

DEBAT NATIONAL SUR LA CARTE D'IDENTITE ELECTRONIQUE

Comptes rendus des débats publics itinérants

- I.** Première étape du débat public itinérant à **Bordeaux, le 8 mars 2005**
- II.** Deuxième étape du débat public itinérant à **Lyon, le 31 mars 2005**
- III.** Troisième étape du débat public itinérant à **Paris, le 11 avril 2005**
- IV.** Quatrième étape du débat public itinérant à **Lille, le 27 avril 2005**
- V.** Cinquième étape du débat public itinérant à **Rennes, le 11 mai 2005**
- VI.** Sixième étape du débat public itinérant à **Marseille, le 25 mai 2005**

*

Première étape du débat public itinérant

Bordeaux, le 8 mars 2005

La première étape du débat public qu'organise le Forum des droits sur l'internet autour du projet de carte d'identité électronique s'est tenue le 8 mars 2005 à Bordeaux.

Autour de Madame Falque-Pierrotin, présidente du Forum des droits sur l'internet intervenaient cinq personnalités : Marcel Desvergues, Président d'Aquitaine Europe Communication, Patrick Nouvel, Directeur commercial domaine identitaire Thales Security System, Jean Péringuey, Président de la communauté de commune de Villandraut et maire de Noaillan, André Vitalis, Directeur du Centre d'Etude des médias Université Michel de Montaigne Bordeaux III, Thierry Wickers, Avocat, Président de la Conférence des Bâtonniers.

La Délégation programme INES (Identité Nationale Electronique Sécurisée) du ministère de l'Intérieur était représentée par Sophie Planté, adjointe au directeur et Fabrice Mattatia, ingénieur en chef des Télécoms.

La séance a été animée par Jean Gonié, juriste au Forum des droits sur l'internet.

Les interventions et les échanges avec la salle ont abordé les points suivants :

1. Sur l'expérimentation menée en Gironde sur la délivrance de carte nationale d'identité électronique en mairie.

1.1 AEC a mené en 2004 avec la préfecture de Gironde une expérimentation « sur la station d'acquisition en mairie » de la carte d'identité électronique. Thales Security System a été le fournisseur de la borne de saisie. Pour MM. Desvergues, Nouvel et Péringuey la saisie des cartes et la prise d'empreintes ont bien fonctionné. De plus, un certain climat de confiance s'est instauré. Les manipulations nécessaires pour la prise d'empreintes ont été bien acceptées. Il a été noté que parmi les personnes ayant participé à l'expérimentation, très peu se sont interrogés sur les dérives possibles de l'utilisation de la biométrie et sur un éventuel « fichage ». De façon générale, la carte est

apparue comme apportant une réponse plus sûre que l'actuelle carte. M. Péringuey a précisé que le risque de fichage est lié à ce que l'on met comme données dans la carte ; à cet égard il souhaite que la carte contienne le minimum de données et surtout pas celles liées à la santé. Il a été précisé par le ministère de l'intérieur que les données de santé et à caractère sanitaire et social ne seront pas dans la CNIE, qu'une telle disposition serait en tout état de cause inconstitutionnelle.

1.2. M. Péringuey, en tant que président d'une communauté de communes où les mairies ont 400 habitants en moyenne, a insisté sur le fait que la mise en place de la CNIE ne doit pas diminuer l'offre de services publics locaux ; que notamment les citoyens sont très attachés à une carte nationale d'identité électronique délivrée dans un service de proximité. A cet égard, il convient qu'en milieu rural la carte soit délivrée par le biais d'une borne itinérante allant dans chaque mairie. Il a également insisté sur la nécessité de maintenir le caractère gratuit de la carte.

1.3. Il a été demandé comment il était possible de recréer une bonne qualité d'environnement photographique (éclairage, fond blanc) dans les mairies par le biais des bornes mobiles (à la différence des « photomats »). A cela M. Nouvel a précisé que Thales travaille actuellement à recréer un environnement favorable par le biais d'un ensemble adaptable pour les mairies (logiciel et matériel).

2. Sur les risques de dérives dans l'utilisation d'un fichier centralisé des empreintes digitales numérisées.

2.1. M. Vitalis et Me Wickers ont précisé que la mise en place d'une CNIE comportait un certain nombre de risques tant en termes de fichage des individus que d'utilisation de la biométrie. Il a été rappelé que l'Histoire est riche d'exemples de fichage des individus et des dérives qui s'ensuivent (Vichy, les Pays-Bas en 1940) et qu'une gestion centralisée des individus par l'Etat est source potentielle de dangers. A cet égard, beaucoup ont souhaité que ne soit pas créé, au nom de la sécurité, une base centralisée d'empreintes digitales numérisées. Pour ce faire, les données numérisées devraient être « embarquées » dans la puce de la carte.

2.2. L'utilisation de la biométrie, en tant que technique, a été discutée. Il a ainsi été avancé que les systèmes biométriques sont générateurs d'erreurs : le contrôle par empreintes digitales connaît un taux de réussite à l'aéroport d'Heathrow (Royaume-Uni) de 99,9%, ce qui génère néanmoins 100 à 200 erreurs par jour. Il est également rapporté que, selon le groupe de l'article 29 (les CNIL européennes), les experts en biométrie faciale notent un taux d'erreur de l'ordre de 40%.

2.3. Le ministère de l'intérieur a souhaité préciser deux choses. D'une part, que les titres d'identité relèvent du domaine réglementaire : par conséquent, le ministère pouvait se passer de l'avis du Parlement et ne pas présenter un projet de loi. Le choix a justement été fait de présenter un projet de loi pour qu'un débat démocratique et ouvert s'engage sur ce sujet important. D'autre part, il a précisé que la projet de CNIE était distinct du projet de passeport biométrique sur lequel le gouvernement a peu de marge de manœuvre compte tenu des engagements européens ; en conséquence, selon ce qu'exprimeront les Français sur la configuration de la carte, les choix publics pourront être différents de ceux rendus sur le passeport. Le ministère a cependant précisé que les moyens de production de la carte et du passeport devraient être mutualisés afin de rendre possible une baisse des coûts.

2.4 Concernant la base centrale, le ministère a précisé que le projet INES n'est pas un projet de police mais un projet portant sur l'identité, il n'y a donc pas selon lui de risque de changement de finalité. Les questions liées à l'informatisation de l'état-civil relèvent de la compétence du ministère de la justice ; elles sont en cours d'examen. Enfin, le ministère a précisé que des fichiers de photographies et d'empreintes existent déjà sous

une forme décentralisée : la nouveauté du projet INES serait de les centraliser et de les numériser. La mise en place d'une base centralisée permettrait également aux services d'agir de manière plus transparente via un système d'habilitations très contrôlé.

2.5 Un débat s'est noué sur les rôles respectifs de l'Etat et des acteurs privés par-rapport à la mise en place d'une CNIE. Le ministère a réaffirmé que c'était à l'Etat et non à des acteurs privés de certifier les identités, quelque que soit la sphère d'usage de celles-ci; certains se sont interrogés sur les conséquences d'une identité unique gérée par l'Etat ; d'autres, enfin, ont estimé nécessaire que le partenaire industriel ait un rôle strictement défini et demandé des garanties en ce sens.

3. Sur les risques de piratage informatique et d'usurpation d'identité

3.1. Il a été rappelé que les risques d'attaques/piratages informatiques existent car aucun système informatique n'est fiable à 100%. A ce titre, la possibilité de voter par le biais de la carte semble, pour l'instant, dangereux (attaques contre le système, atteinte à la confidentialité du vote, usurpation d'identité....).

3.2. Il a été rappelé que la gestion de l'identité à l'ère du numérique doit être observée avec la plus grande prudence. Me Wickers a rappelé qu'une entreprise américaine (ChoicePoint) s'est récemment fait voler 145.000 « identités » (numéros de sécurité sociale, permis de conduire...) de clients dont elle avait la charge. Il a également noté que seulement trois pays dans le monde gèrent les empreintes digitales pour délivrer les titres d'identité : Le Nigéria, la Malaisie et le Kosovo...

3.3. De façon générale, des craintes se sont également exprimées autour des risques d'utilisation frauduleuse de la carte, de copie de la carte et de lecture/accès non autorisé des données de la carte.

3.4. Face au risque d'usurpation d'identité évoqué par un intervenant, le ministère de l'intérieur a souligné que seule une base centrale permettrait de lutter contre les usurpations d'identité et d'éviter la délivrance à une même personne de titres sous plusieurs identités différentes.

4. Sur les usages et le coût de la carte

4.1. Un grand nombre de participants a souhaité que la CNIE serve uniquement à certifier son identité, à l'exclusion des autres usages.

4.2. Il a été souligné que l'instauration d'une carte d'identité électronique engendrera un coût pour la collectivité ainsi que des problèmes d'équipement (lecteurs de cartes) et d'accès. De façon générale le souhait se porte sur la gratuité de la carte (important en termes d'acceptation et d'insertion surtout pour les catégories défavorisées) et pour son accessibilité pour tous (borne ambulante, notion de service public). M. Nouvel a précisé que si la carte propose des services associés, le secteur privé y trouverait une source de revenus et, de ce fait, prendrait en charge une partie des coûts.

4.3 Certains ont souhaité que la CNIE soit accessible sous tous les systèmes et qu'il soit prévu d'utiliser des standards ouverts et libres.

5. sur le principe et l'utilité du débat public

5.1 Beaucoup de questions ont porté sur le processus d'organisation du débat et sur l'utilisation qui sera faite de ses conclusions par le gouvernement. Certains ont également insisté sur la nécessité pour les institutions concernées par le sujet de se mobiliser et de faire part de leurs interrogations.

5.2 Le ministère a rappelé que le projet n'était pas bouclé et que le gouvernement souhaitait recueillir l'avis des Français sur ce dossier avant de le finaliser. Il a été précisé par le Forum des droits sur l'internet que cette consultation n'avait pas de valeur statistique mais une valeur qualitative et que, dans ces matières et compte tenu des enjeux importants de libertés et d'usages, il était important de travailler aussi avec les non-experts. Le FDI a précisé qu'il allait dans les prochains jours réorganiser le débat en ligne pour lui donner plus de lisibilité pour les internautes.

* * *

Deuxième étape du débat public itinérant

Lyon, le 31 mars 2005

La deuxième étape du débat public qu'organise le Forum des droits sur l'internet autour du projet de carte d'identité électronique s'est tenue le 31 mars 2005 à Lyon, au sein de l'Université Lyon II.

Autour de Madame Falque-Pierrotin, présidente du Forum des droits sur l'internet intervenaient quatre personnalités : Yves Bismuth, Avocat, Président d'honneur de l'Association Française du Droit de l'Informatique et de la Télécommunication, Pierre Piazza, chargé de recherche à l'Institut National des Hautes Études de Sécurité, Gilbert Puech, Président de l'Université de Lyon II, Alain Risson, maire de Gluiras et responsable du groupe de travail « Nouvelles technologies » de l'Association des Maires de France.

La Délégation programme INES (Identité Nationale Electronique Sécurisée) du ministère de l'Intérieur était représentée par Sophie Planté, adjointe au directeur.

La séance a été animée par Jean Gonié, juriste au Forum des droits sur l'internet

Les interventions et les échanges avec la salle ont abordé les points suivants :

A titre liminaire il convient de préciser qu'une action d'opposition au projet de carte s'est manifestée avec le déclenchement d'une alerte incendie (fumigènes disséminés dans l'université) et la présence d'affiches dans les locaux de l'université après le début du débat. Cette action a entraîné la suspension momentanée du débat.

Les affiches n'ont pas été signées. Elles portent sur un certain nombre de questions qui reflètent celles posées régulièrement lors des débats : la question de la mise en place d'une « *base de données centrale des empreintes digitales* », l'accès aux données tendra-t-il « *à se généraliser en dehors du contexte d'un « simple » contrôle d'identité* » ? « *Jusqu'où sommes nous prêts à aller dans le fichage au nom d'une soi-disante « protection » ? Qui veut-on protéger et de quoi ?* ».

1. Sur la justification d'une carte nationale d'identité électronique

1.1. M. Piazza s'interroge sur les deux raisons principales avancées par les pouvoirs publics pour justifier la mise en place d'une CNIE : la lutte contre le terrorisme et contre la fraude à l'identité. Sur ces deux points il constate un déficit d'explication qui contribue d'ailleurs à nourrir des craintes et à brouiller les enjeux.

* L'argument selon lequel la biométrisation des titres d'identité constitue une solution pour lutter contre le terrorisme mériterait d'être davantage explicité : un tel dispositif permettra-t-il vraiment de repérer un primo-terroriste ? Ne peut-on pas envisager des cas où quelqu'un obtienne en toute légalité une CNIE et soit pour autant amené à commettre un acte terroriste ? Plus généralement, l'État a-t-il véritablement besoin de ce type de dispositif ?

