 99-416 DC du 23 juillet 1999 sur la loi portant création d'une couverture maladie universelle.

81 Décision n° 99-422 DC du 21 décembre 1999.

82 Voir par exemple la décision n° 2003-467 DC du 13 mars 2003 relative à la loi pour la sécurité intérieure.

b) La convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales

Aux termes de l'article 8 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales (CEDH) :

- « *toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance* » ;

- « *il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui* ».

Toutefois, le Conseil de l'Europe a estimé que l'article 8 de la convention contenait un certain nombre de limites et d'inconvénients au regard du développement nouveau de l'informatique et des technologies de l'information. La portée du terme « vie privée » est insuffisamment définie et la prise en considération de la protection contre l'ingérence de personnes qui ne sont pas une autorité publique est inexistante.

Cette réflexion a conduit à l'adoption en 1981 d'une convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, appelée convention 108, qui a été ratifiée par 31 États membres du Conseil de l'Europe, dont tous les États membres de l'Union européenne. La convention a pour objectif d'assurer la *« protection du respect des droits et des libertés fondamentaux de toute personne physique, et notamment de son droit à la vie privée, à l'égard du traitement des données à caractère personnel la concernant* ».

Initialement, la convention 108 était conçue pour ne pas s'appliquer directement, les parties contractantes s'engageant à adopter des dispositions de droit interne conformes à ses principes fondamentaux.

Entre temps, la Cour européenne des droits de l'homme a estimé dans un avis de 1997 (affaire Z c. Finlande) que la protection des données à caractère personnel jouait un rôle fondamental pour l'exercice du droit au respect de la vie privée et familiale garanti par l'article 8 de la CEDH et précisé par la convention 108 à laquelle elle s'est référée.

c) La directive de 1995 et la loi « Informatique et libertés »

La loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, récemment modifiée par la loi n° 2004-801 du 6 août 2004 afin de transposer la directive européenne 95/46 CE du 24 octobre 1995,

définit les principes régissant les traitements de données à caractère personnel et les règles destinées à en assurer le respect par une autorité administrative indépendante, la Commission nationale de l'informatique et des libertés (CNIL).

- *Les principes régissant le traitement des données à caractère personnel*

Les données faisant l'objet d'un traitement doivent être :

- collectées et traitées de manière loyale et licite ;

- collectées pour des finalités déterminées, explicites et légitimes et ne pas être traitées ultérieurement de manière incompatible avec ces finalités, sauf pour des fins statistiques ou de recherche scientifique ou historique ;

- adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et de leurs traitements ultérieurs ;

- exactes, complètes et, si nécessaire, mises à jour ;

- conservées sous une forme permettant l'identification des personnes concernées pendant une durée qui n'excède pas la durée nécessaire aux finalités pour lesquelles elles sont collectées et traitées.

- *Des formalités simplifiées.*

La loi de 1978, dans sa rédaction antérieure à la loi du 6 août 2004, soumettait à formalités auprès de la CNIL, sans distinction, tout projet de traitement automatisé de données nominatives, et se fondait essentiellement, pour déterminer le contrôle préalable de la Commission, sur un critère organique : la nature publique ou privée du responsable du traitement. Ainsi, les traitements relevant du secteur public, pour être mis en oeuvre, devaient-ils obtenir au préalable un avis favorable de la CNIL alors que les traitements du secteur privé n'étaient astreints qu'à simple déclaration.

Désormais, ne sont soumis à autorisation ou avis de la CNIL, conformément à l'article 20 de la directive, que les seuls traitements présentant des risques particuliers au regard des droits et libertés des personnes. La déclaration est devenue le régime de droit commun pour la plupart des traitements, que ceux-ci relèvent de personnes publiques ou de personnes privées, de larges possibilités d'exemption et d'allègement des formalités étant prévues.

- *Un contrôle renforcé*

En contrepartie, **les pouvoirs de contrôle de la Commission ont été renforcés**.

Ses membres et les agents qu'elle habilite peuvent effectuer des contrôles sur place, accéder aux programmes informatiques et aux données, en demander la transcription par tout traitement approprié, recueillir, sur place ou sur convocation, tout renseignement et toute justification utile, demander communication et prendre copie de tous documents utiles à l'accomplissement de leurs missions.

Alors qu'auparavant, la CNIL, constatant un manquement à la loi, ne pouvait que délivrer des avertissements aux organismes en cause ou les dénoncer au parquet, elle dispose désormais de pouvoirs de sanctions administratives et pécuniaires importants : hormis l'avertissement, la Commission peut, après une mise en demeure infructueuse et à l'issue d'une procédure contradictoire, prononcer une sanction pécuniaire (à l'exception des traitements mis en oeuvre par l'Etat), une injonction de cesser le traitement (pour les traitements relevant du régime déclaratif), ou encore retirer son autorisation (pour les traitements soumis à une telle procédure).

En outre, en cas d'urgence et de violation des droits et libertés résultant de la mise en oeuvre d'un traitement, la Commission peut décider l'interruption temporaire de celui-ci ou le verrouillage de données (pendant trois mois) à l'exception de certains traitements de l'Etat.

Enfin, en cas d'atteinte grave et immédiate aux droits et libertés, le président de la CNIL peut demander en référé au juge d'ordonner toute mesure de sécurité nécessaire à la sauvegarde de ces droits et libertés.

Le montant des sanctions pécuniaires susceptibles d'être infligées par la CNIL peut atteindre 150.000 € lors du premier manquement constaté, et 300.000 € ou 5 % du chiffre d'affaire hors taxes du dernier exercice s'il s'agit d'une entreprise dans la limite de 300.000 €. Le montant de ces sanctions doit être « *proportionné à la gravité des manquements commis et aux avantages tirés de ce manquement* ».

2. Les données biométriques : des données personnelles particulières

a) Les craintes et dangers liés à la biométrie

L'utilisation de la biométrie suscite de nombreuses interrogations en matière de respect des droits de l'homme et de la législation sur le traitement automatisé des données à caractère personnel. Comme pour toute technologie nouvelle, des doutes sont émis sur la maturité et la fiabilité des techniques ainsi que sur la capacité à garder le contrôle de systèmes biométriques déployés à grande échelle. Certains appellent à appliquer le principe de précaution face à un développement irréversible et imprévisible de la

biométrie dans le monde. D'autres craignent que la biométrie ne devienne un instrument de contrôle et de surveillance trop puissant entre les mains de la puissance publique.

