

DEBAT NATIONAL SUR LA CARTE D'IDENTITE ELECTRONIQUE

Synthèses des débats en ligne

* * *

Synthèse de la première semaine de débats - 8 février 2005	1
A propos de la lecture « sans contact » de la carte et la création d'une base d'empreintes digitales numérisées - 24 février 2005.....	7
Deuxième synthèse des contributions des internautes du 8 février au 29 mars 2005.....	9
Synthèse des contributions des internautes sur le thème « biométrie » du 29 mars 2005	16
Synthèse des contributions des internautes sur le thème « vie privée » du 22 avril 2005	20
Synthèse des contributions des internautes sur le thème « sécurité » du 27 mai 2005	28

* * *

SYNTHESE DE LA PREMIERE SEMAINE DE DEBATS - 8 FEVRIER 2005

Bonjour à toutes et à tous,

Après une semaine de débats, il est important de faire une première synthèse des échanges qui ont été menés. D'autant plus que ces échanges ont été nombreux (plus de 1000 messages dont près de 600 contributeurs uniques) et de qualité ! Nous tenons d'ailleurs, à remercier tous les intervenants pour leur participation active qui confirme bien la nécessité d'un tel débat. Nous rappelons qu'un dossier de présentation du projet est disponible sur ce site (<http://www.foruminternet.org/telechargement/forum/pres-prog-ines-20050201.pdf>).

Les discussions portent, tout d'abord, sur le principe même de l'instauration d'une carte nationale d'identité électronique.

D'emblée, un certain nombre d'intervenants refusent d'entrer dans le détail du projet et de répondre aux modalités proposées car ils s'opposent, à titre préalable, à l'idée même de mise en place d'une carte avec des données biométriques. A leurs yeux, cette carte pourrait préfigurer la possibilité de fichier les individus, de recouper diverses informations et, à terme, de voir l'apparition d'une administration orwellienne (spectre du « Big Brother »). Ils craignent également avec cette carte d'être « tracés ». A cet égard, de nombreuses discussions ont eu lieu entre les internautes. A ceux qui notent que ce

traçage existe déjà de facto dans la vie de tous les jours (carte bancaire, téléphone portable...), d'autres répondent que le risque n'est pas le même car avec ce projet ce serait l'Etat qui mettrait en place un tel principe (cf. « Big Brother »).

Ainsi, avant même de savoir quelles modalités pourraient entourer la mise en place de la CNIE, ces intervenants souhaitent savoir dans quelles mesures il est possible de revenir sur ce projet et sur l'état d'avancement du programme INES.

Pour ces participants, le projet de CNIE ne se justifie donc pas et les avantages supposés (lutte contre le terrorisme et la fraude, simplification administrative...) sont loin d'être vérifiés et peuvent être dangereux pour l'individu.

A ces craintes s'ajoutent des interrogations.

Un grand nombre de participants se demande à quoi sert la biométrie et comment elle va être utilisée, quelles informations seront stockées dans la carte et comment elles seront protégées, ou encore soulève le risque d'interconnexions de données administratives entre elles et avec la sphère privée.

I. Les principales interrogations et leurs réponses par le ministère de l'intérieur

1) Que mettra-t-on comme informations me concernant dans la carte ?

De nombreuses interrogations et craintes ont été relevées (ADN, informations de santé, groupe sanguin, relevés bancaires etc.). L'aspect « données de santé » est revenu à de nombreuses reprises, beaucoup d'intervenants craignant que l'existence de telles données sur la carte n'entraîne des discriminations. De l'autre côté, il convient de préciser que d'autres souhaitent, au contraire, que des données de santé (groupe sanguin par exemple) puissent figurer sur la carte car en cas d'accidents cela faciliterait les transfusions.

A ces interrogations, le ministère de l'intérieur a rappelé que le projet prévoit que la puce contiendrait les éléments traditionnels imprimés (nom, prénom, adresse, date de naissance, etc), la photo, les empreintes digitales, le tout crypté pour en empêcher l'accès à l'insu du porteur. Ces éléments sont destinés aux contrôles légaux (contrôle d'identité, passage de frontière). De plus, la carte contiendrait des outils cryptographiques (« clefs » et « certificats » électroniques) permettant, si on le souhaite et grâce à un code secret, de s'identifier sur internet (par exemple pour accéder de manière sécurisée à des téléprocédures), et de signer électroniquement des documents.

Le Ministère a enfin rappelé que la carte ne contiendra aucune donnée sanitaire ou sociale (ni « numéro de sécu », ni dossier médical), et n'aura aucun lien avec la carte Vitale. Elle ne servira pas non plus de carte de paiement.