* L'argument selon lequel la CNIE permettrait de diminuer les coûts liés à la fraude identitaire n'est fondé que sur des études étrangères (principalement américaines ou britanniques) et aucune étude systématique n'a été conduite en France. Dès lors, il se demande s'il est possible de se référer aux chiffres avancés dans des pays étrangers alors que les instruments et dispositifs d'identification qui y sont employés ne sont pas du tout les mêmes que ceux mobilisés en France (par exemple, pour les États-Unis : surtout

le numéro de sécurité sociale et le permis de conduire et pour le Royaume-Uni l'inexistence de carte nationale d'identité depuis 1952).

* Enfin, M. Piazza s'interroge également sur les coûts induits par la mise en place de la biométrie ; aucune information n'étant donnée à ce sujet par le ministère.

A cette argumentation le ministère a précisé que :

* La fausse identité (ou l'usurpation) est souvent à la base du phénomène terroriste et qu'en ce sens, toute action destinée à rendre plus fiable l'identité des citoyens est un moyen de lutter contre les atteintes à la sécurité publique.

* Seuls les ministères des finances et des affaires sociales seraient à même d'établir le coût de la fraude, ce qui n'est pas encore fait. Il précise cependant que depuis que la carte d'identité est gratuite le taux de perte a été multiplié par plus de dix (36.000/an en 1998, plus de 500.000 actuellement), ce qui a un coût pour la collectivité.

1.2. De façon générale, il a été remarqué une absence de coordination entre les différents projets des ministères (CNIE, carte de vie quotidienne, changement d'adresse...) qui donne une impression générale de confusion dans les initiatives.

2. Sur les risques en matière de vie privée et sur l'accès aux données

2.1. M. Bismuth, constatant une actuelle banalisation du contrôle biométrique et une croissance de son acceptation, craint que par ce biais les citoyens abandonnent progressivement des libertés sans même s'en apercevoir. Le projet de CNIE doit donc être entourée de nombreuses garanties (impossibilité d'interconnexions, principe de proportionnalité, le détenteur de la carte doit avoir accès aux données) et ne doit pas se faire au détriment des libertés individuelles. M. Bismuth fait deux propositions. Tout d'abord, il souhaite que la loi instaure officiellement un « *Habeas Data* » qui protégerait officiellement les droits du citoyen à l'ère du numérique. Ensuite, il propose que soit instauré un « *principe de précaution pour les données personnelles* ». A ses yeux, la CNIL ne pouvant vérifier tous les fichiers, la protection des données personnelles doit faire l'objet d'actions de prévention pour faire face à des risques éventuels de dérives à l'instar de ce qui a été mis en place pour l'environnement.

2.2. M. Piazza a rappelé que le débat autour de la carte d'identité électronique comporte beaucoup de fantasmes et de craintes à cause de l'origine historique de « l'encartement » des individus lié à des pratiques de surveillance de catégories de personnes stigmatisées comme déviantes ou dangereuses (le livret ouvrier sous l'Empire, le carnet anthropométrique des nomades sous la IIIe République...). De plus, la carte d'identité a pu servir d'instrument pivot afin d'« épurer » la communauté nationale (apposition de la mention « Juif » sur les cartes d'identité durant l'Occupation). Plus récemment, le durcissement des procédures de contrôle de la domiciliation et de la nationalité (avec la carte nationale d'identité sécurisée généralisée au cours des années 1990) a encore pu avoir des répercussions non négligeables sur les SDF ou les Français naturalisés, nés en France de parents étrangers, ceux nés dans un territoire français ayant ensuite accédé à l'indépendance, etc.

2.3. M. Piazza remarque également que l'appréciation des risques en matière de protection des données (création d'une base centralisée, identifiant unique, interconnexions etc.) dépend des dispositifs législatifs et de la culture dans ce domaine de chaque pays. Par conséquent, vouloir établir une stricte comparaison des risques n'aurait pas de sens. Ainsi, en Belgique la carte d'identité peut comporter des indications inconnues en France depuis le régime de Vichy (numéro d'identification du Registre national de la population et historique des résidences successives du porteur).

2.4. Il a été noté que l'appréciation du risque en matière de protection des données doit être faite en fonction d'une évolution possible de l'usage de la base par les pouvoirs publics. Il convient donc d'adopter une approche dynamique de l'évolution du risque et pas seulement statique.

2.5. A la question de savoir quel type d'agent aura accès aux données, le ministère a précisé que le système serait géré par des agents habilités et que toute consultation des éléments de la base par un agent sera tracée.

2.6. Une forte demande de maîtrise par le citoyen sur les données inscrites sur la carte et dans les fichiers a été exprimée. Le ministère a proposé que des bornes de lecture des données inscrites dans la puce soient mises en place dans les lieux de délivrance des titres. Le ministère a également proposé que soit ouvert aux citoyens un droit d'accès au fichier des accès à la base concernant leurs données personnelles.

3. Sur la biométrie

3.1. Le ministère de l'intérieur a tout d'abord rappelé que la carte comporterait deux empreintes numérisées et que la base de données en comporterait six. Il a ensuite précisé qu'en raison des risques de connaissance de données liées à la santé d'une personne à partir de l'iris de l'œil (cholestérol, grossesse...), le choix a été fait de ne pas utiliser cette donnée biométrique. Pour ces raisons, mais également pour des raisons culturelles (l'empreinte digitale est déjà relevée actuellement lors d'une demande de carte papier), le ministère de l'intérieur a porté son choix sur ce type de biométrie.

3.2. M. Bismuth a estimé que le choix d'utiliser les empreintes digitales comme élément de biométrie a également été fait pour des raisons économiques parce qu'une entreprise française, Sagem, a une position dominante dans ce domaine et que d'autres choix technologiques (iris de l'œil) dépendent de brevets américains.

4. Sur les scénarios alternatifs

Il a été présenté trois types d'alternatives au projet :

4.1. Il a été suggéré d'abandonner le projet de CNIE en renforçant la sécurité de l'actuelle carte nationale d'identité, en la rendant obligatoire et en sécurisant et informatisant l'état-civil. De façon générale, il a d'ailleurs été souligné que, quel que soit le projet retenu par le Gouvernement, sans informatisation de l'état-civil, le projet INES risque d'avoir des failles. A cet égard, il a été rappelé que les questions liées à l'informatisation de l'état-civil relèvent de la compétence du ministère de la justice ; elles sont en cours d'examen par le biais notamment d'une Mission sur la dématérialisation de l'état-civil.

4.2. Plutôt que d'instaurer une carte d'identité électronique avec une base centralisée d'empreintes digitales numérisées, il a été proposé de créer une CNIE sans base centrale où les données numérisées seraient uniquement dans la puce de la carte.

Le ministère a précisé que cette alternative ne répondrait pas à l'objectif du projet qui est de lutter contre la fraude à l'identité : seule une base centrale des empreintes permettrait d'éviter la délivrance à une même personne de titres sous plusieurs identités différentes ou à plusieurs personnes de titre sous une même identité.

4.3. Le ministère de l'intérieur a proposé, dans le débat sur internet, une alternative en termes de biométrie en envisageant (à titre théorique, car cela ne figure pas dans le projet INES) que la puce de la carte contienne les empreintes (qui sont faciles à vérifier

lors d'un passage de frontière), mais que la base centrale ne contienne pas les empreintes digitales, mais un autre élément biométrique comme l'iris de l'œil.

5. Sur la sécurité de la carte et du système

5.1. Certains ont fait part de leur crainte que l'authentification forte prévue pour la carte ne devienne un standard obligé pour tous les usages. La plupart des intervenants ont souhaité une variabilité de l'authentification en fonction de l'usage.

5.2. Le président de l'association Capucine.net a présenté une approche sécurisée de la carte d'identité électronique dans ses accès sur internet. Partant du postulat que l'identification consiste à décliner son identité et l'authentification à apporter la preuve de l'identité, il estime que la carte doit reposer sur un token (jeton) pour assurer la sécurité des transactions sur internet. Il estime que la fraude sur le net repose sur des identifiants statiques numérisables et reproductibles tels que les numéros de carte bancaire, les identifiants/mots de passe et les données biométriques. Seul le token (signature PKI avec une clé privée unique et imprévisible associée à des protocoles de sécurité SSL) garantirait une authentification forte.

6. Sur les usages et le coût de la carte

6.1 A partir de son expérience de mise en place d'une carte d'étudiant électronique (23.000 cartes délivrées pour un coût de 5 euros par an et par étudiant), le Président de l'Université de Lyon II a estimé qu'une CNIE devrait être multiservices et que l'accès aux données personnelles devrait être proportionnel à l'objet de la consultation (par exemple, pour le passage aux frontières, accès des policiers aux empreintes, mais cet accès aux empreintes ne serait pas possible pour des usages de la carte dans la sphère privée).

6.2. M. Risson propose que la carte comporte quatre fonctions alliant divers niveaux de sécurité :

1. Des fonctions très sécurisées liées à l'identification même de la personne (c'est un élément de citoyenneté que de pouvoir prouver de façon incontestable son identité). A cet égard la biométrie peut être utile.

2. Des fonctions de signature électronique afin de pouvoir authentifier une démarche.

3. Des fonctions destinées à garantir les données personnelles des citoyens (nom, prénom, date et lieu de naissance...), protégées par un code PIN.

4. Des fonctions permettant d'avoir accès à des services locaux. Pour ces derniers, il est souhaité que la carte ne comporte aucune information et que celles-ci soient toutes stockées en « back office » et gérées localement.

6.3. M. Risson souhaite que la consultation des données de la CNIE puisse se faire avec et sans contact, à distance. Il a aussi noté qu'il sera impossible de délivrer un titre sécurisé dans les 36.600 communes françaises. Il redoute donc de voir l'apparition de « supers mairies » (3.000 environ, davantage situées au niveau des communautés de communes) seules à même de pouvoir délivrer les cartes. En tant que responsable du groupe de travail « Nouvelles technologies » de l'Association des maires de France, il a souligné qu'il est important, pour cette association, que toutes les mairies gardent la délivrance des titres d'identité.

Sur ce point, le ministère a précisé que cela nécessiterait alors d'équiper toutes les mairies en matériel ce qui est financièrement trop coûteux. Le ministère a précisé que le projet prévoit, à ce stade, que la carte soit retirée à la mairie de demande du titre.

6.4. De nombreux intervenants ont proposé que, si la carte devait être obligatoire, elle soit gratuite à la première délivrance mais payante en cas de perte ou de

renouvellement. Le ministère de l'intérieur a précisé privilégier actuellement une CNIE non obligatoire, notamment afin de prouver en cela que son objectif n'est pas de « fichier » les citoyens, mais plutôt de garantir à ceux qui détiennent une CNIE, que leur identité est mieux protégée.

6.5. Il a été souligné que ce titre d'identité électronique pourrait, dans les faits, entraîner une forme de pression sociale. En effet, même s'il est présenté comme non obligatoire, il risque de facto de le devenir car il représentera, pour beaucoup d'acteurs publics et privés, un outil d'identification plus sûr qu'ils demanderont tous. La CNIE risque donc, pour de nombreux usages, de devenir une norme obligatoire de fait.

6.6. Mme. Falque-Pierrotin a rappelé qu'une carte d'identité électronique aura comme première fonction de certifier l'identité ; ce qui se fait déjà pour la carte papier tant vis-à-vis des administrations, que des commerçants que lors d'un vote. Partant de ce constat elle a noté que la question est de savoir si les citoyens préfèrent que la carte électronique ne serve qu'à cela ou puisse également servir à des usages autres (moyen de paiement par exemple).

* * *

Troisième étape du débat public itinérant

Paris, le 11 avril 2005

La troisième étape du débat public qu'organise le Forum des droits sur l'internet autour du projet de carte d'identité électronique s'est tenue le 11 avril 2005 à Paris, au Conseil Economique et Social.

Autour de Madame Falque-Pierrotin, présidente du Forum des droits sur l'internet intervenaient quatre personnalités : Bernard Didier, Directeur développement des affaires, division sécurité Sagem, Bernard Fitoussi, Préfet, Directeur du Programme INES, François Giquel, Vice-Président de la CNIL, Michel Tubiana, Président de la Ligue des Droits de l'Homme.

La séance a été animée par Jean Gonié, juriste au Forum des droits sur l'internet.

Les interventions et les échanges avec la salle ont abordé les points suivants :

1. Sur les raisons et l'utilité de l'instauration d'une carte nationale d'identité électronique

1.1. M. Tubiana a déclaré que le projet lui inspire perplexité et inquiétudes. En effet :

* Au-delà de la carte d'identité, il estime que l'on ne comprend pas bien ce qui anime les pouvoirs publics (la référence au Règlement européen n'est pas appropriée : il n'y a pas de raisons internationales pour que la France, mette en place une carte nationale d'identité électronique, ce choix est purement national).

* A ses yeux, un document infalsifiable n'existe pas et vouloir parvenir au « risque zéro » et créer un système sans failles signifierait ne plus vouloir simplement authentifier les individus mais fichier et contrôler la population toute entière.