Des **interrogations philosophiques** ont été soulevées devant les membres de la mission, notamment par M. Didier Bigo, chercheur au CERI (Centre d'Études et de Recherches Internationales) et maître de conférence à l'Institut d'Études politiques de Paris. S'attachant à marquer la **différence de nature entre une carte d'identité classique et un titre d'identité biométrique**, il a mis en évidence le passage d'une carte d'identité à une carte d'identification. La vérité de l'identité serait uniquement dans le corps et non plus dans l'identité sociale. La biométrisation de l'identité contribuerait à modifier en profondeur l'identité elle-même, en rendant l'identité indissociable d'un processus d'identification, qui est aussi un processus de contrôle.

La biométrie peut être aussi ressentie comme une **atteinte à la dignité humaine**. Certaines personnes réprouvent l'idée que le corps humain soit utilisé comme une source d'information. Les données biométriques peuvent révéler des maladies ou une origine raciale. Les progrès techniques pourraient donner la possibilité d'extraire beaucoup plus d'informations des données biométriques qu'aujourd'hui.

Le **caractère unique et permanent de la biométrie** pose également des difficultés. La Ligue des droits de l'homme et le Conseil national des barreaux ont rappelé que de nombreuses personnes avaient eu la vie sauve sous l'Occupation en utilisant de fausses identités. Or, l'utilisation généralisée de la biométrie pour s'identifier, notamment avec la mise en place d'un titre d'identité biométrique, rendrait impossible la dissimulation de son identité.

En outre, en cas d'erreur du système, par exemple si une autre personne a les mêmes caractéristiques biométriques (la probabilité est faible mais pas nulle) ou si celles-ci sont altérées en raison d'un accident ou du vieillissement, comment prouver sa bonne foi ?

b) La législation sur la protection des données personnelles applicable aux données biométriques

La loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ne faisait pas explicitement référence aux données biométriques et ce essentiellement en raison du fait qu'à cette date, l'identification ou l'authentification d'une personne reposait sur son état civil et le numéro d'inscription au registre national d'identification des personnes physiques (NIR, également appelé numéro de sécurité sociale).

Toutefois, par nature, un **élément d'identification biométrique ou sa traduction électronique constitue une donnée à caractère personnel entrant dans le champ d'application de la loi de 1978** conformément à l'article 4 de ce texte, aux termes duquel : « *sont réputées nominatives au sens de la présente loi les informations qui permettent, sous quelque forme que ce soit, directement ou non, l'identification des personnes physiques auxquelles elles s'appliquent, que le traitement soit effectué par une personne physique ou morale* ».

Les données biométriques présentent, en effet, la particularité de permettre à tout moment l'identification de la personne concernée sur la base d'une réalité biologique qui lui est propre, qui est permanente dans le temps et dont elle ne peut s'affranchir.

Aussi **la nouvelle loi « Informatique et libertés » du 6 août 2004 les a-t-elle soumises au cadre légal des données à caractère personnel et à la surveillance de la Commission nationale de l'informatique et des libertés, tout en prenant en compte leur spécificité :**

- les traitements des données biométriques nécessaires au contrôle de l'identité des personnes sont désormais soumis à un régime d'autorisation par la Commission (article 25) ;

- les traitements de données biométriques mis en œuvre pour le compte de l'Etat et nécessaires à l'authentification ou au contrôle de l'identité des personnes doivent être autorisés par décret en Conseil d'Etat après avis de la Commission[83] (article 27).

Bien qu'il n'existe pas de dispositions légales ou réglementaires spécifiques définissant ce qui est permis ou non en matière de traitement des données biométriques, **la CNIL s'est déjà efforcée d'encadrer leur utilisation**.

Elle n'a pas adopté une position de principe de refus de collecte de toute donnée biométrique.

Ainsi, elle tient pour légitime le recours, pour s'assurer de l'identité d'une personne, à des dispositifs de reconnaissance biométrique dès lors que la donnée biométrique est conservée sur un support dont la personne a l'usage exclusif[84].

---

[83] *Sous l'empire de la loi de 1978 non modifiée, les actes réglementaires portant création de tels traitements étaient pris après avis motivé de la CNIL ou, en cas d'avis défavorable, après avis conforme du Conseil d'Etat.*

[84] *Voir par exemple la délibération de la CNIL n° 03-015 du 24 avril 2003 portant avis sur les articles 4 et 5 d'un projet de loi relatif à l'immigration.*

En revanche, la CNIL considère que « *la mémorisation et le traitement de données issues des empreintes digitales, compte tenu des caractéristiques de l'élément d'identification physique retenu et des usages possibles des bases de données qui pourraient ainsi être constituées, doivent être justifiés par des exigences impérieuses en matière de sécurité ou d'ordre public* ». Appréciant strictement la réunion de ces critères, elle censure tout projet ne démontrant pas que la collecte de données biométriques est pertinente et proportionnée au regard de la finalité du traitement[85].

La CNIL souligne l'importance de ne pas banaliser le recours à **la biométrie**. Elle **ne doit pas être utilisée seulement parce qu'elle est pratique, mais parce qu'elle constitue le seul moyen d'atteindre le résultat recherché**.

L'attitude de la Commission diffère selon la nature de la donnée biométrique recueillie. Elle considère par exemple que les empreintes digitales présentent un niveau de risque plus élevé que les autres biométries dites « sans traces », du moins en l'état actuel de la technologie. Ces traces peuvent être exploitées pour l'identification des personnes et, dès lors, toute base de données d'empreintes digitales est susceptible d'être utilisée à des fins étrangères à sa finalité première.

En outre, la CNIL applique à ce type de traitement automatisé de données biométriques l'ensemble des principes applicables aux traitements automatisés de données à caractère personnel. Ainsi, l'article 6 de la loi du 6 janvier 1978 modifiée prévoit que les données à caractère personnel ne peuvent être traitées que pour des finalités déterminées, explicites et légitimes ; elles doivent être adéquates, pertinentes et non excessives au regard de ces finalités et conservées pendant une durée qui n'excède pas celle nécessaire aux finalités pour lesquelles elles sont collectées et traitées.

Ce principe de proportionnalité a commandé la plupart des avis et autorisations de la CNIL dans le domaine des applications biométriques.

c) Des limites relatives mais pas absolues au développement des traitements automatisés de données biométriques

Le principe le plus important est que l'instrument doit servir la finalité pour laquelle les données ont été collectées.