2) Qui aura accès aux informations stockées sur ma carte ?

Des interrogations liées à l'accès aux données stockées sur la carte et aux personnes pouvant y accéder ont été souvent posées. Citons, par exemple celles de vincemdk : « qui pourra avoir accès aux données ? Sous quelles réserves d'habilitations ? Les données biométriques seront elles cryptées ? Quel contrôle sera exercé sur l'exercice de cette base de données d'emprunts biométriques ? Cela sera t il du ressort de la CNIL?,pourtant déjà largement débordée par ses nouvelles attributions... » et celle de AuCroqueurDesMendiants : « On aimerait bien connaître, avant de se prononcer, la liste complète des autorités qui, dans chaque pays, ont ou auront accès à ces informations ».

Il a été répondu que les accès à la partie identité/biométrie et aux bases de données ne seront techniquement et juridiquement possibles qu'aux agents habilités, pourvus du matériel spécifique, pour des usages prévus par la future loi qui sera débattue par le

Parlement.

Pour le passage aux frontières, les autorités des pays concernés n'auront accès qu'aux informations d'identité/biométrie dans la puce en mode « passeport » selon lequel seuls les pays européens pourront lire les empreintes, l'identité et la photo étant elles lisibles par tout pays. Aucune autre administration, et aucun intérêt privé, n'aura accès aux bases de données du système.

3) Quelles garanties réelles existent pour prévenir un risque d'interconnexion ?

Encore une fois de nombreuses craintes. Craintes pour le présent : que, dès la mise en place de la CNIE les administrations et les services privés puissent avoir un accès aux données de cette carte. Mais aussi craintes pour le futur : peur que les données informatisées ne tombent « en de mauvaises mains » si un régime totalitaire venait à voir le jour en France... c'est ce que craint NaSH qui écrit que « si dérive il y a, ce genre de décision (la CNIE) pourrait accélérer énormément le passage à une éventuelle dictature ».

Des précisions ont été apportées par le ministère de l'intérieur. Il a été rappelé qu'il est impossible en l'état actuel en France d'envisager de telles interconnexions (cf. loi Informatique et Libertés). Par principe, les données personnelles d'un particulier ne peuvent être collectées par une administration que pour une finalité précise. On ne peut déroger à ce principe que de manière exceptionnelle. Ainsi, une administration ne peut communiquer des informations à une autre que si le transfert est prévu et encadré par la loi, dans le cadre d'objectifs limitativement définis. Ces dérogations sont soumises au contrôle de la Commission Nationale de l'Informatique et des Libertés.

II. Les avantages de la CNIE

Des intervenants ont estimé que carte portait un intérêt certain et offrait des avantages. Ainsi RC note que « la CNIE offre beaucoup d'avantages: elle est plus sûre que la carte papier, (...), elle remplace les certificats électroniques qui sont nécessaires à la réalisation des formalités administratives comme TELETVA (et qui coutent 50 € par an), elle pourrait aussi servir à s'identifier sur Internet pour la réalisation d'opérations sur les comptes bancaires (ce qui serait beaucoup plus sûr que les actuels codes secrets) ».

D'autres ont estimé que la CNIE permettrait un gain de temps pour les formalités administratives courantes, et s'inscrit dans le cadre de la modernisation de l'administration : « cette carte recèle un énorme potentiel pour faciliter la vie des citoyens et diminuer les coûts administratifs » (Aymeric77), « cette carte permettra aux utilisateurs du service public (c'est dire nous) de faciliter les démarches administratives » (vicoleboss).

Chambery note que la CNIE offrirait de « multiples avantages » comme « la sécurisation des achats par mails parce qu'on donne son numéro de carte mais aussi son numéro d'identité, son numéro fiscal pour le paiement des impôts ».

D'autres enfin, estiment que la CNIE rendrait service aux citoyens ; c'est le cas de steph29 : « si ce système est bien foutu, lorsque quelqu'un perdra ces papiers, il devrait être possible de les remplacer très vite (comme dans d'autres pays pratiquant déjà ce système). [...] - enfin un truc intelligent ».