* L'argument selon lequel la CNIE permettrait de diminuer les coûts liés à la fraude identitaire n'est fondé sur aucune donnée chiffrée.

* Il est difficile de comprendre les différents projets des ministères (CNIE, carte de vie quotidienne, carte vitale 2, changement d'adresse...), ce qui donne une impression générale de confusion dans les initiatives.

* On ne sait pas ce que l'on mettra dans la carte, qui contrôlera quoi, qui sera responsable de quoi...

1.2. Le ministère de l'intérieur a rappelé que la France doit mettre en place rapidement un système sécurisé des titres d'identité car il ne sera bientôt plus possible de se rendre aux Etats-Unis sans un titre sécurisé. Le Règlement européen de décembre 2004 concerne les titres de transport ; or, le ministère précise que la carte d'identité est également un titre de transport. Enfin, il rappelle que certains de pays européens ont déjà commencé à mettre en place une carte nationale d'identité électronique.

1.3. En ce qui concerne les passeports biométriques en Europe, il a été rappelé que seulement six pays ont déjà mis en place ce nouveau titre. Constatant que la mise en place d'éléments biométriques met plus de temps que prévu, la Commission européenne vient de demander aux Etats-Unis le report de la date d'entrée en vigueur du passeport biométrique pour l'entrée des ressortissants de l'Union sur le territoire américain, demande refusée par le Gouvernement américain. Sur ce point M. Didier précise que si les européens n'adoptent pas le passeport biométrique, il faudra, pour entrer sur le territoire des Etats-Unis, obtenir un visa auprès du consulat américain dont la délivrance sera subordonnée à la fourniture d'éléments biométriques qui, cette fois, seront collectés par les autorités américaines.

1.4. M Tubiana rappelle qu'aux Etats-Unis, le permis de conduire sert de document d'identité, or n'importe qui peut aisément en obtenir un faux. Les Etats-Unis ne sont donc pas un exemple dans ce domaine. De façon générale, il estime ainsi que ce n'est pas parce que les américains imposent un passeport biométrique que l'Union Européenne doit faire la même chose. M. Giquel a rappelé que les recommandations de l'OACI ne portent que sur un élément biométrique et que l'Europe, d'elle-même, a choisi d'introduire un second identifiant biométrique : les empreintes digitales. De plus, il constate qu'il n'est pas précisé quelles données devront figurer sur le passeport. Il rappelle également qu'il existe d'autres scénarios pour la mise en place d'une CNIE en Europe : en Italie (carte sans base centrale et avec biométrie) ou encore en Belgique (carte sans biométrie mais avec base centrale car ce pays dispose d'un Registre national de la population). Par ailleurs, il rappelle que la CNI actuelle (1986) est infalsifiable (il n'y a pas été constaté de vols de CNI vierge).

1.5. A la question de savoir comment il est possible d'envisager un tel projet sans avoir de données chiffrées sur la fraude à l'identité, le ministère de l'intérieur a précisé qu'il n'y a pas d'organisme en France chargé d'évaluer le phénomène de la fraude dans sa globalité et que l'on ne dispose pas d'outils statistiques pour cette estimation (ce qui n'est pas le cas au Royaume-Uni par exemple). En outre, la fraude documentaire recouvre en effet différentes situations : la fabrication de faux documents, l'usurpation d'identité, le vol d'identité, etc. La mise en place d'un mécanisme d'authentification d'identité essaie de répondre à toutes ces situations. Le ministère reconnaît néanmoins que les données étrangères utilisées ne sont pas pertinentes et qu'une telle estimation est nécessaire ; il travaille sur ce point.

1.6. M. Didier a rappelé que l'on constate une augmentation des chiffres de la fraude partout dans le monde. Mais, concernant la délivrance des droits sociaux à New York, on a constaté une diminution de 10% des demandes après la mise en place d'un système sécurisé biométrique.

1.7. A la question de savoir pourquoi les Français n'ont pas été consulté plus tôt alors que ce projet est prévu depuis longtemps, le ministère de l'intérieur a tout d'abord rappelé que, les titres d'identité relevant du domaine réglementaire, il aurait pu ne pas présenter un projet de loi. Le choix a justement été fait de présenter un projet de loi pour qu'un débat démocratique et ouvert s'engage sur ce sujet important. De la même manière, le recours au débat public organisé par le Forum des droits sur l'internet n'était pas obligatoire. M. Tubiana estime qu'il convient de travailler en amont de façon collective, ce qui est rare dans un pays comme la France ; il constate à cet égard que l'existence même de ce débat public est un immense progrès.

1.8. Certains ont noté que le projet de CNIE devra bien s'articuler avec celui de dématérialisation de l'état-civil car sans une informatisation de l'état-civil, le projet de CNIE risque d'avoir des failles. Beaucoup ont rappelé qu'il conviendrait également que le projet CarteVitale 2 soit articulé avec le projet INES.

1.9. Certains ont rappelé que, de façon générale, l'objectif d'une sécurisation totale des titres d'identité doit parfois être relativisé : pendant la période de l'Occupation, la falsification de documents a en effet permis de sauver la vie de nombreuses personnes.

2. Sur les risques en matière de vie privée et sur la création d'un fichier centralisé des empreintes digitales numérisées.

2.1. M. Giquel a tout d'abord précisé que la CNIL ne peut prendre position sur le projet car elle n'est pas encore officiellement saisie. Il a ensuite rappelé les positions antérieures de la CNIL sur des problématiques proches.

* Sur la carte nationale d'identité : La CNIL a précisé, en 1980 et 1986, que la constitution d'un fichier national était envisageable si elle était limitée à la gestion et à la délivrance de la carte (pas de photos ou de signatures) et que son accès était exclusivement réservé aux agents habilités. La CNIL a également précisé que le relevé d'empreintes n'est envisageable que s'il est conservé dans un fichier, ni numérisé ni centralisé.

* Sur la biométrie : il s'agit de données à caractère personnel (article 2 de la loi de 1978). Le traitement de ce type de données relève du régime d'autorisation de la CNIL (article 25 de la loi du 6 août 2004) ce qui n'était pas le cas sous l'ancienne version de la loi. Ces données présentant des risques particuliers, leur traitement sous forme centralisée ne peut être envisageable que pour des raisons impérieuses de sécurité ou d'ordre public. S'il n'y a pas de constitution d'une base centralisée, cela ne pose pas de problème particulier (ex. : fichier d'empreintes digitales de l'OFPPA, ou encore fichier des Aéroports de Paris).

2.2. M. Giquel a enfin rappelé que les grands principes de la loi de 1978 (finalité et proportionnalité du traitement : les données collectées doivent être pertinentes, non excessives, adéquates...), doivent être appliqués au projet INES : quelle est la finalité explicite du projet (la lutte contre la fraude documentaire ou la recherche des infractions ou la lutte contre le terrorisme ?), qui a accès à quelles données (les commerçants pourront-ils avoir accès à certaines données ?) qui pourra imposer la détention d'une telle carte et son passage dans un lecteur ?, n'y a-t-il pas d'autres moyens d'atteindre les objectifs poursuivis ? etc.

2.3. Certains ont souhaité savoir quelle maîtrise aura le citoyen sur les données inscrites sur la carte et dans les fichiers : pourra-t-il stocker lui-même des informations sur la carte ? aura-t-il accès aux données ?...). Le ministère de l'intérieur a estimé qu'il semble compliqué, tant en termes de sécurité que de responsabilité, que le citoyen stocke lui-même des informations sur la carte. Enfin, le ministère a précisé que, à la suite d'une proposition faite sur le forum de discussion, il réfléchit à un système permettant au titulaire de la carte de lire les informations qu'elle contient à tout moment.

2.4. En ce qui concerne les garanties du projet, le ministère de l'intérieur a annoncé que :

1. L'ensemble du dispositif sera crypté par le niveau le plus élevé de sécurité.
2. L'ensemble des accès aux fichiers sera tracé ce qui permettra d'identifier la personne qui en aura eu accès.
3. Les accès aux fichiers ne pourront se faire que par habilitation.
4. Les dispositions pénales relatives à l'usurpation d'identité seront étendues aux accès indus aux fichiers.
5. Il sera créé un nouveau délit portant sur le fait de lire ou d'exploiter indûment les données contenues dans la puce électronique de la carte.
6. Les données de santé et à caractère sanitaire et social ne seront pas dans la CNIE, une telle disposition serait en tout état de cause inconstitutionnelle.
7. Un contrôle sera assuré par la CNIL et les instances judiciaires.

2.5. M. Tubiana considère que l'appréciation du risque en matière de protection des données doit être faite en fonction d'une évolution possible de l'usage de la base par les pouvoirs publics. Partant du constat que le fichier STIC (Système de Traitement des Infractions Constatées) fait l'objet de dérapages et d'une utilisation croissante par les pouvoirs publics, il craint de ce fait un glissement dans l'usage et la consultation d'un fichier centralisé des empreintes digitales. A cet égard, il estime que les garanties évoquées pour le contrôle de l'accès aux données sont illusoire : il n'y a pas de possibilité d'engager de responsabilité et personne ne contrôlera l'accès aux données si ce n'est l'administration elle-même.

2.6. M. Tubiana estime que, face à ce risque de diminution des libertés individuelles par les pouvoirs publics, il faut qu'émerge un réel « tiers de confiance » disposant de moyens et d'une indépendance suffisants pour contrôler l'utilisation qui sera faite du système. A cet égard, le ministère de l'intérieur a rappelé que la confiance n'exclue pas la vérification et a proposé comme garantie qu'un organisme comme le Forum des droits sur l'internet organise régulièrement des débats similaires à celui qui se tient actuellement afin de dresser des constats réguliers sur les garanties mises en place.

2.7. Le ministère a précisé que seule une base centrale des empreintes permettrait d'éviter la délivrance à une même personne de titres sous plusieurs identités différentes ou à plusieurs personnes de titre sous une même identité. Le ministère n'a pas souhaité préciser si le projet INES était envisageable sans base centralisée.

3. Sur la biométrie

3.1. M. Didier a défini la biométrie comme une technique permettant d'établir un lien automatique entre le monde abstrait (nom, prénoms, etc.) et le monde réel (l'individu en lui-même). A ce titre il estime que seule la biométrie permet de mesurer le vivant et d'identifier et d'authentifier les individus de façon performante. Elle permet ainsi de s'assurer que lors de la délivrance d'un droit celui-ci est délivré à la bonne personne, de gérer les interdits et d'authentifier l'individu à chaque utilisation de son droit. La biométrie, pour être performante, doit être évaluée en fonction de trois critères :

1. L'universalité : la biométrie a-t-elle un caractère universel (ex. : la prise en compte des cheveux exclut les chauves, etc.) ?
2. L'unicité : la biométrie a-t-elle un caractère unique (permet-elle d'identifier une personne unique) ?
3. L'immutabilité : la biométrie a-t-elle un caractère immuable (l'information biométrique va-t-elle se dégrader dans le temps) ?

3.2. En ce qui concerne le choix de l'empreinte digitale comme identifiant biométrique, M. Didier a précisé que cette technique de biométrie bénéficie de plus d'un siècle d'expérience par les pouvoirs publics en matière de lutte contre la criminalité. Il précise qu'il s'agit d'une technique fiable, maîtrisée et ayant acquis une certaine maturité industrielle. En revanche, il estime que l'iris de l'œil fait l'objet d'une technologie plus jeune sur laquelle on ne dispose pas assez de recul. A cet égard il rappelle que l'utilisation d'un élément biométrique dépend également des objectifs poursuivis en terme de sécurité. Si le but de la CNIE est d'assurer davantage de sécurité, il convient de rappeler qu'en France on ne dispose pas aujourd'hui de l'iris des personnes condamnés pour infractions graves mais en revanche des empreintes digitales d'une grande partie d'entre elles.

3.3. Il a été remarqué qu'au Royaume-Uni on estime que, pour 2 à 5% de la population (empreintes abîmées ou illisibles, manchots etc.), il ne sera pas possible d'enregistrer les empreintes digitales. M. Didier précise qu'en France le taux de la population concerné est d'environ 2 %. Il précise que ce taux peut être ramené à 0,2 % avec l'utilisation complémentaire d'autres techniques. Il précise qu'aux Etats-Unis, selon le FBI, l'impossibilité de lecture concerne 0,5 % de la population criminelle et 2,5 % de la population civile. M. Didier estime donc qu'il y a en effet une partie de la population française qui risque de ne pouvoir être « enrôlée ». Le ministère de l'intérieur a précisé que les cas où les empreintes digitales n'auront pu être relevées seront signalés. M. Giquel a tenu à préciser que les difficultés de l'authentification biométrique ont, par ailleurs, été montré dans un récent rapport publié par la London School of Economics en mars dernier.

3.4. A la question de savoir pourquoi il est prévu qu'une photo numérisée soit dans la puce, M. Didier a précisé que la numérisation permet de signer la photo pour en assurer l'authenticité. Il s'agit donc d'une sécurité supplémentaire.