---

[85] *Pour un exemple d'avis favorable et défavorable, voir la délibération de la CNIL n° 2004-075 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.*

Cela implique comme préalable la définition précise des objectifs assignés à un système de traitement automatisé de données biométriques. Ainsi, **le choix entre une fonction d'authentification ou d'identification dépend de la finalité envisagée** et des circonstances dans lesquelles le système sera employé. Ce dernier ne doit pas être inutilement surdimensionné, c'est-à-dire disproportionné par rapport à la finalité première qu'il doit remplir.

Ainsi, dans un rapport récent[86], le comité consultatif de la convention 108 convient que **le contrôle des passeports peut avoir d'autres finalités légitimes que la simple authentification**. Si la finalité n'est pas uniquement de vérifier que l'utilisateur du passeport est le détenteur légitime mais également, par exemple, de contrôler que la personne concernée n'est pas sur une liste de personnes recherchées, l'identification est nécessaire. Cette finalité supplémentaire doit être explicitée pour qu'il soit possible de juger si le système d'identification choisi est nécessaire.

En somme**, il n'y a rien qui soit *a priori* interdit si les finalités le justifient**.

Une fois ce principe énoncé, **l'appréciation de ce qui est proportionné et de ce qui ne l'est pas est plus difficile**. Au travers de ses avis et autorisations, la CNIL a tenté de définir une graduation des moyens auxquels il est possible de recourir en fonction des buts recherchés. Elle admet le recours à la fonction d'identification si des exigences impérieuses en matière de sécurité ou d'ordre public existent.

Des difficultés peuvent se poser lorsqu'un traitement automatisé créé pour une finalité première est également utilisé pour une autre fin accessoire.

Comme on l'a vu, le Conseil constitutionnel autorise les utilisations multiples d'un fichier, à condition qu'elles ne revêtent pas un caractère excessif. De la même manière, la CNIL a nuancé son interprétation du principe de finalité. Elle a ainsi admis dans un avis rendu le 7 décembre 1998 que le fichier des personnes hospitalisées d'office tenu par les directions départementales de l'action sanitaire et sociale pouvait être consulté par les services de police dans le cadre de la procédure administrative d'autorisation d'un port d'arme.

Par un raisonnement assez proche, le comité consultatif de la convention 108 estime qu'il serait excessif et contraire au principe de proportionnalité d'exiger qu'un système employant des données biométriques soit plus perfectionné que ne le requiert la finalité première du traitement pour l'unique raison que, dans des cas exceptionnels, ces données pourraient être requises pour une finalité secondaire.

---

[86] *Rapport d'étape sur l'application des principes de la Convention 108 à la collecte et au traitement des données biométriques (février 2005. réf : T-PD (2005) BIOM F). La Convention 108 est le nom donné à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du Conseil de l'Europe.*

3. La création d'un fichier central : dangers et garanties

Il a été vu précédemment que le droit positif ne fixait pas de limites très claires entre ce qui est permis ou pas. Si le principe de proportionnalité interdit certaines choses, il exige surtout des garanties.

Les différents systèmes de titre d'identité électronique présentés dans ce rapport ne posent pas les mêmes difficultés au regard du principe de proportionnalité. L'appréciation de ce qui est excessif ou non par rapport à l'objectif de lutte contre la fraude est délicate. La jurisprudence du Conseil constitutionnel et celle de la Cour européenne des droits de l'homme manquent de précédents pour affirmer si certains systèmes de titre d'identité électronique sont contraires ou non aux normes constitutionnelles ou conventionnelles.

a) Vers un fichier central des Français ?

Les débats autour de la création d'un titre d'identité électronique, éventuellement obligatoire, ont fait ressurgir les craintes à propos de la constitution d'un fichier des Français.

Depuis la période de Vichy, la France n'a pas connu de projet de fichier national des Français à proprement parler. Depuis la réintroduction d'une carte nationale d'identité en 1955, et en dépit de nombreuses réformes et modernisations de ce document, aucun fichier des Français n'a été reconstitué. Seul un fichier de gestion de la carte nationale d'identité a été créé en 1986 pour la mise en œuvre de la nouvelle carte d'identité sécurisée.

Lors de leur audition, MM. Alain Weber, responsable de la commission Libertés et informatique à la Ligue des droits de l'homme, et Thierry Wickers, président de la Conférence des bâtonniers, se sont déclarés farouchement opposés à la constitution d'un fichier assimilable à un fichier des Français. Ils ont mis en exergue le risque de détournement de ce fichier.

Cette singularité française s'explique en grande partie par le poids de l'histoire. **De nombreux pays européens disposent d'un fichier de la population**. Lors de son déplacement en Belgique, une délégation de la mission d'information a constaté l'ampleur du registre de la population et la quantité des informations qui y sont rassemblées sur chaque individu.

Ce débat important et lourd de symbole doit toutefois être relativisé.

Comme le reconnaît la CNIL, il existe en France un fichier nominatif pas comme les autres : le Répertoire national d'identification des personnes physiques (RNIPP). **Plus qu'un fichier des Français, le RNIPP est un fichier de population.**

La CNIL est extrêmement réticente à son utilisation et s'est efforcée de la cantonner au domaine de la protection sociale. La loi subordonne d'ailleurs l'utilisation du NIR pour le compte de l'Etat à une autorisation par décret en Conseil d'Etat après avis motivé et publié de la CNIL[87].

Dans une délibération du 29 novembre 1983[88], la Commission a recommandé que l'emploi du NIR comme identifiant des personnes dans les fichiers ne soit ni systématique, ni généralisé et qu'en conséquence, chaque traitement automatisé soit doté d'identifiants diversifiés et adaptés à leurs besoins propres. La crainte est que le NIR devienne un identifiant unique rendant aisé l'interconnexion des fichiers.

Mais les reproches faits au RNIPP ne portent pas directement sur le fait que ce fichier est de facto un fichier de la population française. Ils portent sur les conditions dans lesquelles ce fichier est utilisé et sur le risque que le NIR serve d'identifiant universel.

Il est compréhensible que la création éventuelle d'un « fichier des Français » soulève des craintes. Mais, dans ce cas, la logique voudrait que le RNIPP soit modifié ou supprimé. Si les drames de l'histoire devaient se reproduire, nul doute qu'un pouvoir malintentionné se servirait du répertoire.