III. Les réserves

Au-delà de ce refus de principe, de ces interrogations et de ces approbations s'ajoutent des réserves qui viennent de participants qui, sans être particulièrement hostiles au projet, insistent sur ses aspects pratiques. Ces réserves sont apparues notamment à

travers les réponses aux grands thèmes posés en introduction au débat. Trois types de réserves peuvent ainsi être dégagés :

- 1) Les réserves en termes de sécurité et de biométrie
- 2) Les réserves liées au coût de la carte
- 3) Les réserves liées à la possibilité de « fracture numérique ».
- 4) Les réserves liées à la nature même du système

1) Les réserves en termes de sécurité et de biométrie

En l'état actuel des technologies et de la sécurisation des systèmes, les internautes ont majoritairement noté qu'il sera très difficile de pouvoir assurer une sécurité à 100% de la carte. D'autres se demandent comment il sera possible de faire évoluer le système pour que le niveau de sécurité soit constamment adapté aux nouveaux risques. Enfin, d'autres se demandent, à l'instar de vincemdk, ce qu'il en est « des personnes dont les mains auraient pu être sectionnées, ou dont les empreintes ne sont pas suffisamment lisibles? ».

A ces réserves, il a été répondu que les cartes à puce sont beaucoup plus sécurisées que tout autre support (l'adoption de la puce a divisé le taux de fraude par 10 dans le secteur bancaire). Les puces actuelles ont atteint un niveau de sécurité qui n'a pas été cassé. De toute façon, l'objectif est un niveau de sécurité hors d'atteinte des fraudeurs (certains ont cité l'ordinateur quantique capable de casser la sécurité des puces. Un tel ordinateur, s'il existe un jour, ne sera en tout cas pas disponible aux fraudeurs dans les 20 prochaines années).

En ce qui concerne les personnes dépourvues d'empreintes digitales, elles constituent une exception que le système aura à gérer...

2) Les réserves liées au coût de la carte

Pour de nombreux intervenants, le projet de CNIE coûte cher et ils se demandent concrètement qui va payer : la collectivité ou l'individu lui-même ?

A cet égard, les internautes rappellent que l'actuel CNI papier est gratuite, la rendre payante serait mal perçu, les services associés ne le justifiant pas.

D'autres intervenants seraient favorables au paiement de la carte en cas de renouvellement de papier ou de perte de la carte. Beaucoup sont d'accord avec l'idée de payer une somme de l'ordre d'une dizaine d'euros pour avoir un lecteur de carte au domicile. Ainsi pour certains, il s'agit d'un faux débat : une carte gratuite est en fait payée par le consommateur/contribuable. La rendre payable par l'utilisateur permet de responsabiliser ce dernier...

A cela le ministère a souhaité préciser que, depuis que la carte est gratuite, le taux de perte a été multiplié par 10 et atteint 10% de la production.

3) Les réserves liées à la possibilité d'exclusion de certaines populations

Sur ce point trois idées principales :

1. Risque de « fracture numérique » entre ceux qui ne savent pas se servir des technologies de l'information et de la communication et les autres (personnes âgées etc.).
2. Risque de « fracture territoriale » entre les territoires desservis par l'internet haut débit et les autres.
3. Dans le cas où la CNIE serait obligatoire et payante : risques de « fracture sociale » entre ceux qui auront les moyens financiers et les autres.

De façon générale, et comme cela a été rappelé, crainte de la marginalisation de ceux qui sont les « ni-ni (ni urbains, ni jeunes) » (danyd44) et crainte d'une éventuelle « déshumanisation » des relations avec l'administration.

De plus, beaucoup sont contre le fait que la CNIE puisse éventuellement être obligatoire car, actuellement, il est rappelé qu'elle ne l'est pas. Il a néanmoins été souvent noté que si la CNIE n'est pas obligatoire cela risque de créer aussi une fracture sociale entre ceux qui ont la carte et ceux qui ne l'ont pas...

4) Les réserves liées à la nature même du système

Le débat sur le logiciel libre est vite apparu. Certains ont ainsi souhaité, que la CNIE soit « accessible sous tous les systèmes (Mac OS, Linux, *BSD, etc etc...) » (Beretta) et ont appelé à ce que soient utilisés des « standards ouverts et libres (gnu/linux etc) » (rZR).

IV. Les propositions

Un grand nombre de propositions intéressantes ont été envoyées. Parmi celles-ci, on peut par exemple retenir :

1) Les propositions en termes de garanties / protection de la vie privée

Le besoin de garanties se fait cruellement sentir. Certains ont même suggéré que soit instaurée une sorte de Commission de suivi de la mise en place de la carte pendant les premières années.