4. Sur la sécurité de la carte et du système

4.1. Le ministère a précisé que la durée d'un certificat électronique est au maximum de trois ou quatre ans alors que la carte ou le passeport sont valables dix ans.

4.2. En ce qui concerne la lecture « sans contact » à distance des données de la carte, le ministère a précisé que le dispositif sera très sécurisé et que les commerçants ne pourront pas lire les données inscrites sur la carte.

5. Sur les usages et le coût de la carte

5.1. M. Tubiana estime que la carte ne doit servir qu'à l'authentification de l'identité de la personne et du titre. La Ligue des droits de l'homme rappelle qu'elle s'oppose à l'inscription de toute autre information, quelle qu'elle soit et estime qu'il devra par ailleurs toujours être possible de prouver son identité par tous moyens. Concrètement, la photo semble suffisante dans l'idée d'une authentification du porteur. Mettre d'autres informations que l'identification de la personne, risque de créer une fracture dans la société entre ceux qui auront la carte et ceux qui ne l'auront pas. Ainsi, la carte pourrait devenir, dans les faits, discriminante car elle risque, pour de nombreux usages, de devenir une norme obligatoire d'identification.

5.2. A la question de savoir quel sera le coût de la carte (coût à l'unité et coût du système dans sa globalité), le ministère de l'intérieur a déclaré ne pas pouvoir se prononcer sur ce point où aucune décision n'a encore été prise ; il a de plus précisé que certains aspects feront l'objet d'appels d'offres publics (ce qui nécessite de la confidentialité) et qu'il ne pouvait, dès lors, annoncer des chiffres globaux de marché.

5.3. M. Didier estime que le surcoût d'une carte d'identité électronique lié à la biométrie représente environ 20 % du coût total d'un système de grande ampleur et bénéficiant d'un haut niveau de sécurité. Ceci reviendrait à une estimation de 2 à 4 euros par personne, selon les options, pour le système, les terminaux et une maintenance sur dix ans. A titre d'exemple il précise que le Royaume-Uni a estimé un coût de 35 livres par carte à (en novembre 2003), et l'Italie de 25 à 30 euros (en octobre 2003).

5.4. Le ministère de l'intérieur a annoncé que la carte sera délivrée par le préfet du département. Une entité publique validera les modalités de délivrance des certificats.

5.5. Le ministère de l'intérieur a précisé que la France et l'Allemagne coopèrent dans le domaine de la carte d'identité électronique. Cette coopération ne porte que sur les normes et les standards. Il s'agit donc avant tout d'une coopération industrielle.

* * *

Quatrième étape du débat public itinérant

Lille, le 27 avril 2005

La quatrième étape du débat public qu'organise le Forum des droits sur l'internet autour du projet de carte d'identité électronique s'est tenue le 27 avril 2005 à Lille, à l'Université de Lille II.

Le Forum des droits sur l'internet avaient invité cinq personnalités à intervenir : Christian Cabal, Député et auteur d'un rapport sur la biométrie au sein de l'Office Parlementaire d'Evaluation des Choix Scientifiques et Technologiques, Frédéric Lagandré, Responsable du Pôle technique, Direction de la Sûreté, Aéroports de Paris, Jean-Jacques Lavenue, Professeur de droit, Université Lille 2, Meryem Marzouki, Présidente de l'association IRIS (Imaginons un Réseau Internet Solidaire) et chercheuse au CNRS, Hubert Vigneron, Président de la section "carte à puce" du Gixel (Groupement des industries électroniques).

La Direction de programme INES (Identité Nationale Electronique Sécurisée) du ministère de l'Intérieur était représentée par Sophie Planté, adjointe au directeur.

La séance a été animée par Jean Gonié, juriste au Forum des droits sur l'internet.

Les interventions et les échanges avec la salle ont abordé les points suivants :

1. Sur l'utilité de l'instauration d'une carte d'identité électronique et sur les risques en matière de vie privée.

1.1. M. Cabal a estimé qu'il est important, dans notre société actuelle, de pouvoir certifier de son identité et s'assurer qu'un individu est bien ce qu'il prétend être. Pour ce faire, on doit pouvoir accéder à une certification de l'identité facilement, rapidement (cf. embarquement dans un avion), de façon non invasive au regard de la vie privée et à un coût raisonnable. M. Cabal estime que seules les empreintes digitales répondent à ces trois critères, car l'iris de l'œil, bien que techniquement au point, est une technologie invasive (données d'ordre médical).

1.2. M. Cabal précise que les techniques de biométrie ne doivent pas porter atteinte aux principes fondamentaux énoncés dans la loi Informatique et libertés. A cet égard, la CNIL a un rôle majeur à jouer. M. Cabal précise que, sous réserve du respect de ces principes, les craintes autour du projet de carte d'identité électronique sont infondées et que la volonté qu'ont certains de masquer leur identité n'est pas un comportement normal : un citoyen qui n'a rien à se reprocher n'a, a priori, pas de raisons d'adopter une telle attitude. Sur ce dernier point, un certain nombre de personnes, dont Bruno Villalba, maître de conférences à Lille 2, ont répondu que l'anonymat est un droit et qu'un endroit où il n'y a plus d'anonymat possible est un lieu où il n'y a plus d'espace privé.

1.3. A titre liminaire, M. Lavenue considère que dans un monde parfait, soucieux de la protection de la vie privée et des libertés des citoyens, où l'administration aurait mis en place toutes les assurances possibles protégeant les administrés, une CNIE offrirait un potentiel considérable de simplification et d'économie à l'administration et à ses usagers. Seulement à ses yeux, cela est impossible et comme il le précise, le meilleur des mondes n'est pas nécessairement souhaitable.

1.4. M. Lavenue a souhaité, en prenant l'exemple de l'accord PNR, mettre en évidence un aspect international de la question de la protection des libertés en montrant, à travers les dérives de cet accord, que le futur est déjà là et que l'évolution n'est pas nécessairement favorable. Le 28 mai 2004, l'Union Européenne et les Etats-Unis ont signé un accord sur les transferts de données relatives aux passagers à destination des Etats-Unis (accord PNR pour Passenger Name Record). En vertu de cet accord, tout passager européen embarquant sur un vol à destination des Etats-Unis doit désormais accepter la communication au ministère américain de la sécurité intérieure de 34 des 39 données personnelles contenues dans son dossier passager (PNR).

1.5. M. Lavenue a précisé que les 34 données récoltées vont de l'itinéraire complet du voyageur en passant par le mode de paiement de son voyage où encore l'agence où le billet a été acheté. Il n'est pas exclu que des informations personnelles supplémentaires puissent également être recherchées suite à un examen des données PNR. A cet égard, M. Lavenue estime que l'on peut s'interroger sur l'incidence de la différence de statut des données personnelles entre la législation européenne et la législation américaine. Le fait, par exemple que la « Déclaration d'engagement du bureau des Douanes », annexée à la décision de 2004, précise que « l'accès aux fichiers liés à des comptes de courrier électronique mentionnés dans un PNR obéira aux exigences de la loi des Etats-Unis... » peut laisser craindre que les européens n'aient guère de pouvoirs concrets en ce domaine. Dans ce cadre, M. Lavenue estime qu'il pourrait être alors envisagé qu'à partir du numéro d'identité bancaire ou de l'adresse électronique obtenus dans le PNR puissent être consultées toutes sortes de données comme les numéros de cartes de crédits, les listes des derniers achats effectués par une personne, les numéros de compte en banque...

1.6. M. Lavenue se demande s'il y a lieu de s'inquiéter ou si, au contraire, il s'agit d'hystérie voire de paranoïa. A cet égard, il estime qu'une légère dose de paranoïa peut parfois être salutaire quand il s'agit de protection des libertés et que ce « cas d'école » est là pour permettre de mettre en évidence des failles dans la réglementation qui, au final, peuvent purement et simplement autoriser les services américains à s'introduire dans le système et à y prélever les informations qui les intéressent. De plus, des transferts ultérieurs de ces informations peuvent être envisagés à la discrétion du Bureau des Douanes des Etats-Unis (CBP). Il est précisé que le CBP est considéré comme étant propriétaire des données ; une utilisation marchande des ces dernières pourrait alors s'avérer possible.

A cette argumentation, le ministère de l'intérieur a précisé que les mesures énoncées concernant la PNR sont dès à présent entrées en vigueur, et que, même si l'on peut le déplorer, l'introduction des nouvelles générations de titres ne change radicalement rien à la problématique des données PNR. Le ministère estime que lier les deux résulte de l'amalgame.

1.7. A partir du constat sur ce qui passe aux Etats-Unis en 2005, M. Lavenue estime qu'avec la mise en place d'une CNIE en 2007 apparaît clairement le risque qu'en signant avec une carte à puce, le flux des informations sur le citoyen risque de s'enrichir et de limiter ce que l'on peut considérer comme relevant actuellement de l'espace privé : le bénéfice de l'anonymat, le droit à l'oubli, voire à la dissimulation. M. Lavenue insiste sur le fait qu'il convient de veiller à ce que la sécurité ne devienne pas une idéologie et à cet égard rappelle les propos Benjamin Franklin : « Quiconque est disposé à abandonner une partie de sa liberté au nom d'une prétendue sécurité, ne mérite ni l'une ni l'autre ».

1.8. Mme. Marzouki a fait savoir que l'association IRIS considère que le projet de CNIE est injustifié, nocif, et introduit suivant un procédé déloyal et antidémocratique. L'association se prononce donc contre ce projet et envisage, notamment avec ses partenaires de la Ligue des Droits de l'Homme et de DELIS (Droits Et Libertés face à

l'Informatisation de la Société), des actions de sensibilisation aux dangers de ce projet et de mobilisation afin d'y faire échec.

1.9. Pour Mme. Marzouki, le projet est injustifié car les arguments du ministère de l'intérieur sur sa nécessité ne sont pas convaincants. Le ministère ne fournit aucun chiffre permettant de constater l'ampleur déclarée de la fraude en termes de falsification de la carte d'identité actuelle, d'usurpation d'identité et de délivrance induite de titres multiples. Cette ampleur supposée de la fraude reste pourtant, à l'examen et selon les déclarations même des représentants du ministère, le seul argument servant à justifier la création d'une base de données centralisée comportant notamment des éléments biométriques. Elle précise qu'il y a donc là un risque très fort d'atteinte au principe de proportionnalité, principe fondamental en matière de protection de la vie privée et des données personnelles.

A cette argumentation le ministère a précisé que :

- * Le Sénat a justement mis en place une mission d'information sur la nouvelle génération de documents d'identité et la fraude documentaire afin notamment de pouvoir établir des données chiffrées sur la fraude.

- * Seuls les ministères des finances et des affaires sociales seraient à même d'établir le coût de la fraude, ce qui n'est pas encore fait. Le ministère précise cependant que depuis que la carte d'identité est gratuite le taux de perte a été multiplié par plus de dix (36.000/an en 1998, plus de 500.000/an actuellement), ce qui a un coût pour la collectivité et des conséquences directes en matière d'usurpation d'identité (les cartes n'étant pas perdues pour tout le monde).

1.10. Pour Mme. Marzouki, le projet est nocif car, en dépit des déclarations du ministère de l'intérieur visant à assurer que le projet permettra à la fois une sécurisation complète des informations et des garanties de limitation d'usage des données contenues dans la carte et dans la base de données centralisée, le projet ouvre la voie à de graves dérives. Ces dérives induisent un très fort risque d'atteinte au principe de finalité, autre principe fondamental en matière de protection de la vie privée et des données personnelles.

Mme. Marzouki estime que ces dérives portent principalement sur :

1. La possibilité de fichage généralisé.

- * par la mise en place d'une base de données centralisée, contenant notamment des informations biométriques.

- * par les techniques de biométrie choisies (face et empreintes digitales) qui sont justement celles qui laissent des traces, traces qui de surcroît peuvent être collectées à l'insu de la personne concernée, et donc sans son consentement (possibilité de photographie dans des lieux publics, relevé d'empreintes).

- * par le fait que le projet est conçu pour plusieurs utilisations, dont la diversité dépasse la seule gestion de l'état civil. Ces utilisations incluent les transactions avec des opérateurs privés, à travers le certificat de signature électronique. A cet égard, elle estime que la présentation du projet par le ministère de l'intérieur entraîne la confusion par le mélange des genres (projet destiné, outre l'état civil, à la lutte contre le terrorisme, à la lutte contre l'immigration illégale, à la signature électronique pour les transactions administratives comme pour les transactions commerciales et même à des utilisations individualisées au moyen d'un « portfolio personnel »...).

En ce qui concerne la création d'une base centralisée des données biométriques, le ministère de l'intérieur rappelle que l'objectif du projet (lutter contre la fraude à l'identité) ne peut être valablement atteint que si une telle base existe car c'est le seul moyen permettant d'éviter la délivrance à une même personne de titres sous plusieurs identités différentes ou à plusieurs personnes de titre sous une même identité ; c'est à dire le seul moyen de fiabiliser le lien entre un individu et son identité.