En conséquence et à supposer que le titre d'identité électronique soit rendu obligatoire, il semble que **le débat devrait moins se focaliser sur la création ou non d'un fichier national de gestion de ce titre, qui existe déjà, que sur les conditions et les limites de son utilisation**.

b) Encadrer les fonctions d'identification d'une base de données à caractère personnel

La création d'une base de données biométriques reliée à une base de données d'identité pour assurer l'unicité de la délivrance et du renouvellement des titres d'identité exige des précautions importantes. Les fonctions d'identification d'un tel fichier permettent l'utilisation des données pour d'autres fins que celle pour laquelle elles ont été collectées.

Si le choix se porte vers un système de bases de données qui ne permet pas de retrouver l'identité d'un individu à partir d'empreintes digitales, l'encadrement de l'utilisation d'un tel fichier pose peu de difficultés. L'architecture du fichier limite des utilisations abusives ou illégales. C'est particulièrement le cas du modèle dit à « lien faible » dont la conception rend impossible le rétablissement de liens en clair entre les

---

[87] *Article 27 de la loi du 6 janvier 1978 modifié. Lorsque l'utilisation du NIR ne se fait pas pour le compte de l'Etat, l'autorisation de la CNIL est nécessaire.*

[88] *Délibération n° 83-058 du 29 novembre 1983 portant adoption d'une recommandation concernant la consultation du Répertoire national d'identification des personnes physiques et l'utilisation du numéro d'inscription au répertoire.*

données d'identité et les données biométriques. Ce choix est irrévocable. En revanche, le modèle avec un lien cryptographique à sens unique de l'identité vers la biométrie laisse ouverte la possibilité de rétablir des liens en clair et, par voie de conséquence, d'utiliser le fichier à d'autres fins. Un arbitrage entre ces deux modèles doit prendre en compte cet effet cliquet.

Si le choix se porte vers un fichier d'identification forte, des précautions techniques et juridiques sont à prendre.

Techniquement, les données biométriques choisies ne doivent pas excéder ce qui est strictement nécessaire à la bonne exécution de la finalité première, c'est-à-dire garantir l'unicité de l'identité. Le respect du principe de proportionnalité le requiert. Cela signifie par exemple que les empreintes digitales relevées n'ont pas besoin d'être roulées mais seulement posées. Les empreintes roulées sont uniquement utilisées en police judiciaire. Ce point technique nuancerait certaines critiques considérant qu'un tel fichier d'identité équivaudrait à un fichier automatisé des empreintes digitales (FAED) généralisé à l'ensemble des Français.

Juridiquement, il faut arrêter précisément les circonstances et raisons qui justifient l'utilisation du fichier à des fins d'identification.

Une première utilisation possible est l'identification de victimes de catastrophe naturelle majeure, de personnes disparues ou amnésiques. L'exemple du tsunami en Asie a été évoqué par plusieurs des personnes entendues. Cette utilisation n'appelle pas de réserves particulières. La seule exigence est de s'assurer que la consultation du fichier est effectivement motivée par une de ces raisons. L'autorisation d'un magistrat apparaît néanmoins indispensable.

Une deuxième utilisation est l'identification de personnes à partir de leurs données biométriques, voire à partir de traces anonymes, à des fins de police judiciaire. En effet, en droit positif, un magistrat peut consulter n'importe quel fichier pour les besoins de l'enquête ou de l'instruction[89]. En cas de flagrance, un officier de police judiciaire y est aussi autorisé[90].

Plusieurs personnes, tout particulièrement MM. Alain Weber, responsable de la commission Libertés et informatique à la Ligue des droits de l'homme, et Thierry Wickers, président de la Conférence des bâtonniers, ont clairement exprimé leur opposition à la constitution d'un fichier biométrique, pouvant servir a fortiori à des fins d'identification judiciaire. M. François Giquel, vice-président de la CNIL, a jugé pour sa part que le principe de proportionnalité ne serait pas respecté.

---

[89] *Articles 77-1-1 et 99-3 du code de procédure pénale.*
[90] *Article 60-1 du code de procédure pénale.*

Pour la Ligue des droits de l'homme, il y aurait confusion entre ce fichier et le FAED. Plus encore, la Ligue s'oppose à la création pure et simple d'un fichier d'identification. Elle estime qu'une fois le fichier créé il sera impossible de revenir en arrière. Les garanties et limites arrêtées ne résisteraient pas longtemps aux tentations d'utiliser le fichier à des fins de police judiciaire. A l'occasion d'affaires criminelles médiatiques, il serait certainement reproché au législateur d'avoir retiré au magistrat un moyen d'enquête ou d'instruction peut-être déterminant. En somme, créer un fichier reviendrait à mettre le doigt dans un engrenage. Pour appuyer son propos, elle a évoqué l'exemple du fichier automatisé des empreintes génétiques dont le champ d'utilisation n'a cessé de s'accroître depuis sa création en 1998.

Doit-on dès lors interdire l'utilisation du fichier à des fins de police judiciaire ? Il s'agit d'une question de principe qu'il appartiendra au législateur de trancher. Si toutefois le choix effectué permettait de telles utilisations, plusieurs garde-fous seraient indispensables.

Tout d'abord, l'autorité judiciaire, gardienne de la liberté individuelle en vertu de l'article 66 de la Constitution, doit seule permettre l'utilisation du fichier à des fins de police judiciaire. **Aucune consultation du fichier à des fins d'identification ne devrait être possible sans autorisation d'un magistrat.**

Enfin, une règle de conduite modératrice devrait être suivie. La consultation du fichier ne serait autorisée qu'en motivant la demande et en indiquant qu'aucun autre moyen ne permettrait d'obtenir l'information utile. La consultation du fichier ne doit pas être une solution de facilité.

Une troisième utilisation, si le législateur l'autorisait, pourrait être la consultation de ce fichier par les services en charge de la défense des intérêts fondamentaux de l'Etat et de la lutte contre le terrorisme à des fins de renseignement.

Cette utilisation en dehors du contrôle du juge est problématique. Les auditions de MM. Pierre de Bousquet de Florian, directeur de la surveillance du territoire, et Marcel Faure, commissaire divisionnaire et chef de la division nationale de répression des atteintes aux personnes et aux biens, ont révélé la forte demande des services de renseignements et de police pour ce type d'utilisation. Au Royaume-Uni, le projet de carte d'identité prévoit que le directeur général des services de sécurité, le chef des services secrets ou le directeur général de l'Agence du crime organisé (équivalent de l'Office central pour la répression du banditisme) peuvent se voir communiquer les informations figurant dans le Registre national d'identité.