D'autres font des propositions très élaborées, par exemple celle de AAA : « Il faut rendre inaccessible les données individuelles aux personnes qui ne sont pas identifiées par le porteur de la carte comme autorisées à y accéder. Cela signifie qu'aucune de ces données ne soient stockées en dehors de la carte. Ni sur un système informatique ni même imprimée sur la carte elle-même. C'est un avantage sur la situation actuelle où la consultation de données personnelles stockées sur informatique peut se faire et se fait souvent à l'insu de la personne. De plus, l'exposition en clair des données biométriques (photo, empreinte) et personnelle (date de naissance, adresse) rend ces données accessibles à toute personne en contact avec le document papier sur lequel les données sont imprimées, que cette personne ait le droit ou pas de s'en servir. Il faut que l'accès aux données de la carte ne soit possible qu'en présence du porteur de la carte. Cette notion de présence pouvant être étendue à la consultation à distance ou à la transmission de données présente dans la carte par un réseau de données. Mais dans tous les cas, le porteur de la carte doit savoir à qui il présente ses données. Cela passe par exemple par une authentification et une présentation de l'identité du représentant de l'autorité demandant d'accéder aux données. ».

2) Les propositions en termes de services

Au-delà de la certification de l'identité, il a été noté que la CNIE pourrait permettre d'accéder à d'autres applications comme :

Des téléprocédures, du vote électronique, des services marchands (services bancaires, achats en ligne, abonnements divers...), le paiement de procès-verbaux en ligne... RC propose que soient prévus « des sections supplémentaires qui permettraient de remplacer le permis de conduire, la carte vitale, la carte de mutuelle. Bref tout ce dont nous avons besoin quotidiennement et que nous devons garder sur nous ».

Genium va dans le même sens puisqu'il suggère que la carte comporte des « données non obligatoires » qui si le citoyen « le veut, pourrait enrichir sa carte électronique ». Ce seraient « d'autres données personnelles, permettant son authentification pour des actions citoyennes (vote électronique, déclaration et paiement des impôts), des actions d'authentification et de paiement électronique sur le web (données bancaire...), voire des actions sociales (enregistrement de demandes d'aides sociales, secu,...) ».

* * *

A PROPOS DE LA LECTURE « SANS CONTACT » DE LA CARTE ET LA CREATION D'UNE BASE D'EMPREINTES DIGITALES NUMERISEES - 24 FEVRIER 2005

A la lecture des derniers messages, de nombreuses questions ont porté sur deux aspects du projet INES : la lecture « sans contact » de la carte et la création d'une base d'empreintes digitales numérisées.

Le dossier de présentation du programme INES précise que « la consultation des données d'identité (photo et empreintes) par les autorités habilitées se fera sans contact ». La notion de « sans contact » a fait l'objet de nombreuses craintes. En effet, la perception générale a été qu'il y a un risque qu'à l'insu du porteur la puce sans contact puisse être lue à distance où même qu'elle permette un traçage des porteurs de carte (quels usages du système RFID (Radio Frequency Identification) ? quels risques de géolocalisation ?...).

De nombreuses interrogations ont également porté sur l'opportunité de mettre en place une base d'empreintes digitales numérisées et sur les risques d'utilisations futures qui pourraient en être faites : utilité de la base d'empreintes par rapport à la vérification de l'identité, risques de croisement de fichiers ?...

Le ministère de l'intérieur a souhaité apporter des réponses (cf. résumé des réponses ci-dessous).

Que pensez-vous de ces éléments de réponse ? Vous conviennent-ils ou estimez-vous, au contraire, qu'il faut plus d'explications, ou encore pensez-vous à d'autres solutions possibles ?

* *

Synthèse des réponses du ministère de l'intérieur :

1) Sur l'aspect lié au risque de voir la puce sans contact lue à distance, à l'insu du porteur, par un intrus ou par l'Etat.

Le ministère de l'intérieur a tout d'abord rappelé qu'il convient de différencier le type de puce sans contact : « Il ne faut pas confondre les étiquettes RFID de la grande distribution avec l'interface radio d'une carte d'identité: pour faire une analogie, l'une est comme une affiche de publicité dans la rue, faite pour être vue de tous, l'autre est votre papier à lettre. Tous deux sont en papier, là s'arrête la ressemblance. L'étiquette RFID est faite pour répondre à tout signal; une carte intelligente, elle, ne répond qu'aux sollicitations autorisées ».

Le projet de CNIE prévoit deux modes d'accès sans contact à la puce. Il s'agit :

1) d'un code qui permettra d'accéder à la partie de la puce contenant l'identité et la photo (c'est à dire les mêmes informations que celles imprimées sur la CNIE : accéder à la puce n'apporte aucune information supplémentaire). Ce code se déduit des éléments imprimés sur la carte et nécessite donc de présenter la carte lors du contrôle (pas d'action à distance possible). Il s'agit d'un mode d'accès identique à celui retenu pour les passeports des pays extra-européens (« contrôle d'accès basique »).