2. Le risque de voir les utilisations des données biométriques contenues dans la carte et dans la base être étendues dans l'avenir. Partant du constat que les fichiers STIC

(Système de Traitement des Infractions Constatées) et FNAEG (Fichier National Automatisé des Empreintes Génétiques) ont fait l'objet de dérapages et d'une utilisation croissante par les pouvoirs publics, Mme. Marzouki craint, de ce fait, un glissement dans l'usage et la consultation des données.

3. Le fait que la CNIL n'a pas les moyens d'assurer un contrôle efficace. La nouvelle loi informatique et libertés donne moins de pouvoir de contrôle à la CNIL car elle peut permettre des extensions d'utilisation par l'État sans, dorénavant, avoir besoin d'un accord de la CNIL. C'est le cas avec l'article 27-I nouveau de la loi du 6 août 2004 qui concerne, notamment, la mise en place de traitements sur des « *données biométriques nécessaires à l'authentification ou au contrôle de l'identité des personnes* ». Par cet article, la CNIL perd la faculté de s'opposer à la mise en place de tels fichiers car leur mise en place est désormais prise après un avis motivé et publié de la CNIL mais celui-ci n'a pas à être nécessairement conforme.

1.11. Pour Mme. Marzouki, le projet est déloyal et antidémocratique car la façon dont il est présenté vise à cacher à la population l'ampleur du risque, afin d'obtenir son consentement par un processus de légitimation du projet et de ses objectifs. De plus elle estime que les décisions s'avèrent être déjà prises à un niveau de détail très avancé. Elle fait savoir que les négociations avec les communes, notamment à travers des discussions avec l'Association des Maires de France (AMF) sont déjà en cours pour déterminer combien de villes disposeront des dispositifs et de l'infrastructure nécessaires au déploiement du projet. A ses yeux cela montre que les détails de mise en oeuvre du projet sont déjà en cours d'adoption, alors même qu'un débat public se déroule (organisé par le FDI sur mission du ministère de l'Intérieur), que la CNIL n'a pas encore été saisie pour avis, et que le projet de loi n'a pas été transmis au Parlement.

A cet égard elle estime :

1. Qu'il est faux de prétendre que le projet est dicté par des obligations internationales. Les standards élaborés par l'OACI et le Règlement européen du 13 décembre 2004 ne concernent que les passeports et documents de voyage. De plus, le standard de l'OACI est restreint à un seul élément biométrique, la photographie. Enfin, les deux documents (OACI et règlement européen) sont sujets à caution démocratique par leurs modes de discussion et d'adoption. Ainsi, la « *lettre ouverte au Parlement européen contre l'immatriculation biométrique de tous les citoyens et résidents européens* » par les ONG Privacy International, Statewatch et European Digital Rights – fédération européenne dont IRIS est membre – dénonçait, dès novembre 2004, le fait que les textes ont été adoptés dans l'urgence et que les citoyens ont été tenus à l'écart du débat ; il y était d'ailleurs déploré une absence de débat public en France sur ce sujet.

2. Qu'il est faux de prétendre que la France n'avait aucune responsabilité dans l'adoption de ces documents. Mme. Marzouki a rappelé que par son suivi des développements européens et internationaux, IRIS a montré à plusieurs reprises que la France joue un rôle moteur parmi ses partenaires dans l'adoption de réglementations internationales portant gravement atteinte à la vie privée et à la protection des données personnelles.

A cette argumentation le ministère de l'intérieur a précisé que :

* il est injuste de dire que le projet est mené de manière non démocratique car la loi du 6 janvier 1978 modifiée le 6 août 2004 aurait permis de se passer du vecteur législatif pour créer le projet INES. C'est justement en raison de l'importance du projet, que le ministre de l'intérieur a souhaité ne pas utiliser le décret, et a voulu qu'INES soit adopté par la représentation nationale et face l'objet d'un débat en toute transparence. Preuve en est le présent débat. Enfin, le ministère a précisé que le choix d'une loi a été conforté par la décision du Conseil d'Etat du 5 janvier 2005 qui précise que seule une loi peut mettre à la charge des communes une charge de l'Etat, en l'occurrence le dépôt des demandes de titres.

* Il est faux de dire que la France n'a pas d'engagements européens à respecter. Le Règlement européen sur les passeports qui a été adopté est exécutoire de plein droit,

c'est à dire sans même qu'une loi ne soit nécessaire pour le transposer. Dans ce cadre, le gouvernement français est bien obligé de délivrer des passeports biométriques à compter de fin 2006. Le ministère souligne qu'il est en revanche exact de dire que s'agissant des CNI, il n'y a pas à ce jour d'obligations. C'est pourquoi le débat porte exclusivement sur ce titre et que toutes les contributions sont les bienvenues. Les opinions exprimées sur la configuration de la carte éclaireront les choix publics qui pourront être différents de ceux rendus sur le passeport, voire mener à l'abandon du projet de CNIE.

1.12. De façon générale, Mme. Marzouki estime que les décisions qui seront prises pour la CNIE seront, parce qu'elles concernent l'ensemble de la population, des décisions structurantes. En effet, elles vont, d'une part, structurer tous les choix ultérieurs en matière de mode de vérification d'identité, que ce soit pour des besoins publics ou privés (même les plus quotidiens comme une opération de retrait de courrier postal recommandé ou de présentation d'un chèque bancaire à une caisse de supermarché). Elles vont, d'autre part, structurer l'ensemble du marché de la biométrie et la sécurisation des transactions, qu'il s'agisse des infrastructures, des matériels ou des logiciels.

1.13. M. Villalba dénonce l'absence de réflexions sociales et politiques sur un tel sujet. Il constate ainsi que le débat porte principalement sur les aspects techniques du projet (coûts, faisabilité technique, fiabilité...) mais peu sur les aspects politiques et sociaux (quelle utilité réelle du projet ?). Il constate également que, sous prétexte qu'il convient de ne pas être paranoïaque, le projet n'offre aucune garantie sur l'avenir (rien ne dit que l'utilisation de la base ne sera pas élargie, rien n'est précisé sur l'évolution des techniques d'identification, sur d'autres coûts à venir etc.).

1.14. A la question de savoir en quoi la mise en place de la carte permettra de lutter contre le terrorisme, le ministère de l'intérieur a reconnu que cet argument pour expliquer la création de nouveaux titres est mal compris. C'est pourquoi le ministère précise que le projet vise à lutter contre les fausses identités, quelle qu'en soit l'origine :

* la falsification de document (de passeport souvent) qui consiste à modifier le document original (changement de la photo par exemple) ;

* la contrefaçon (qui concerne elle aussi principalement le passeport) qui consiste en la réalisation de faux documents ;

* l'usurpation, qui consiste à prendre l'identité de quelqu'un d'autre par l'utilisation d'une authentique CNI mais dérobé à son légitime titulaire ou « prêtée » par ce dernier ;

* l'identité fictive qui consiste à faire établir d'authentiques passeports ou CNI pour un individu imaginaire.

Le ministère estime que, sur tous ces points, les titres français doivent être améliorés et précise que les fausses identités sont pratiquement toujours utilisées dans les infractions de grande ampleur (mais aussi dans des moins grandes) comme le terrorisme et les divers trafics. En ce sens, toute action destinée à rendre plus fiable l'identité des citoyens est un moyen de lutter contre les atteintes à la sécurité publique.

2. Sur l'accès aux données

2.1. A la question de savoir comment un citoyen pourra vérifier et/ou modifier les données personnelles contenues dans sa carte d'identité électronique, M. Vigneron a tout d'abord rappelé que pour d'autres applications c'est déjà possible :

- Pour le téléphone mobile : on peut modifier son répertoire contenu dans la carte SIM,
- Pour la carte bancaire : même si l'on ne peut rien modifier l'utilisateur peut vérifier ses transactions ultérieurement en s'identifiant avec son PIN par l'intermédiaire d'un lecteur (exemple des lecteurs Xiring),

- Pour la carte Vitale : même si elle ne permet pas la modification du contenu de la carte par son propriétaire, des bornes permettent la consultation des droits inscrits dans la carte ainsi que leur mise à jour.

M. Vigneron a ensuite précisé que, pour la carte d'identité électronique, il convient de distinguer deux types d'accès aux données. L'accès au bloc "portfolio personnel" est différent de celui aux données personnelles contenues par l'administration.

1. Le portfolio permettrait aux titulaires, s'ils le souhaitent, de stocker, à titre personnel, des informations complémentaires dans la carte, soit pour faciliter leurs transactions électroniques (stocker de manière « exportable » nom, prénom, adresse, pour remplir des formulaires), soit pour remplacer d'autres papiers (numéro de permis de conduire, numéro fiscal, etc). Dans ce cadre, la vérification ou la modification des données contenues dans la carte pourrait se faire par l'intermédiaire d'un lecteur personnel et en s'identifiant au moyen d'un code PIN.

2. L'accès aux données personnelles contenues dans les serveurs de l'administration est encadré juridiquement (cf. droit d'accès et de rectification) et pourra se faire après authentification de la carte, par le biais d'un serveur authentifié et d'un canal sécurisé. Ces opérations se feront par la partie carte à contact.

2.2. Le ministère de l'intérieur rappelle que les titres contiendront trois types de données :

1. Les données visibles par tous sur la carte, les mêmes qu'aujourd'hui.
2. Les empreintes des deux index : accessibles seulement par la police et la gendarmerie.
3. Les données liées à la signature électronique : le ministère précise que les usages de cette signature sont en premier lieu destinés aux téléprocédures administratives. Le débat reste ouvert sur les autres usages que les citoyens désireraient.

3. Sur les personnes habilitées à consulter les données

3.1. A la question de savoir quel type d'agent aura accès aux données, le ministère a précisé que :

1. s'agissant de la base de données INES :

* le système sera géré par des agents habilités (agents chargés de la délivrance des titres, mairies et préfectures) et que toute consultation des éléments de la base par un agent sera tracée.

* Seules la police et la gendarmerie auront accès à la base des données biométriques, dans le cadre que fixera le projet de loi (possibilité réservée aux seuls officiers de police judiciaire sous le contrôle du parquet, dans les conditions prévues par le code de procédure pénale). Ces consultations seront également tracées.

* Le journal de ces consultations sera accessible au citoyen qui en fera la demande, s'agissant de ses propres données personnelles.

2. s'agissant de la puce :

* Le citoyen pourra avoir accès aux données contenues sur la puce de son titre, probablement à partir de bornes installées dans les lieux de délivrance des titres.

4. Sur la biométrie

4.1. M. Lagandré a fait part de l'expérience des Aéroports de Paris (ADP) en matière de contrôle biométrique. Les ADP ont équipé 100.000 employés travaillant dans des zones de sûreté de carte avec empreintes digitales (coût de la carte entre 6 et 7 euros). Il n'y a pas de base centralisée mais divers bases d'empreintes digitales numérisées. Grâce à ce

système, 32.000 contrôles quotidiens sont opérés ; de plus la carte se lit sans contact ce qui engendre un gain de temps conséquent. La mise en place de la biométrie a été bien acceptée par les employés (trois mois après la mise en place de la carte, et alors qu'elle n'était pas encore obligatoire, 97% des employés avaient déjà choisi librement d'y avoir recours). A cela M. Villalba remarque, d'une part, qu'il convient de manier avec précaution de tels résultats car l'on peut difficilement comparer l'acceptabilité de la biométrie chez une population salariée restreinte utilisant un document lié à leur travail avec celle qu'auraient tous les citoyens sur un titre d'identité d'ampleur nationale. D'autre part, l'acceptabilité d'une telle carte professionnelle dans une entreprise doit toujours être fortement relativisée les employés n'ayant souvent pas d'autre alternative que de suivre le choix de leur direction.

4.2. Mme. Marzouki estime que la mise en oeuvre du projet INES entraînera une banalisation de l'usage de la biométrie et forgera le consentement de la population à se soumettre à des atteintes de plus en plus invasives à leur vie privée. Elle précise que l'usage de la biométrie constitue un véritable changement d'échelle car, comme IRIS l'avait déjà rappelé à la conférence internationale des autorités de protection des données en septembre 2001, ces techniques permettent « *la mesure et la reconnaissance de ce que l'on est, à la différence d'autres techniques de mêmes finalités, mais permettant de mesurer ou vérifier ce que l'on possède (carte, badge, document, ...) ou ce que l'on sait (mot de passe, code pin, ...)* ». C'est pourquoi IRIS souhaite que la carte ne comporte aucun élément biométrique.

4.3. En tout état de cause, Mme. Marzouki rappelle que l'utilisation des techniques biométriques comporte encore de graves insuffisances notamment en termes d'authentification et de sécurité. C'est pourquoi, avant de développer la biométrie, il convient de mener des études et des débats sur son utilité réelle, voire appliquer un principe de précaution sur la biométrie.