Cette utilisation du fichier nécessiterait des précautions toutes particulières si elle était admise.

D'une part, seules les personnes habilitées et individuellement désignées devraient pouvoir accéder au fichier.

D'autre part, un organisme indépendant sur le modèle de la Commission nationale de contrôle des interceptions de sécurité[91] pourrait être chargé de s'assurer du bien fondé des consultations du fichier. La CNIL pourrait remplir cet office et émettre des avis à l'occasion de chaque consultation du fichier.

c) Renverser les schémas classiques : observer Big Brother

Un titre d'identité électronique adossé à un fichier central demande une vigilance particulière pour déterminer les modalités et la durée de conservation des données, les conditions de leur mise à jour, les catégories de personnes habilitées à modifier et à consulter ces données et les conditions dans lesquelles les personnes intéressées peuvent exercer leurs droits d'accès et de rectification. Ces précautions en matière de protection des données personnelles sont habituelles.

Toutefois, le **passage à un titre électronique devrait être l'occasion d'innover réellement en matière de respect de la vie privée et de protection des données personnelles**.

En effet, **plusieurs principes restent souvent lettre morte** en dépit des efforts de la CNIL. Il en va ainsi de la **mise à jour** des données ou du **droit d'accès aux données et du droit à leur rectification**. Très peu de personnes exercent leurs droits en raison de la lourdeur apparente ou réelle des procédures. Ils restent théoriques.

La mise en place d'un titre électronique incluant une fonction d'authentification offre l'opportunité d'exercer réellement ces droits en ayant accès à ses propres données personnelles à distance. **En s'authentifiant grâce à la carte, chaque personne pourrait en temps réel contrôler les informations recueillies, leur exactitude ainsi que les consultations passées du fichier**.

Appliqué dans un premier temps au seul fichier des titres d'identité, ce dispositif pourrait être étendu à la quasi-totalité des traitements automatisés publics.

Lors de son déplacement en Belgique où le nouveau titre d'identité électronique prévoit cette application, la délégation de la mission

---

91 Autorité administrative indépendante, cette Commission émet un avis sur les autorisations d'interception de sécurité. Au cas où la Commission estime qu'une interception de sécurité a été autorisée en méconnaissance des dispositions du présent titre, elle adresse au Premier ministre une recommandation tendant à ce que cette interception soit interrompue. Voir la loi n° 91-646 du 10 juillet 1991.

d'information a pris conscience du bouleversement qu'un tel dispositif entraînerait. Comme l'a dit M. Luc Vanneste, directeur général de la direction des institutions et de la population, « *Big brother serait désormais surveillé par des millions de personnes* ». Ce renversement des rapports de force ferait de chaque individu le gendarme de ses propres données.

d) Renforcer les moyens de la CNIL

La CNIL souffre depuis longtemps d'un manque de moyens. Ils sont au moins inférieurs de moitié à ceux de ses homologues européennes et moins importants que ceux alloués à d'autres autorités administratives indépendantes françaises.

Dans son rapport sur la loi portant création de la Haute autorité de lutte contre les discriminations et pour l'égalité au nom de votre commission des Lois, votre rapporteur notait ainsi que le budget alloué à cette autorité administrative indépendante en 2005 était de 10.700.000 euros, celui du Médiateur de la République de 7.752.583 euros, celui du Conseil supérieur de l'audiovisuel de 32.476.075 euros, et celui de la CNIL de 7.675.748 euros seulement.

La création d'un titre d'identité électronique rendrait plus impérieux encore l'effort budgétaire réclamé à juste titre par son président, notre collègue M. Alex Türk, dans la mesure où les tâches de contrôle dévolues à la Commission augmenteraient considérablement, quel que soit le système retenu.

4. Garder la maîtrise des données et de leur diffusion

La loi du 6 janvier 1978 a inspiré l'ensemble des législations étrangères relatives à la protection des données personnelles. Deux préoccupations majeures l'ont guidée : contrôler la centralisation de données personnelles par l'Etat et limiter le développement de bases de données privées incontrôlables.

Près de trente ans plus tard, les enjeux ont évolué. L'Etat, dès lors qu'il est démocratique, n'apparaît plus comme le principal danger. Le nouveau défi consiste à **maîtriser l'expansion de bases de données privées et la diffusion désordonnée de ces informations vers des pays n'offrant pas les mêmes garanties en matière de protection des données personnelles** ou vers des acteurs non étatiques porteurs de menaces contre les libertés individuelles (organisations criminelles, entreprises privées, voire des individus).

L'Etat démocratique ne doit pas être nécessairement considéré comme un Leviathan ou un Big Brother. Face aux évolutions actuelles, **l'Etat**

doit user de sa puissance pour protéger ses citoyens contre l'évasion de leurs données personnelles.

A cet égard, le développement de la biométrie dans le monde entier impose à l'Etat de maîtriser ces technologies. La biométrie est en effet au croisement d'enjeux de défense, de sécurité, de liberté et de respect de la vie privée. Elle doit être considérée comme un secteur stratégique au même titre que les industries de défense et faire l'objet de la même attention.

Si la centralisation des données biométriques dans une base nationale soulève des interrogations légitimes, le problème est aussi et surtout leur circulation. De quel contrôle des données peut-on se prévaloir si celles-ci sont largement diffusées ?

Paradoxalement, ces réflexions peuvent plaider en faveur d'une centralisation des données biométriques par l'Etat. S'il ne le fait pas, le risque est grand que d'autres Etats le fassent à notre place en arguant que le niveau de sécurité de nos titres d'identité ou documents de voyage est insuffisant.

La politique américaine en ce domaine illustre parfaitement une telle attitude. Outre leur demande d'inclure rapidement des éléments biométriques dans les passeports, les Etats-Unis relèvent depuis bientôt un an les empreintes digitales et la photographie de l'ensemble des étrangers entrant sur leur territoire. A terme, ce fichier comportera plusieurs centaines de millions d'individus, les données biométriques étant conservées 75 ans. En poussant à l'extrême la logique de ce dispositif, les passeports nationaux n'auront bientôt plus qu'une valeur relative par rapport à cette base de données.