2) d'un autre code et d'un matériel spécifiques pour accéder aux empreintes. Ce code et ce matériel seront réservés aux seuls services de contrôle (police, gendarmerie, douanes) européens pour les contrôles d'identité et les passages aux frontières. Il s'agit d'un mode d'accès identique à celui retenu pour les passeports européens (« contrôle d'accès étendu », prévu par le règlement européen du 13 décembre 2004).

Il est enfin précisé qu'aucun autre accès sans contact n'est prévu. A cet égard, deux exemples sont donnés : on ne pourrait ni « suivre quelqu'un à la trace grâce à des bornes dans la rue (ces bornes ne connaissent pas les codes des cartes qui passent à proximité) », ni « connaître les noms des participants à une manifestation ».

2) Sur l'aspect nécessité de mettre en place une base d'empreintes digitales numérisées.

Le ministère a précisé qu'il n'est pas nécessaire de mettre en place une base d'empreintes digitales si la seule finalité de la carte est de prouver que le porteur en est bien le titulaire.

Dans le cas d'un simple contrôle il n'y a donc pas de besoin de se connecter à une base d'empreintes.

Cependant, le ministère estime que l'on ne peut « en déduire trop vite » qu'il ne faut pas de base d'empreintes. Un système sans base d'empreintes :

- n'empêcherait pas les usurpations (un imposteur peut se faire faire une carte au nom d'une personne dont il connaît la date et le lieu de naissance) ou les identités multiples (un imposteur se fait faire 10 cartes à 10 noms différents) puisqu'il n'y a pas de contrôle possible. Une base d'empreintes empêcherait ces fraudes.

- si la puce est cassée (ou la carte perdue), le titulaire se retrouverait avec une carte sans valeur et doit redémontrer son identité pour en obtenir une nouvelle. Au contraire, avec une base d'empreintes, la carte cassée gardera sa valeur (un policier contrôlera dans le fichier au lieu de contrôler dans la puce), et si besoin une nouvelle carte sera délivrée sans formalité au titulaire (puisque l'on est sûr que c'est bien lui).

En tout état de cause, la loi devra encadrer strictement un tel dispositif.

3) Sur l'aspect lié au risque de « traçage » des porteurs de cartes notamment par le biais d'un suivi de leurs actions sur internet.

Le ministère de l'intérieur a rappelé qu'avec le GSM, un opérateur de téléphonie sait déjà où l'abonné se trouve « à 100m près, 24h/24 » et qu'avec la carte Visa, « votre banquier sait tout de vos dépenses ». Il en est de même avec les cartes de fidélité, les compagnies aériennes ou encore les grandes surfaces qui savent « tout » des habitudes de vie de leurs clients. En outre, avec internet, il est techniquement possible de savoir qui est l'internaute en ligne, malgré un pseudonyme, et d'obtenir l'historique de toutes les navigations sur le web.

En conclusion le ministère a souhaité préciser qu'un Etat qui voudrait « cliquer » quelqu'un n'aurait pas besoin d'investir dans une carte d'identité électronique ; il lui suffirait de recourir à ces moyens (GSM, CB, internet, cartes privatives) déjà existants. Aux yeux du ministère, cela montre que le contrôle des accès aux fichiers existants (fichiers des opérateurs GSM, CB, internet et fichiers clients des grands groupes) est « le vrai problème fondamental de protection de la vie privée ».

* * *

DEUXIEME SYNTHESE DES CONTRIBUTIONS DES INTERNAUTES DU 8 FEVRIER AU 29 MARS 2005

Après plus d'un mois de débats, voici une seconde synthèse des contributions des internautes.

Les principales inquiétudes et interrogations dont faisaient part de nombreux messages se font à la fois plus précises et plus nombreuses. Elles portent tant sur la lecture « sans contact » de la carte et les risques de traçage que sur la création d'une base d'empreintes digitales numérisées ou encore sur la sécurité des procédures utilisées. En revanche, peu de nouvelles modalités et d'usages associés sont proposés.

Même si, dans la plupart des cas, le ministère de l'intérieur a apporté des réponses, (voir le dossier de présentation : <http://www.foruminternet.org/telechargement/forum/pres-prog-ines-20050301.pdf>; ou encore : « A propos de la lecture « sans contact » de la carte et la création d'une base d'empreintes digitales numérisées » <http://www.foruminternet.org/forums/read.php?f=16&i=1733&t=1733> ainsi que les nombreux autres messages du ministère), le débat fait apparaître des demandes d'informations complémentaires sur le projet (dossier plus conséquent, réponses plus précises aux questions...).