4.4. Mme. Marzouki rappelle également que le marché de la biométrie présente de très forts potentiels économiques et que, de l'avis de tous les acteurs industriels, il est encore seulement en émergence.

5. Sur la lecture « sans contact » des données

5.1. Le ministère de l'intérieur envisage de mettre en place, dans un premier temps, une consultation bimode des données de la carte. La consultation des données d'identité (photo et empreintes) par les autorités habilitées se ferait sans contact car cela se conjuguerait avec les applications passeport (qui comportera également une puce sans contact insérée dans le livret), serait plus facile à utiliser (lors de contrôles de masse dans des aéroports par exemple) et s'utiliserait moins. L'authentification automatique de la carte et la mise en oeuvre des fonctions électroniques offertes au porteur se feraient avec contact (et avec un code secret), grâce à un lecteur de cartes externe ; le mode « avec contact » restant une méthode plus sécurisée.

5.2. Le ministère précise que tous les Etats s'interrogent sur la possibilité d'utiliser le sans contact à l'heure actuelle. En tout état de cause, cette technologie ne sera introduite en France pour la carte nationale d'identité électronique que si les études montrent qu'il n'y a pas de risque de capture des informations à l'insu du porteur, et selon les normes qui permettront de s'en assurer.

5.3. Mme. Marzouki estime que le choix d'une puce à lecture sans contact entraîne des risques de lecture non autorisée (*skimming*) et d'interception indue des données transmises de la puce au lecteur sans contact (*eavesdropping*). A cet égard elle précise que le gouvernement américain subordonne la mise en oeuvre du passeport à puce sans contact à l'obtention de la garantie que tous les risques de cet ordre peuvent être écartés

(déclaration de Frank Moss, représentant du Département d'État US à la conférence CFP à Seattle le 13 avril 2005). De plus, elle estime qu'il n'y a pas de justification impérative à la lecture sans contact, l'argument avancé de « limitation de l'usure de la carte » étant peu sérieux. C'est pourquoi IRIS souhaite que, si la carte doit comporter une puce pour l'authentification du document, la lecture de cette puce ne se fasse pas sans contact.

5.4. M. Vigneron a souhaité lever l'amalgame qui a pu être souvent fait entre RFID (Radio Frequency Identification) et carte à puce sans contact ; les étiquettes RFID n'ayant rien à voir avec l'interface radio sécurisé d'une carte à microprocesseur. Il précise de plus qu'il convient d'apporter des précisions sur les notions de « skimming » et « eavesdropping » telles que décrites par Mme. Marzouki. En effet, M. Vigneron estime qu'il ne peut y avoir de lecture de la puce sans contact à l'insu de la personne car, selon les critères établis par l'OACI pour les contrôles d'accès basiques (« basic control access »), ce n'est qu'après une lecture optique préalable de la bande MRZ (« Machine Readable Zone ») que les fonctions « sans contact » peuvent être rendues disponibles.

6. Sur la sécurité de la carte et du système

6.1. A la question de savoir dans quelle mesure il est possible de prévenir la création de fausse carte à puce et de falsifier son contenu, M. Vigneron a précisé, à titre préalable, que les garanties des mécanismes sécuritaires entourant les certificats électroniques ont, pour l'instant, une durée de vie limitée (5 ans au plus). Il a ensuite tout d'abord précisé que le microprocesseur de la carte a plus de 30% de son système d'exploitation consacré à sa propre sécurité. Ensuite que les moyens de duplicata de puce sont très chers et traçables. Enfin, le contenu des données dans la puce est crypté.

6.2. A la question de savoir si des entreprises de certification privées pourraient certifier la carte, le ministère estime que l'Etat pourrait être son propre certificateur.

7. Sur le coût de la carte et son caractère obligatoire

7.1. M. Vigneron a annoncé que le marché de la carte à puce dans ses applications administration électronique (cartes d'identité, cartes de santé, permis de conduire, cartes émises par les municipalités, cartes des personnels de l'administration...) est prometteur puisqu'il est estimé à 60 millions de cartes au niveau mondial en 2005 et plus de 100 millions en 2006 (selon IDC). Cela ne représente toutefois qu'une faible part des cartes à microprocesseur dans le monde (1,7 milliard en 2005 dont 1,2 en téléphonie mobile). Mais le marché potentiel est considérable (à terme sur les 6,5 milliards d'individus un certain nombre est susceptible d'avoir une ou plusieurs cartes) et les chinois annoncent déjà 100 million de cartes d'identité cette année (marché captif). Aujourd'hui l'industrie française de la carte fournit 60 à 70 % du marché mondial. A cet effet, M. Vigneron estime que l'intérêt des industriels français est de permettre l'émergence de standards internationaux tout en capitalisant sur une implémentation nationale de référence ; c'est pourquoi le Gixel travaille également avec les allemands.

7.2. M. Vigneron a précisé que le prix d'une carte dépend de nombreux facteurs et que les prix annoncés englobent souvent plusieurs éléments (le prix de fabrication de la carte, le coût de son émission, et le coût du système - ou son amortissement). Dans les projets traités par Axalto, la partie carte représentait de 30 à 50 % du total du projet. Parmi les paramètres importants pour le prix de revient de la carte, il convient de prendre en compte le volume, la taille mémoire, les éléments graphique et personnalisation ainsi que la standardisation. M. Vigneron a donné des exemples de coûts de carte allant des coûts les plus bas (en Belgique coût de 10€, proche du prix de revient car le prix de revient d'une carte est toujours à un chiffre) aux plus élevés (Royaume-Uni : 35£) en passant par des coûts moyens (Italie : 25 à 30 €). M. Vigneron a précisé

que la carte d'identité électronique en Finlande coûte 40 € mais que, du fait de son caractère non obligatoire, elle ne se vend pas et se développe peu

7.3. Le ministère de l'intérieur a rappelé que la délivrance des cartes d'identité et des passeports coûte actuellement 180 millions d'euros par an. Le ministère a souhaité rapporter ce chiffre à celui annoncé par Dominique de Villepin le 12 avril dernier : 205 millions d'euros. Le ministère estime que l'écart va progressivement diminuer et la carte coûter de moins en moins cher au regard des économies escomptées (diminution de la fraude, simplification et automatisation de certains actes, gains de temps....).

7.4. M. Cabal a estimé, en tant que parlementaire, intéressant de songer à ne rendre la carte payante qu'en cas de renouvellement ou perte.

7.5. Mme. Marzouki estime que la carte doit demeurer non obligatoire et doit continuer d'être délivrée gratuitement. Elle précise que la décision de rendre la carte obligatoire n'avait pas été envisagée depuis le régime de Vichy et que le fait de la rendre payante introduit un caractère discriminatoire et une rupture d'égalité des citoyens devant la loi.

8. Sur le lieu de délivrance de la carte et sur la perte/vol de la carte

8.1. Le ministère de l'intérieur a annoncé qu'en raison du coût, mais aussi pour des raisons de sécurité et de charge de travail pour les petites collectivités, il serait impossible d'équiper les 36.500 communes françaises. Le projet prévoit donc de se concentrer l'émission et la délivrance de la nouvelle carte sur quelques centaines de mairies. Afin que les petites collectivités locales ne soient pas défavorisées, des dispositifs de stations d'acquisition mobiles devraient être déployés ; cela permettra également la délivrance de la carte pour les personnes ne pouvant se déplacer (personnes handicapés, personnes âgées, prisonniers...). Le ministère précise que l'Etat financera les appareils de transmission des actes d'état-civil, mettra en place de l'internet sécurisé haut débit dans chaque lieu de délivrance et indemniserà les collectivités pour cette nouvelle tâche.

8.2. A la question de savoir ce qui est prévu en cas de perte ou de vol de la carte, le ministère a précisé qu'un centre d'appel recevra 24h/24 les demandes d'opposition et que le certificat embarqué sur la carte sera immédiatement désactivé. Lors d'un usage de la carte sur internet, les interlocuteurs pourront vérifier, sur une liste tenue par le ministère de l'intérieur, que la carte n'est pas en opposition.

9. Sur les scénarios alternatifs

9.1. Mme. Marzouki a précisé qu'IRIS considèrerait comme acceptable une alternative présentant les caractéristiques suivantes :

- En termes de finalités et d'usages :
 - * La CNIE doit uniquement permettre d'authentifier le porteur (la personne est bien celle qu'elle prétend être), à l'exclusion de toute possibilité d'identification d'un individu anonyme parmi une population.
 - * La CNIE ne doit pouvoir faire l'objet d'aucune autre utilisation. Les certificats de signature électronique et autres utilisations individuelles doivent être complètement dissociés de la carte, de son support et de sa gestion.
 - * Si la carte doit comporter une puce, celle-ci ne doit servir qu'à authentifier la carte comme étant un document non falsifié.
 - * Si la carte doit comporter une puce pour l'authentification du document, la lecture de cette puce ne doit pas se faire sans contact.
- En termes de données contenues dans la carte et dans les fichiers d'état civil :

* La carte ne doit comporter aucun élément biométrique (cf. l'Italie a développé une carte électronique où les empreintes digitales sont facultatives ; la Belgique propose une carte sans biométrie mais avec base centrale, ce pays disposant d'un Registre national de la population).

* La photographie du titulaire de la carte ne doit pas figurer sous forme numérisée dans la puce, mais uniquement de manière visible sur la carte pour identification par un contrôleur humain.

* Il ne doit pas y avoir de constitution de base de données centralisée (par exemple en Italie la carte fonctionne sans base centrale).

Cinquième étape du débat public itinérant

Rennes, le 11 mai 2005

La cinquième étape du débat public qu'organise le Forum des droits sur l'internet autour du projet de carte d'identité électronique s'est tenue le 11 mai 2005 à Rennes, à la « Maison du Champ de Mars ».

Le Forum des droits sur l'internet avaient invité cinq personnalités à intervenir : Annie Blandin, maître de conférence à Ecole Nationale Supérieure des Télécommunications de Bretagne, Emmanuel-Alain Cabanis, Professeur de médecine et Président de la société de Biométrie Humaine, Simon Chignard, Vice-Président de l'association multimédia BUG, Martial Gabillard, Président de l'Association des villes et collectivités pour les communications électroniques et l'audiovisuel (AVICCA), Vania Joloboff, Silicomp – AQL, société d'ingénierie en informatique.

La Direction de programme INES (Identité Nationale Electronique Sécurisée) du ministère de l'Intérieur était représentée par Sophie Planté, adjointe au directeur.

La séance a été animée par Jean Gonié, juriste au Forum des droits sur l'internet.

Les interventions et les échanges avec la salle ont abordé les points suivants :

1. Sur l'utilité de l'instauration d'une carte d'identité électronique et sur les risques en matière de vie privée.

1.1. M. Cabanis définit la biométrie comme étant la mesure du vivant (du grec bio – vivant, et metros – mesure) et donc une activité de la médecine qui mesure une partie du corps. Il estime ensuite que l'on a toujours eu recours à la biométrie et précise que la grande différence réside actuellement dans l'introduction de l'informatique qui multiplie la puissance de la biométrie.

1.2. M. Cabanis estime que l'introduction de l'informatique révolutionne également notre rapport aux libertés individuelles. Il estime que, contrairement à ce que l'on entend souvent, l'informatique renforce nos garanties, nos droits, car elle protège les données personnelles. Dans le cas de la biométrie, le recours à l'électronique protège notre identité en faisant en sorte qu'on ne la confond pas avec celle de notre voisin ou celle d'un usurpateur intentionnel. C'est ce qu'il appelle le « paradoxe de la liberté » : le fait de pouvoir être connu, identifié avec certitude permet à un être humain de garantir son identité et ainsi d'être libre car démontrer son unicité s'est affirmer sa différence vis-à-vis des autres.

1.3. M. Gabillard considère que les enjeux abordés lors du débat public sont de la première importance car ils touchent à l'identification même des individus. A ce titre, il estime que le débat public doit se poursuivre encore quelques mois, de nombreux points demeurant encore flous et de nombreuses questions sans réponses ; un débat mené avec précipitation donnerait l'impression que tout est bâclé, voire déjà décidé. Or, dans ce domaine très sensible de l'identité il convient qu'un consensus national soit recherché.

1.4. M. Chignard considère également qu'au regard des enjeux, on ne sait ni les raisons profondes pour lesquelles un tel projet est mis en place (lutte contre le terrorisme, développement des échanges en ligne ?...) ni où est l'urgence dans l'adoption de ce texte. Cela donne une impression générale de confusion dans les objectifs. Il se demande

si un tel projet aurait été accepté il y a trente ans (cf. projet SAFARI en 1974) ou même dix ans.

1.5. Partant du fait que le concept de la CNIE introduit de nouveaux éléments dans la vie d'un citoyen (biométrie, signature électronique etc.), M. Chignard estime important de mettre en place des moyens de sensibiliser et d'informer ces derniers. A ce titre, il propose qu'une telle sensibilisation commence par avoir lieu auprès des jeunes dans le cadre de la Journée d'appel et de préparation à la Défense. Cette proposition a été accueillie avec le plus grand intérêt par le ministère de l'intérieur.