Le système européen de visas biométriques en cours d'élaboration obéit à une logique assez similaire.

Face à ce risque de perte de contrôle des données, deux points méritent un développement particulier.

a) Sécuriser les données

Aucun système informatique n'est infaillible. **Les systèmes utilisés devraient donc faire l'objet d'audit et d'évaluation réguliers**, le cas échéant sous la direction de la CNIL, afin de maintenir un niveau très élevé de sécurité.

b) La puce sans contact

La technologie d'identification par radiofréquence, appelée RFID, permet à un lecteur de récupérer à une distance de quelques centimètres à quelques mètres des informations stockées dans une micropuce, grâce à une antenne imprimée en filigrane.

L'industrie du « sans contact » est en plein essor. Le marché mondial de la RFID pourrait tripler dans les trois prochaines années pour atteindre 5,5 milliards d'euros en 2008. Surtout utilisée dans les activités de logistique (gestion des stocks, de l'acheminement...), cette technologie pourrait s'étendre à de nouveaux domaines.

D'ores et déjà, **cette technologie inquiète les défenseurs du respect de la vie privée**, qui redoutent de voir les consommateurs espionnés par un mouchard. La CNIL est attentive à son développement.

Dans le cadre de la mise en place de titres d'identité ou de voyage électroniques, l'utilisation du « sans contact » a été étudiée. Elle permettrait de lire un passeport par exemple sans qu'il soit nécessaire de le sortir pour le présenter devant un lecteur. La gestion des flux à la frontière, notamment dans les aéroports, serait fluidifiée. Cette solution a également été envisagée par le projet INES.

Plusieurs problèmes importants requièrent de la prudence avant d'intégrer cette technologie aux pièces d'identité.

D'une part, plusieurs personnes entendues ont souligné les **risques de captation des données à l'insu du porteur**. Une grande incertitude règne en la matière. La sensibilité des données contenues dans la puce, avec ou sans biométrie, interdit de choisir une telle solution pour des raisons de simple confort. Comme il a été vu, une présence humaine doit être maintenue lors du contrôle des titres pour des raisons de sécurité et de fiabilité.

Les partisans de cette technologie répliquent qu'il serait possible de protéger les passeports par un écran métallique dans la couverture et un code qui n'est lisible qu'en ouvrant le passeport. Mais dans ce cas, l'intérêt du « sans contact » s'évanouit puisqu'il faut manipuler le passeport.

D'autre part, la lecture des titres à distance pourrait être le fait des autorités publiques. **Les personnes seraient contrôlées à leur insu sans qu'il soit procédé à un contrôle d'identité individualisé**. L'ensemble des règles relatives aux contrôles, aux vérifications et aux relevés d'identité[92] pourrait s'en trouver bouleversé.

Il apparaît donc prématuré de recourir à cette technologie qui n'offre pas les garanties nécessaires en matière de protection des données.

*

* *

[92] *Articles 78-1 à 78-6 du code de procédure pénale.*

CONCLUSION

La mission a été directement confrontée à la recherche de l'équilibre entre la protection des libertés individuelles et la sécurité de l'identité.

Deux réflexions ont guidé son travail.

D'une part, la sécurisation de l'identité n'est pas antinomique de la sauvegarde des libertés. Protéger l'identité d'un individu, c'est protéger les droits attachés à sa personne, que ce soit le droit de propriété ou la liberté d'aller et venir. Protéger l'identité, c'est aussi sécuriser les relations contractuelles. Si le système d'identité est altéré, les conditions de la confiance ne sont plus réunies de la même façon que la fausse monnaie porte atteinte à la confiance dans le système monétaire.

D'autre part, il faut se garder de sacrifier la liberté au nom de la sécurité et rester conscient qu'un système parfait n'existe pas. L'objectif raisonnable que les autorités publiques doivent se fixer est de contenir la fraude dans ses proportions acceptables en évitant les solutions excessives qui pourraient conduire à transformer un système d'identité en un système de contrôle et de police. De là à invoquer, comme certains interlocuteurs de la mission, au nom de la période de l'occupation, un droit à la dissimulation d'identité, il y a un pas qui reste difficilement franchissable en régime démocratique.

Les enjeux sont tels que M. Nicolas Sarkozy, ministre d'Etat, ministre de l'intérieur et de l'aménagement du territoire, a souhaité prendre le temps de la réflexion avant de mettre en œuvre le projet d'identité nationale sécurisée. Il a ainsi déclaré devant les préfets, le 20 juin 2005, que : « *Ce chantier a fortement évolué ces derniers mois. Il va impacter en profondeur et durablement la vie quotidienne des Français. Or, si des dispositions européennes nous obligent à mettre rapidement en œuvre un passeport biométrique, il n'en va pas de même pour la carte d'identité électronique. Je ne veux donc pas qu'on s'y engage sans avoir pris le temps nécessaire pour réfléchir à toutes ses conséquences. Il ne s'agit pas de revenir sur des évolutions qui sont pour certaines nécessaires, mais de bien mesurer où l'on veut aller, sous quelles conditions et à quel prix*. »

La mission d'information estime pour sa part que la question essentielle réside moins dans le principe que dans les modalités de l'introduction de titres d'identité électroniques. De nombreux Etats l'ont d'ores et déjà décidé ou l'envisagent. Les Etats-Unis relèvent les empreintes digitales des étrangers entrant sur le territoire américain et les conservent soixante-quinze ans. La France doit prendre toute sa part dans la réflexion sur les utilisations de la biométrie, sous peine de se voir imposer les solutions des autres. Les progrès technologiques ne doivent pas être redoutés mais utilisés afin que le renforcement de la sécurité et la protection des libertés se soutiennent mutuellement.

La rencontre entre biométrie et informatique démultiplie la puissance de cette technique d'identification et contribue à faire du dossier INES un projet majeur de ce début du XXIème siècle. La qualité du débat qui s'est instauré, tant avec des citoyens initiés qu'avec le grand public, notamment dans le cadre du Forum des droits sur l'Internet, la volonté gouvernementale d'approfondir à la lumière de ce débat ses réflexions sur le projet INES, la continuité de ce dossier avec le titre fondateur que souhaitait mettre en place le gouvernement de M. Lionel Jospin, permettent d'espérer aboutir à des solutions largement consensuelles.

Réunie le mercredi 29 juin 2005, la commission a autorisé la publication du présent rapport.