En réaction à ces demandes, et afin de faciliter la poursuite du débat et d'approfondir les aspects suscitant le plus d'interrogations, le Forum des droits sur l'internet va publier, chaque semaine, une synthèse des contributions des internautes portant sur les thèmes retenus pour les fils de discussion :

Biométrie (B), En pratique (P), Sécurité (S), Usages (U), Vie privée (V) / voir <http://www.foruminternet.org/forums/read.php?f=16&i=2139&t=2139>.

A chaque semaine correspondra un thème, le premier sera la biométrie.

A chaque synthèse des contributions des internautes, le ministère de l'intérieur publiera un document reprenant les réponses qu'il a pu apporter sur le forum mais aussi offrant des précisions et informations complémentaires sur le projet INES.

I. Sur le principe même de la carte nationale d'identité électronique

Un certain nombre d'internautes déclarent être **peu convaincus** des motifs invoqués en faveur de la mise en place d'une telle carte.

Bibz se demande « *Pourquoi une telle carte ? Quelle est la nécessité fondamentale qui m'induit à penser que cette carte devrait être indispensable ? Peut-être pour me faciliter la vie ? (...) Notre vie est déjà très facilitée, pourquoi en rajouter encore avec une CNIE qui a pour but de me faciliter les facilités qui découlent déjà d'une facilitation ?* ».

Pour certains, les raisons de la mise en place de la carte nationale d'identité électronique émane d'une volonté de « *flicage* » (Minas) du gouvernement ou font suite aux « *délires sécuritaires développés par les américains* » (Zebulon) depuis les attentats du 11 septembre 2001. D'autres, comme RFID ou Eupalinos, n'y voient qu'une question d'argent (fabrication des puces, des cartes, des lecteurs etc.). Katwoman se demande comment la CNIE pourrait avoir un impact sur l'immigration illégale et s'il n'y a pas d'autres solutions que la biométrie pour rendre des documents plus difficiles à falsifier.

Fabien Petitcolas estime quant à lui qu'il n'y a pas de preuve établissant que la CNIE permettrait de réduire le terrorisme et se demande si le commerce électronique a vraiment besoin de cette carte (« *quel est le véritable taux de fraude ? Justifie-t-il cette carte ? Quels avantages pour le citoyen ?* »).

A l'opposé, certains estiment que les peurs exprimées autour du projet de carte d'identité électronique sont exagérées ; c'est, par exemple, le cas de Pinky qui dit avoir « *la nette impression que nous tombons dans une obsession nevrotique* ».

Au delà, d'autres, à l'instar de Miniroulie, estiment que **la mise en place d'une telle carte se justifie** dans la mesure où le système prévu permettrait « *plus de justice et de facilité pour la Justice pour refaire des papiers perdus ou retrouver d'éventuels malfaiteurs* ». ABADIE estime également que les avantages présentés dans le projet se justifient. Pour cet internaute, « *la carte électronique présente de meilleures garanties en cas de perte ou de vol : le rapprochement obligatoire de l'individu et du document électronique exclu toute utilisation d'une carte volée ou perdue. De plus, la perte ou le vol une fois signalée permet de détecter toute tentative d'utilisation. Ce n'est pas le cas avec la carte actuelle où on peut mettre une autre photo sans problème et celui à qui on présente la dite carte ne sait pas qu'elle est fausse. Le remplacement peut être fait très rapidement puisque tous les éléments sont disponibles pour une duplication* ».

II. Les principales inquiétudes et interrogations

1. Sur le risque de croisement de fichiers et sur l'accès aux données.

De nombreuses interrogations ont porté sur l'opportunité de mettre en place une base d'empreintes digitales numérisées et sur les risques d'utilisations futures qui pourraient en être faites.

a. Le risque de croisement de fichiers

De nombreuses questions ont porté sur le risque de **croisement de fichiers**. Phil13 a fait part de sa crainte que la CNIE soit un moyen permettant d'accéder à divers fichiers interconnectés entre eux. Pclerc a évoqué la crainte d'un profilage, d'un « *délit de faciès électronique* ». Freez se demande où seront stockées « *l'ensemble des données pour les vérifications nécessaires et sous la responsabilité de quelle administration?* ». Constatant que les interconnexions de fichiers existent depuis déjà longtemps et qu'en tout état de cause la CNIE ne pourra être que plus sûre que la carte actuelle, Neoxon estime que la véritable question est celle de l'encadrement de ces interconnexions et des consultations des données.

b. L'accès aux données

Des questions ont porté sur les garanties qu'il convient d'apporter sur les **personnes pouvant accéder** aux données (Qui aura accès aux informations personnelles contenues dans les fichiers centraux et dans la carte ?). Darhf souhaite que « *L'Etat n'ait accès à des données privées sur le citoyen qu'avec son propre consentement ou celui de la justice (indépendante) dans les affaires relevant de la sécurité* ». D'autres estiment que l'accès aux données par des personnes habilitées doit faire l'objet d'un traçage et que cet accès doit se faire « *au vu et au su des porteurs de carte* ».