2. Le lien entre carte nationale d'identité électronique et passeport biométrique

2.1. Mme. Blandin a rappelé que le projet de CNIE a un double rattachement à la politique européenne. Par sa fonction principale, la certification de l'identité, il s'inscrit dans le cadre d'obligations définies au niveau communautaire. Dans sa fonction subsidiaire, en tant qu'outil permettant d'accéder à des téléprocédures et à des transactions électroniques, il répond aux incitations prévues par les actions au titre du développement de la société européenne de l'information.

2.2. Mme. Blandin estime que la question de savoir dans quelle mesure le projet de CNIE s'inscrit dans le cadre d'obligations communautaires est déterminante. En matière de passeports et autres documents de voyage, la France doit en effet appliquer le règlement du 13 décembre 2004 établissant des normes pour les éléments de sécurité et les éléments biométriques intégrés dans ces documents délivrés par les Etats membres. Deux identifiants biométriques sont à intégrer successivement (photo faciale puis les empreintes digitales). Le règlement, destiné à protéger les documents contre la falsification, est un approfondissement de l'acquis de Schengen dans le contexte de la gestion de « l'après 11 septembre ». Il a pour base juridique l'article 62 du Traité CE et ne requiert à ce titre que l'avis du Parlement, ce qui a facilité son adoption « dans l'urgence ».

2.3. Mme. Blandin précise que ce règlement ne s'applique pas à la carte d'identité nationale : l'article 1 du règlement exclut la carte de son champ d'application. Dès lors, la non extension du débat au projet de passeport s'expliquerait par le caractère directement applicable du règlement. Elle note que cette interprétation stricte semble toutefois être en contradiction avec les finalités du règlement. En effet, bien que relevant a priori de la compétence nationale, la carte d'identité est aussi un document de voyage. La directive du 29 avril 2004 est claire sur ce point puisqu'elle prévoit que tout citoyen a le droit de se rendre dans un autre Etat membre en disposant d'une carte d'identité ou d'un passeport. Le règlement est donc susceptible de s'appliquer à la CNIE. Le lien entre CNIE et passeport est d'ailleurs fait par le gouvernement lui-même puisqu'il prévoit une procédure identique en matière de délivrance des cartes et des passeports et qu'il aligne les exigences biométriques pour les cartes sur celles du passeport (sans contact etc.). Juridiquement en revanche, l'interprétation stricte peut conduire à des discriminations en matière de libre circulation des personnes dans l'Union. Tel est le cas si un Etat se fonde sur une interprétation similaire en limitant au contraire le nombre d'éléments biométriques insérés dans la carte à un seul ou n'en prévoyant pas du tout (cf. Belgique, Italie...).

2.4. Mme. Blandin se demande si l'enjeu véritable de cette interprétation ne réside pas dans la délimitation des compétences nationales et communautaires. Si l'interprétation large de la portée du règlement l'emporte, cela signifie que l'exercice de la compétence nationale en matière de cartes d'identité est subordonné à la mise en œuvre de la compétence communautaire en matière de passeports. A l'inverse, l'interprétation stricte conduirait à subordonner la compétence communautaire à la compétence nationale. A ses yeux, c'est bien le sens du débat en cours. Les citoyens sont appelés à débattre du projet et au lieu de s'exprimer essentiellement sur les éléments de différenciation de la carte par rapport au passeport, on discute surtout des implications de la biométrie sur les

données personnelles et la vie privée. Dans ces conditions, elle estime que, si un rejet se manifeste, on ignorera dans quelles conditions on appliquera le règlement s'agissant des passeports. En revanche, si le projet suscite des réactions favorables, le règlement bénéficiera d'une légitimité au plan national.

3. Sur la biométrie

3.1. M. Cabanis précise que l'on peut éventuellement avoir des informations médicales par une identification par l'iris de l'œil (l'iris peut changer de couleur avec l'absorption de certains médicaments). Il a néanmoins estimé que l'iris est plus fiable que les empreintes. A cet égard, et reprenant des chiffres avancés dans le rapport du député Cabal (cf. débat de Lille), il a précisé que le FAR (« *False Acceptation Rate* », c'est-à-dire le taux qui détermine la probabilité pour un système de « reconnaître » une personne qui normalement n'aurait pas dû être reconnue) est plus fort pour les empreintes digitales (0,008%) que pour l'iris (0,0001%). De même, le FRR (« *False Rejection Rate* », le taux qui déterminent la probabilité pour un système donné de ne pas « reconnaître » une personne qui normalement aurait dû être reconnue) est plus fort pour les empreintes digitales (2,5%) que pour l'iris (0,25%). La reconnaissance faciale est la moins fiable (respectivement 0,45% pour le FAR et 17% pour le FRR).

3.2. M. Joloboff a précisé que les empreintes ne doivent pas servir à signer ou valider une transaction électronique, notamment parce que la biométrie n'est pas une méthode confidentielle (laisse traces) et c'est une méthode rigide (car pas révocable ; on peut changer un mot de passe, pas les empreintes). Il a également précisé que les empreintes qui seront prises pour la CNIE seront des empreintes dites « plates » (prises par scanner) à la différence des empreintes « roulées » établies dans le cadre judiciaire. Il estime de ce fait, qu'il ne sera pas possible d'exploiter de manière croisée des fichiers constitués sur la base de données différentes (empreintes plates/empreintes roulées), ce qui protégerait les données personnelles données dans le cadre d'INES.

4. Sur l'accès aux données et les personnes habilitées à consulter les données

4.1. Le ministère de l'intérieur a précisé que l'accès à la base ne se fera que par des personnes habilitées. Tous les accès à la base donneront lieu à un « journal » (qui retrace les interrogations faites). La CNIL et les magistrats auront un droit d'accès indirect aux données. Les personnes habilitées seront les agents qui rentreront les données pour la délivrance des titres. Ils n'auront un accès à la base qu'en mode écriture, et limité aux données alphanumériques (nom, prénoms etc...) et à la lecture de la photo. Ils ne pourront ni consulter les empreintes digitales, ni lire les données personnelles d'un autre individu. En outre, sous le contrôle du procureur de la république, les officiers de police judiciaire pourront accéder à la base dans le cadre de leurs missions de contrôle de l'identité des personnes (article 78-2 du code de procédure pénale) et de vérification d'identité (article 78-3 CPP).

4.2. Par ailleurs, le ministère de l'intérieur a précisé que, s'agissant de l'accès aux données de la puce du titre, il sera « hiérarchisé » selon le caractère confidentiel des informations contenues. Pour les empreintes digitales, seules les forces de police pourront les lire. Pour ce qui est des données de l'état-civil, de l'adresse etc ... le titulaire de la carte, en saisissant son code PIN pourra donner accès aux administrations qui en auraient besoin dans le cadre des téléprocédures administratives.

5. Sur le contrôle du système

5.1. M. Gabillard estime que la CNIL a un rôle fondamental à jouer dans le cadre du contrôle du système, sous réserve qu'elle ait la possibilité de le faire. Pour cela il lui faut non seulement plus de moyens humains mais surtout plus de pouvoir de contrôle notamment a posteriori. Sans la mise en place d'une CNIL renforcée, le projet ne doit pas voir le jour. A l'opposé, d'autres personnes ont noté que, dans les faits, même avec des

moyens renforcés, la CNIL n'aura jamais la possibilité d'exercer un contrôle effectif du système.

5.2. Mme. Blandin estime que ce serait une erreur que d'espérer que tous les problèmes de contrôle du système seront résolus en donnant davantage de moyens à la CNIL. Elle rappelle que la Directive européenne du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données n'a été transposée qu'en août 2004 (le délai est normalement de trois ans). Dans cet esprit, elle ne voit pas comment il sera possible de modifier dans un délai raisonnable le statut et les pouvoirs de la CNIL pour lui donner les moyens de contrôler le système. Par conséquent, elle propose que soit menée une réflexion sur le principe de précaution appliqué aux nouvelles technologies.

5.3. M. Chignard propose que 5% du budget annuel du projet INES (205 millions d'euros) soient sanctuarisés à des fins de contrôle du système. Cette proposition a été accueillie avec le plus grand intérêt par le ministère de l'intérieur.

5.4. Certains ont noté que des agents de l'administration opèrent déjà des utilisations indues vers tous types de fichiers. A cet égard, ils craignent le risque d'une évolution possible de l'usage de la base de la CNIE par les pouvoirs publics par le biais d'un élargissement du contenu de la base à d'autres données ou de l'accès à d'autres agents.

6. Sur la sécurité de la carte et du système et la lecture « sans contact » des données

6.1. Silicom – AQL est une société d'ingénierie en informatique agréée par le ministère de la Défense comme centre d'évaluation de la sécurité des technologies de l'information (CESTI) dans le domaine « techniques informatiques et réseaux » ; à ce titre, M. Joloboff estime que le projet actuel de carte mérite d'être questionné sur quatre points :

1. Si la carte est dotée d'une signature électronique se pose le problème de la durée de validité de la clé de signature (comment la renouvelle-t-on ?....)
2. Comment peut-on garantir qu'entre le moment où les données seront saisies et celui où la carte sera fabriquée, aucune interférence ou fraude n'intervienne ? A cet égard, M. Joloboff estime notamment que, pour des raisons de sécurité, il convient de limiter au maximum le nombre de centres de saisies et de fabrication.
3. Il pourrait être possible de lire, à l'insu de la personne les données inscrites dans la carte (cf. aspect sans contact de la carte). A cet égard, il convient que le ministère de l'intérieur précise les moyens envisagés pour empêcher cela.
4. La mise en place de la biométrie entraîne le problème de la traçabilité : des entreprises privées pourraient relever des traces d'empreintes et se constituer ainsi des fichiers d'empreintes digitales.

6.2. Certains ont remarqué qu'il existe actuellement de nombreuses techniques permettant de passer outre les mécanismes de sécurité reposant sur la biométrie (exemple d'un chercheur japonais qui a fabriqué avec de la gélatine de [vraies-fausse empreintes digitales](#) qui ont leurré 11 des 15 systèmes biométriques testés). Sur ce point, le ministère de l'intérieur a assuré qu'il existe des moyens de se prémunir de ce type de manœuvre par l'acquisition de matériels suffisamment pointus et fiables. En outre, toute utilisation des titres lors des contrôles aux frontières, ou des contrôles d'identité, se fait et demeurera sous le contrôle d'un agent. Le ministère met en avant le facteur humain qui est, à ses yeux, une sécurité supplémentaire contre l'utilisation de fausses empreintes.

6.3. A ceux qui s'inquiètent de la possibilité de lecture sans contact de la carte, le ministère a rappelé que ce choix n'est pas encore acté. Il a aussi été rappelé qu'en plus d'un contrôle d'accès basique (qui donne une autorisation de lecture sans contact seulement s'il y a une vision optique préalable de la bande MRZ - « Machine Readable

Zone » - ce qui rend une lecture à travers un sac impossible), le projet de passeport européen prévoit un contrôle d'accès étendu pour les empreintes digitales (celles-ci ne seront lisibles que pour les agents qui disposeront d'un matériel spécifique et avec un second niveau de sécurité).

7. Sur le caractère obligatoire de la carte

7.1. A la question de savoir à partir de quel âge la carte nationale d'identité électronique sera obligatoire, le ministère a répondu que le choix définitif n'est pas encore arrêté : ce sera soit à partir de la majorité pénale (13 ans), soit à partir de 18 ans (dans tous les cas pas à partir de 12 ans comme en Belgique).

8. lieu de délivrance de la carte

8.1. Souhaitant préciser le choix qui a été fait de ne retenir que quelques centaines de mairies comme lieu de délivrance de la carte, le ministère de l'intérieur a rappelé que des milliers de communes ne délivrent le plus souvent qu'un titre par jour. Il est important, pour le ministère de l'intérieur, qu'un juste équilibre entre aménagement du territoire et sécurité du système soit trouvé.

9. Sur les services associés à la carte

9.1. M. Gabillard estime que la carte d'identité électronique pourrait être un outil pratique créateur de confiance dans les rapports humains. Il considère que si l'Etat ne met pas en place un tel projet et ne développe pas une offre dans le domaine de l'administration électronique et des certificats, le secteur privé risque de s'emparer de ce domaine. Il précise que le secteur de l'administration en ligne doit rester le fait de la puissance publique afin d'éviter une privatisation rampante des services qu'offre l'Etat et une remise en cause consécutive des exigences de service public.

9.2. M. Gabillard estime que si la carte doit être obligatoire, elle doit être gratuite. Selon lui, l'argument selon lequel depuis que la carte est gratuite elle est davantage perdue ne tient pas : on ne perd pas une carte qui sert réellement dans la vie de tous les jours.