OBSERVATIONS DE MME ALIMA BOUMEDIENE-THIERY ET M. RICHARD YUNG
SÉNATEURS SOCIALISTES

Nous partageons les hypothèses et les scénarios qui sont présentés dans le rapport de la Mission d'information de la Commission des Lois sur la nouvelle génération de documents d'identité et la fraude documentaire.

Toutefois, nous souhaitons mettre en exergue certains points qui font débat.

Officiellement, le programme INES vise à simplifier les démarches administratives en permettant notamment à l'usager porteur de la carte de signer électroniquement des documents et d'accéder à des télé-procédures. Cependant, les intentions gouvernementales semblent être principalement d'ordre sécuritaire. En effet, selon le gouvernement, la nouvelle CNI, si elle était obligatoire, permettrait de combattre l'usurpation d'identité et de lutter plus efficacement contre le terrorisme. Néanmoins, nous pensons que sur ce dernier point l'efficacité serait faible dans la mesure où les terroristes ont les moyens de disposer de documents authentiques.

On peut aussi sérieusement douter de l'efficacité de la carte nationale d'identité électronique car ce nouveau titre d'identité n'empêchera pas non plus la fraude documentaire. Bien au contraire, il n'est pas certain que le coût exorbitant de la mise en œuvre de cette carte (estimé à plus de 200 millions d'euros par an) sera inférieur à celui de la fraude. Préalablement à toute réforme, des études quantitatives doivent donc être menées afin de déterminer la véritable ampleur de l'usurpation d'identité en France.

D'autre part, la nouvelle carte d'identité électronique risque de porter très gravement atteinte à certains droits fondamentaux et libertés publiques malgré les garanties proposées par le gouvernement. Le débat en la matière doit donc être poursuivi.

Il ne faut pas non plus que la CNIE contribue à l'émergence de nouvelles fractures territoriales. En effet, pour des raisons de coûts, de sécurité et de charge de travail pour les petites collectivités locales, l'avant projet de loi envisage de concentrer l'émission et la délivrance de la nouvelle carte d'identité sur environ 340 mairies (4.000 à terme). Les autorités gouvernementales doivent donc être à l'écoute des maires d'environ 32.000 petites communes qui se verraient dépossédés de l'état civil.

Nous recommandons donc au gouvernement de poursuivre et d'élargir le débat qui a été initié. Pour ce faire, il doit se baser sur les avis du Forum des droits de l'Internet et prendre en considération les craintes déjà exprimées par certains de nos concitoyens. L'Etat ne doit pas non plus

négliger les solutions alternatives et les recommandations du rapport de notre mission d'information. De même, une réflexion nationale sur les autres usages – notamment les applications privées – de la CNIE doit être organisée.

Nous exigeons également du gouvernement qu'il tienne compte de l'avis de la Commission Nationale de l'Informatique et des Libertés, qui sera rendu prochainement, car le respect de la vie privée doit être à la base de toute réforme de la carte nationale d'identité.

A l'instar du Parlement Européen, les socialistes sont fermement opposés à la création de fichiers centralisés ainsi qu'à l'interconnexion des bases de données. Néanmoins, si un fichier devait être constitué, les citoyens devraient pouvoir le consulter, savoir qui l'a consulté et, le cas échéant, rectifier d'éventuelles erreurs.

En outre, afin de prévenir toute dérive policière, la lecture « sur place » des données contenues dans la puce devrait être privilégiée par rapport à la « lecture à distance », prévue dans l'avant-projet de loi. Toutefois, nous recommandons aussi d'étudier plus en détail le système de base à « lien faible ».

De même, il faut poursuivre le débat sur la question de savoir si la nouvelle carte d'identité doit rester gratuite et facultative. Avant de réformer la CNI, il faut s'assurer que le nouveau document permettra de justifier son identité sans banaliser le contrôle d'identité dans notre pays.

Certes, les Sénateurs socialistes ne remettent aucunement en cause l'existence de la CNI car, comme le dit Pierre PIAZZA, « la carte nationale d'identité est un instrument d'identification qui matérialise une appartenance commune à la nation »93. Cependant, les possibilités offertes par la modernité ne doivent pas être un prétexte pour instituer un titre d'identité dont l'essence serait profondément policière. Le principe de proportionnalité doit donc guider cette réforme, qui ne doit pas relever du seul Ministère de l'Intérieur. Un véritable débat social et politique doit être à présent engagé.

Enfin, les Sénateurs socialistes prônent une réforme de l'état civil afin de réduire le risque de fraude et réclament une meilleure « sécurisation » du permis de conduire et du passeport.

---

[93] *Propos recueillis par Stéphane FOUCART, Le Monde, 17 juin 2005.*

ANNEXE

AUDITIONS ET DÉPLACEMENTS DE LA MISSION

1. Auditions

Mercredi 16 février 2005

Université de Paris-Panthéon-Assas

M. Christophe NAUDIN,	chargé de recherche au département « menaces criminelles contemporaines de l'Institut de criminologie »

Mardi 1er mars 2005

Ministère des affaires étrangères

M. François BARRY-DELONGCHAMPS,	directeur des Français à l'étranger et des étrangers en France
Mme Françoise LE BIHAN,	chef du service des Français à l'étranger
M. Serge MUCETTI,	sous-directeur de l'administration consulaire et de la protection des biens

Ministère de l'intérieur

M. Daniel CANEPA,	secrétaire général
M. Bernard FITOUSSI,	directeur des systèmes d'information et de communication, ancien directeur du programme INES
M. Bernard SCHMELTZ,	sous-directeur des étrangers et de la circulation transfrontières

Mardi 15 mars 2005

Commission nationale de l'informatique et des libertés (CNIL)

M. François GIQUEL,	vice-président
M. Philippe LEMOINE,	membre
Mme Sophie VUILLIET-TAVERNIER,	directeur des affaires techniques

Services du Premier ministre

M. Philippe WOLF,	responsable du centre de formation de la direction centrale de la sécurité des systèmes d'information

Ministère des affaires étrangères

M. Daniel LABROSSE,	chef du service central de l'état-civil

Ministère de la justice

M. Marc GUILAUME, directeur des affaires civiles et du sceau

Mercredi 16 mars 2005

Office parlementaire d'évaluation des choix scientifiques et technologiques

M. Christian CABAL, député de la Loire, membre de l'Office, auteur d'un rapport sur « *les méthodes scientifiques d'identification des personnes à partir de données biométriques et les techniques de mise en œuvre* »

