

Carte nationale d'identité électronique

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'immuabilité : 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 montrées 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.