9.3. Mme. Blandin estime que l'ajout d'autres fonctions dans la carte est ce qui différencie la carte et justifie le débat. A ses yeux, cette fonction subsidiaire de la carte appelle trois points :

1. La légitimité de l'intervention de l'Etat dans la sphère marchande, de son intervention directe es qualité sur le marché dit de la confiance. Elle estime que l'on est ici à contre-courant de la tendance actuelle qui consiste à exclure un nombre croissant d'activités du champ de la sphère publique lorsqu'elles sont de nature économique (conformément à la définition large en droit communautaire de ce type d'activités). Cette définition pose le problème des limites entre activités économiques et activités relevant de l'exercice de l'autorité publique. En les franchissant, l'Etat s'expose à ce que l'on reformule la question initiale de la légitimité de l'intervention publique dans la sphère marchande en se demandant, au contraire, si ce n'est pas la certification d'identité qui pourrait être une activité d'entreprise : on peut ainsi se demander si un certificat garantissant l'identité d'état-civil peut faire office de CNIE.

2. Ce faisant, l'Etat, qui serait son propre certificateur, entre en concurrence avec des prestataires de services de certification (PSC). Et il dispose d'un avantage en terme d'accès au bloc « identité » qui est réservé aux autorités habilités par lui. Le risque n'est donc pas nul de voir émerger un monopole de la certification qui fausserait la concurrence sur ce marché ou de voir les prestataires privés revendiquer un accès au bloc « identité » confidentiel.

3. Dans le cadre de la signature électronique, le certificat fourni par l'Etat n'est pas un certificat comme les autres : ce sont des certificats de haut niveau qui seront insérés dans la carte. Au-delà des exigences en matière de preuve et de validité des écrits, la signature électronique (avec identification forte) et l'identification authentifiée risquent donc d'être utilisées à tout propos sous la pression éventuelle de destinataires imposant le recours aux certificats de la CNIE.

Sixième étape du débat public itinérant

Marseille, le 25 mai 2005

La sixième étape du débat public qu'organise le Forum des droits sur l'internet autour du projet de carte d'identité électronique s'est tenue le 25 mai 2005 à Marseille, à l'Hémicycle de la communauté urbaine.

Autour de Madame Falque-Pierrotin, présidente du Forum des droits sur l'internet intervenaient cinq personnalités : Eric Caprioli, Avocat, membre de la délégation française auprès des Nations Unies sur les questions de commerce électronique, Olivier Chavrier, Directeur de la division identité et sécurité, Gemplus, Xavier Guchet, sociologue, Université Paris I, Christophe Jolivet, membre du bureau du Club de la Sécurité des Systèmes d'Information Français, Daniel Kaplan, délégué général, Fondation Internet Nouvelle Génération.

La Direction de programme INES (Identité Nationale Electronique Sécurisée) du ministère de l'Intérieur était représentée par Sophie Planté, adjointe au directeur.

La séance a été animée par Jean Gonié, juriste au Forum des droits sur l'internet.

Les interventions et les échanges avec la salle ont abordé les points suivants :

1. Sur l'instauration d'une carte nationale d'identité électronique et sur les risques en matière de vie privée

1.1. M. Caprioli rappelle qu'identifier consiste à exprimer l'identité d'une personne. Celle-ci recouvre l'ensemble des composantes grâce auxquelles il est établi qu'une personne est bien celle qui se dit (nom, prénoms, nationalités, filiation...), ainsi que tous les traits juridiquement pertinents qui se retrouvent aussi bien dans le numéro national d'identification attribuée par l'INSEE que sur la carte nationale d'identité délivrée par le ministre de l'intérieur. Il rappelle que Gérard Cornu définit l'identité comme « *ce qui fait qu'une personne est elle-même et non une autre ; par extension ce qui permet de la reconnaître et de la distinguer des autres ; l'individualité de chacun, par extension, l'ensemble des caractères qui permettent de l'identifier.* ».

1.2. M. Kaplan estime qu'il existe des risques de dérives lentes dans l'utilisation des fichiers par l'administration : la tentation de croiser les données de divers fichiers se fera en effet, certes progressivement, mais de façon certaine. Il rappelle que le but de la CNIL est, justement, qu'un système n'atteigne pas son point maximal d'activité ; c'est pour cela que tout système doit comporter, voire admettre, un degré d'erreurs et d'inefficience.

2. Sur la biométrie

2.1. M. Caprioli rappelle qu'en matière biométrique, la loi Informatique et Libertés s'applique. Il fait connaître un jugement du TGI de Paris du 19 avril 2005 qui a interdit la mise en place d'un système de contrôle du temps de travail par le biais des empreintes digitales. Les juges ont rappelé que l'empreinte digitale n'est pas une donnée comme les autres puisqu'elle « *permet d'identifier les traits physiques spécifiques qui sont uniques et permanents pour chaque individu* ». Elle doit donc être traitée avec une grande vigilance. « *Son utilisation qui met en cause le corps humain et porte atteinte aux libertés individuelles peut cependant se justifier lorsqu'elle a une finalité sécuritaire ou protectrice de l'activité exercée dans les locaux identifiés* ». Pour ce faire, il se fonde sur l'article L. 120-2 du code du travail qui prévoit qu'on ne peut porter atteinte aux libertés

sauf si c'est justifié par la nature de la tâche à accomplir et proportionné au but recherché. Les juges s'appuient également sur la directive européenne sur la protection des données personnelles qui reprend ces principes pour refuser le recours à cet identifiant.

2.2. A cet égard, M. Caprioli estime que les données biométriques devront être embarquées dans la puce de la carte. La gestion des données de la personne physique ne devrait pas être centralisée au sein d'une base de données.

2.3. Après avoir rappelé que l'on a trois moyens de s'authentifier (avec ce que l'on sait – code PIN – avec ce que l'on a - carte bleue – avec ce que l'on est – biométrie), M. Jolivet estime que tout système biométrique doit prendre en compte trois éléments. Tout d'abord, le degré d'acceptabilité pour les utilisateurs, ensuite la vitesse d'acquisition des données, enfin la précision d'un système : ce dernier doit être suffisamment sensible afin de réduire au minimum le taux de faux rejets (le taux qui détermine la probabilité pour un système de ne pas « reconnaître » une personne qui normalement aurait dû être reconnue). Concernant INES, il insiste sur la nécessité de dupliquer la base centrale afin d'obtenir une continuité du service en cas de panne.

2.4. A partir des travaux qu'il a mené sur la biométrie, M. Guchet a constaté que la mise en place des techniques biométriques dans les écoles ou encore aux Aéroports de Paris n'entraîne ni craintes ni réactions particulières mais révèle au contraire une certaine atonie sociale. Il précise cependant que la relativement bonne acceptabilité sociale de ces techniques ne signifie pas pour autant que la requalification biométrique de l'identité est sans problème. A une question qui lui signifiait que les expériences décrites ne concernent qu'une faible partie de personnes, M. Guchet reconnaît qu'il est impossible, en l'état, de savoir si la biométrie sera bien acceptée à l'échelle d'une population : il recommande à cet effet une analyse précise des usages.

2.5. M. Guchet note que la biométrie n'est pas un outil au service de problématiques purement techniques, elle est aussi un instrument de pouvoir car elle s'accompagne de rapports de force et de changements qui modifient la nature même du pouvoir qui s'exerce sur les gens. Ce thème est apparu fortement dans le contexte scolaire où la biométrie inaugure un type de pouvoir et de contrôle social assez nouveau qui ne passe plus forcément par les surveillants traditionnels et s'appuie sur d'autres relais. Il remarque que le fait de prendre acte de la nature politique de la biométrie ne signifie pas pour autant que la biométrie menace de nous asservir mais de comprendre ses conséquences.

2.6. M. Guchet estime que la biométrisation de l'identité contribue à modifier en profondeur l'identité elle-même, c'est-à-dire la manière dont on la définit et la manière dont elle se construit. La biométrie signifie que l'identité est indissociable d'un processus d'identification, qui est un processus technique de contrôle. Il estime que c'est là où se situe la nouveauté. Traditionnellement, l'identité se détermine plutôt à partir d'un processus de reconnaissance. L'identité sociale, construite dans un processus de connaissance ou de reconnaissance, n'est pas une identité techniquement mesurable ; l'identité biométrique, c'est l'identité construite via des techniques de mesure. Ce qui est intéressant dans la biométrie, ce n'est pas de réfléchir à l'identité en soi, mais au processus à partir duquel cette identité se détermine ; c'est la notion que l'on a de l'identité qui se trouve ainsi bouleversée en profondeur.

3. Sur l'accès aux données

3.1. Le ministère de l'intérieur a précisé que l'accès du citoyen aux données contenues sur la puce se fera par le biais d'un accès direct, probablement à partir de bornes installées dans les lieux de délivrance des titres. En revanche, l'accès au contenu de la base se fera par le biais d'un accès indirect, ce mode d'accès étant celui réservé aux

fichiers gérés habituellement par le ministère de l'intérieur. Un accès direct ne peut être envisageable car, outre les données d'état-civil et biométriques, la base contiendra le « journal » des consultations de la base réalisées par les agents habilités.

4. Sur la sécurité du système et sur la signature électronique

4.1. M. Caprioli estime qu'une identité sécurisée doit répondre à différentes conditions afin de prouver la fiabilité du procédé d'identification. Il rappelle que la loi du 9 décembre 2004 prévoit dans son article 3 une ordonnance dont l'objectif est d'assurer la sécurité des informations échangées par voie électronique entre les usagers et les autorités administratives et de favoriser la signature électronique des actes des autorités administratives. Il rappelle également que cette loi prévoit qu'un référentiel général de sécurité définisse des exigences de sécurité pour différentes fonctions qui contribuent à la sécurité des informations échangées par voie électronique (notamment fonctions de signature électronique). Au vu des fonctions de la carte telles que présentées par le ministère de l'intérieur, M. Caprioli se demande si la CNIE entrera dans le cadre de ce référentiel de sécurité, ce qui serait souhaitable.

4.2. A titre liminaire M. Chavier a rappelé qu'un système sécurisé à 100% n'existe pas. Pour autant, il estime que l'introduction des cartes à puce a renforcé la sécurité. En effet, introduites dans les années 1990 pour le paiement, elles ont permis une diminution de 80% des fraudes au paiement bancaires alors que, dans le même temps, les volumes de paiement augmentaient de 120%. De plus, la carte associée à un code PIN permet une sécurité accrue dans l'accès aux données. Dans ce cadre, une carte d'identité électronique fondée sur une carte à puce et de la signature électronique permettra une authentification sécurisée sur le net. Enfin, si l'on veut davantage de garanties sur la sécurité d'un système, il convient que celui-ci fasse l'objet d'évaluation par des laboratoires indépendants puis de certification par un autre organisme.

4.3. Il a été remarqué que l'usage de la carte à des fins d'authentification pour des transactions commerciales est risqué pour les ordinateurs familiaux qui ne sont pas assez sécurisés et font l'objet de nombreuses attaques.

5. Sur les usages

5.1. M. Caprioli, notant que l'Etat sera sa propre autorité de certification, estime que l'étendue de sa responsabilité sera difficilement mesurable. De façon générale, l'Etat sera responsable (certificats défaillants, failles de sécurité...) de la fiabilité du procédé de signature électronique : outil de signature (système clé asymétrique) et certificat. Dans le cadre d'une authentification sur des services marchands, M. Caprioli estime que l'on pourrait limiter la valeur d'usage du certificat : pour toute transaction au-delà d'une certaine somme le certificat ne serait plus valable. La responsabilité de l'Etat ne serait ainsi engagée que dans le cadre de cette somme (transaction de 10.000 euros par exemple).

5.2. M. Kaplan estime que le développement d'une carte « signeuse » est dangereux et présente des risques. En effet, parce que la CNIE bénéficiera d'un statut officiel et qu'elle proposera un dispositif très fort d'authentification et de signature, elle risque d'inciter un grand nombre d'acteurs à se reposer sur elle pour leurs relations avec des tiers (clients, fournisseurs, usagers, partenaires...).

5.2. Or, M. Kaplan note qu'une telle évolution ne serait pas neutre. Les relations humaines reposent depuis toujours sur une part, souvent prépondérante, de confiance. Dans certains cas, le fait de ne pas exiger de preuve d'identité ou de signature peut même constituer le ciment d'une relation forte et durable, le signe d'une confiance réciproque. Si le recours, a priori commode, à la CNIE contribue à faire basculer ces relations de l'informel au formel, de la confiance à la sécurité, cela peut avoir des

conséquences sur les relations sociales. Trop sécuriser une relation enlève paradoxalement de la confiance. En outre, le marché balbutiant des services de confiance sera nécessairement touché par l'émergence d'un dispositif de référence tel que la CNIE ce qui risque, à terme de nuire à l'innovation.

6. Sur le processus du débat

6.1. Certains ont regretté que le débat public ne fût pas assez connu. De façon générale, beaucoup ont souhaité que le débat sur la carte nationale d'identité électronique puisse se prolonger car il est fondamental d'informer et de recueillir les avis des Français sur un tel projet.

Contact : contact@foruminternet.org