Ministère de la justice

M. Philippe LAGAUCHE, directeur-adjoint auprès du directeur des affaires criminelles et des grâces

Ministère de l'intérieur : direction centrale de la police aux frontières

Mme Elisabeth RUMI, commissaire principal, chef du bureau de la fraude documentaire

M. Pierre GARCIA, capitaine

Ministère de l'intérieur : direction centrale de la police judiciaire

M. Marcel FAURE, commissaire divisionnaire, chef de la division nationale de répression des atteintes aux personnes et aux biens

Mardi 22 mars 2005

Secrétariat général du Comité interministériel pour les questions de coopération économique européenne (SGCI)

M. Patrick DELAGE, préfet, secrétaire général adjoint pour les affaires intérieures et de justice

Mme Ghislaine TERRIER, chef du secteur « libre circulation des personnes »

Observatoire national de la délinquance

M. Alain BAUER, président du conseil d'orientation

Mardi 29 mars 2005

Ministère de l'intérieur : direction de la surveillance du territoire

M. Pierre de BOUSQUET de FLORIAN, préfet, directeur de la surveillance du territoire

Mme Annie GASTELLIER, commissaire divisionnaire en charge des affaires juridiques

Banque de France

M. Christian NOYER, gouverneur de la Banque de France, président de l'Observatoire de la sécurité des cartes de paiement

M. Denis BEAU, directeur adjoint auprès du directeur général des opérations de la Banque de France

Société THALES SECURITY SYSTEMS

M. Pierre MACIEJOWSKI, directeur général

M. Philippe DUSAUTOIR, directeur du domaine « identification, logique, solutions et solutions NRBC (Nucléaire, Radiologique, Bactériologique et Chimique) »

M. Patrick NOUVEL, directeur technique

Mardi 5 avril 2005

Conférence des bâtonniers

M. Thierry WICKERS, président

Conseil national des barreaux

M. Gérard TCHOLAKIAN, membre de la Commission libertés et droits de l'homme

Barreau de Paris

Mme Jeanine MULLER-JACQUOT, avocat au barreau de Paris

Société de biométrie humaine

M. Emmanuel-Alain CABANIS, président, professeur des universités, chef du service de neuro-imagerie au centre hospitalier national d'ophtalmologie des Quinze-vingts

Mme Yvette DELOISON, secrétaire général

Mercredi 6 avril 2005

Ligue des droits de l'homme

Mme Monique HEROLD,	vice-présidente, responsable du groupe de travail sur la bioéthique ;
M. Alain WEBER,	responsable de la commission libertés et informatique
M. Pierre SUESSER,	responsable de l'intercollectif droits et libertés face à l'informatisation de la société

Groupement des cartes bancaires

M. Jean-Pierre BUTHION,	responsable du département « produits et services »
Mme Martine BRIAT,	directeur des affaires juridiques et bancaires

Mardi 12 avril 2005

Institut national des hautes études de sécurité (INHES)

M. Pierre PIAZZA,	chargé de recherche

Commission internationale de l'état civil (CIEC)

M. Paul LAGARDE,	secrétaire général

Mardi 17 mai 2005

Société SAGEM

M. Bernard DIDIER,	directeur du développement

Mercredi 1er juin 2005

Institut national de la statistique et des études économiques (INSEE)

M. Guy DESPLANQUES,	responsable du département « démographie » à la direction des statistiques démographiques et sociales

Institut national des télécommunications (INT)

Mme Bernadette DORIZZI,	professeur, chef du département électronique et physique

Agence pour le développement de l'administration électronique (ADAE)

M. Jacques SAURET,	directeur

Centre d'études et de recherches internationales (CERI)

M. Didier BIGO,	chercheur

2. Déplacements

Mercredi 9 mars 2005

Eragny (Val-d'Oise)

Centre de recherche de la SAGEM

M. Bernard DIDIER, directeur du développement

et les membres de son équipe

Jeudi 17 mars 2005

Lyon

INTERPOL

M. Jean-Michel LOUBOUTIN, directeur exécutif des services de police

et les experts placés sous son autorité

Tribunal de grande instance de Lyon

M. Xavier RICHAUD, procureur de la République

Mme Danielle GIRARD-ZAMPINO, vice-présidente, présidente de la première chambre civile

Mme Christiane POLI-DAUCHELLE, procureur-adjoint, responsable de l'état civil

Lundi 11 avril 2005

Paris

Forum des droits sur l'Internet : Débat national sur la carte d'identité électronique

Du lundi 25 au mercredi 27 avril 2005

Washington

Congrès

M. James F. SENSENBRENNER,	président de la commission judiciaire de la Chambre des représentants

Department of State

Mme Maura HARTY,	« US Assistant secretary » pour les affaires consulaires du département d'Etat

Department of Homeland Security (DHS)

M. Bob MOCNY,	directeur adjoint du programme US-Visit

Ambassade de France

M. Jean-Pierre ALLEX-LYOUDI,	consul général de France

Visite d'un laboratoire scientifique d'Etat (expertise de documents contrefaits)

Visite de l'aéroport international de Baltimore-Washington (BWI)

Mercredi 11 mai 2005

Val Maubué

Centre national de production des titres

M. Louis PUCHEU,	chef du service central des systèmes de communication et d'information (SCSCI)
M. Alain CANOVAS,	adjoint auprès du chef du service central du SCSCI
M. Jean-Jacques BRETIN,	chef de centre
M. Franck TOURRETTE	adjoint du chef de centre

Jeudi 12 mai 2005

Bruxelles et Woluwe-Saint-Pierre

Ministère de l'intérieur : direction générale « institutions et population »

M. Luc VANNESTE,	directeur général
Mme Christiane ROUMA,	conseillère technique, responsable du registre national
M. Denis VAN MELSEN,	chef de projet CIE
M. Luc SMET,	conseiller général
M. Ronny DEPOORTERE,	senior vice-président de la société ZETES

M. Willy DERETTE, représentant de la société STERIA

Commune de Woluwe-St-Pierre, commune du Grand Bruxelles (examen des modalités pratiques de délivrance de la carte d'identité)

Mme VAEYE, directrice du service de la population

M. VAN VLIEBERKE, directeur de l'informatique

3. Contribution écrite de l'Association des maires de France (AMF)