2. Sur la biométrie

Certains sont **contre l'utilisation de la biométrie** dans la CNIE **par principe** exprimant leurs peurs face à cette forme d'identification directement inscrite dans le rapport au corps et craignant des dérives futures.

D'autres sont également **contre la biométrie mais plus pour des raisons « pratiques et techniques »**. Pour Lohran, il semble « *dangereux de stocker des données non révocables sur un dispositif matériel susceptible d'être dérobé* ». Dans le même sens, rfid274 estime qu'il « *ne faut pas mettre en dur dans un vecteur matériel des données non révocables, mais, par exemple, un certificat généré à partir des*

données biométriques, ce qui change tout. La carte perdue, on révoque le certificat, et on en régénère un nouveau à partir des données fondamentales stockées dans un serveur au ministère de l'intérieur ».

Au contraire, d'autres, à l'instar de Michel Lo, estiment qu'il y a « **des aspects positifs** » dans la biométrie comme « **le renforcement de la preuve de l'identité qu'on ne peut rejeter** », ce que confirme Richard qui se prononce en faveur des empreintes digitales estimant que cela permettra de résoudre davantage de crimes et délits.

Pour autant, la plupart des messages sont interrogatifs (pourquoi utiliser une telle technique ?, est-elle réellement plus efficace en terme de sécurité ?, pourquoi l'empreinte digitale ? - Pingouin se demande d'ailleurs si l'utilisation de l'iris de l'oeil comme donnée biométrique ne serait pas plus sûre que le recours à une empreinte digitale – combien de doigts devront être numérisés ?)

→ Le ministère de l'intérieur fait valoir que les données biométriques dans la carte ne seront accessibles qu'aux seuls agents agréés munis d'un lecteur spécial, ce qui limite les risques en cas de vol.

3. Sur les données contenues dans la carte et sur le rôle de l'Etat

a. Les données contenues dans la carte

Sur ce point, les avis divergent et les propositions sont nombreuses.

Rappelant les chiffres de la fraude d'identité aux Etats-Unis en 2004, richardrgf estime que **la carte ne devrait contenir qu'un minimum d'informations** (nom, prénom, adresse, sexe, couleur des yeux et, éventuellement, empreintes digitales), « *il faut interdire tout ajout d'autres informations et faire en sorte que cette puce soit limitée en capacité et autorisation d'écriture au strict nécessaire* ».

Le guet partage cet avis ; il propose que les renseignements « *primaires* » soient réduits au minimum et que le chargement d'autres informations ne soit possible qu'avec l'autorisation expresse du titulaire. Pour cet internaute, toutes les informations de la puce doivent pouvoir être lues et effacées par le titulaire ; ce dernier doit savoir exactement quelles sont les informations qui peuvent être consultées par un tiers.

Merlot remarque que le lieu de naissance et la date de naissance n'entrent pas dans l'identité et peuvent porter préjudice à la personne concernée. « *Il faut donc un système qui garantisse que chaque CNI est unique* ». Pour lui, « *ce système est composé des noms, prénoms et n° de la carte* » ; il précise que « *l'adresse ne fait pas partie de l'identité, qu'elle peut être variable au cours de la vie de la carte et qu'elle n'est d'aucune utilité sur le visuel* » et demande à quoi peut « *servir la photo numérisée dans la puce puisqu'il est prévu d'y inclure les empreintes digitales qui sont beaucoup plus fiables* ».

Enfin, Zorglub42 estime que « *si la CNIE est mal conçue, son vol permettrait à une personne malveillante d'accéder d'un seul coup à peu près tout ce qui est dessus. Les documents actuels sont multiples, et cela est un avantage* ».

Julesandolfi propose que la puce de la carte contienne « *outré la photo et l'empreinte digitale de son porteur, la nationalité, les renseignements du domicile et d'état civil sans filiation pour ne pas heurter ceux qui n'en ont pas, et en tenant compte des ex-départements français d'Algérie tels 91-Alger, 92-Oran, 93-Constantine, etc, et NON PAS ALGERIE comme c'est le cas actuellement ce qui crée de sérieux problèmes aux passages des frontières notamment aux USA* ».

Au contraire, Flapi estime qu'il serait « **dommage de se priver d'unifier sur un même support plusieurs fonctions**, uniquement parce que certaines d'entre elles ne sont pas accessibles à tout le monde » et jpg33700 qu'il « *est temps de réduire le nbre*

de paperasses à fournir avec l'instauration d'un document électronique passe-partout. Il existera toujours des abus, mais ils finissent toujours par être dénoncés ».

Jjf évoque le fait que « *l'assurance maladie s'achemine vers une gestion des droits en ligne (projet « Sesam-Vitale en ligne »)* » et qu'ainsi « *Vitale 2 n'aura plus de données administratives ou de santé dans sa puce* ». Au vu du coût de la carte Vitale 2, il se demande si la France, à l'instar d'autres pays européens, ne devrait pas intégrer un volet santé et social sur la CNIE et rappelle qu'il est également prévu que la carte Vitale 2 assure les fonctions d'authentification et de signature électronique.

→ Le ministère de l'intérieur a précisé que les données de santé et à caractère sanitaire et social ne seront pas dans la CNIE et a rappelé que les informations personnelles imprimées sur la carte seront les mêmes que celles qui figurent sur l'actuelle carte d'identité.

b. Sur le rôle de l'Etat et sur l'avenir d'une identification électronique des citoyens

Certains ont fait part de leurs inquiétudes sur le fait que des sociétés privées puissent intervenir dans la gestion du système (exemple de l'adaptation de la messagerie Microsoft/MSN avec la carte d'identité électronique belge). Ceci créerait une confusion entre la fonction régaliennne (attribution de l'identité) et les applications privées, commerciales ou non, associées à ce nouvel outil d'identification des personnes. De façon générale, le partage des tâches entre le secteur public et le secteur privé a suscité de nombreuses interrogations (craintes d'une privatisation « rampante » de l'Etat et une remise en cause consécutive des exigences de service public).

A cet effet, il est également rappelé que le choix des données à inscrire sur la carte (limitées à l'identité ou élargies) ainsi que le niveau de sécurité à atteindre sont de fait liés au choix qui sera fait en matière d'usages potentiels de la CNIE (dans quelle mesure est-il souhaitable que les usages de la CNIE s'ouvrent à des usages publics/privés qui dépassent le cadre de l'identification simple ?).

A cet égard, de nombreux messages estiment que, **si la carte devait être mise en place, elle devrait se limiter à l'identification de la personne et relever du seul contrôle de l'Etat.**

Enfin, des interrogations ont porté sur **l'avenir d'une identification électronique** des citoyens en cas de changement de régime (spectre du retour d'un régime du type vichyste) ou d'un élargissement du champ du contrôle de l'identité (Beretta cite l'exemple de l'élargissement des fichiers d'empreintes génétique initialement restreint aux seuls criminels sexuels).

4. Sur la lecture, à distance et à l'insu du porteur, des données inscrites sur la carte et le traçage.

Le dossier de présentation du programme INES précise que « *la consultation des données d'identité (photo et empreintes) par les autorités habilitées se fera sans contact* ». La notion de « sans contact » a fait l'objet de nombreuses craintes.

Même si certains estiment que la carte d'identité électronique ne présente aucun danger et permet de meilleures garanties en carte de porte ou de vol, la perception générale est qu'il y a un risque, qu'à l'insu du porteur, **la puce sans contact puisse être lue à distance** et qu'elle permette un **traçage des porteurs de carte.**

De nombreux messages ont ainsi évoqué le risque que la puce sans contact permette une lecture à distance des données inscrites sur la carte (« *L'identification « sans contact » aggravera encore le flicage, puisqu'on pourra être contrôlé sans même qu'on le sache* »

Franchick) et que cela entraîne également un traçage des porteurs de carte. S'agissant plus précisément du traçage, certains internautes ont rappelé qu'un tel traçage existe déjà (téléphone portable, carte bancaire). Gonzague rappelle les nombreuses réticences exprimées au moment de l'apparition de la carte bancaire dans les années 1970 pour une utilisation aujourd'hui largement acceptée.

En revanche, d'autres estiment qu'il s'agit, dans ce cas, d'un traçage choisi (« *Etre « tracé » reste pour l'instant en grande partie un choix* » cirspec).

A l'instar du message de cirspec (« *si le dispositif était de très courte portée, une puce « ordinaire » donnerait toute satisfaction* »), le souhait général est d'en limiter la portée à quelques centimètres (l'exemple du pass Navigo mis en place par la Ratp a été mentionné).

5. Sur la sécurité des procédures et du système

Il a été fait référence aux **limites des techniques de sécurité et au contournement de la protection de la carte bancaire** (la Yes Card - fabrication de fausses cartes à puce bancaires, la loi de Moore - hypothèses sur le progrès des performances de la technique qui se sont avérées fausses à terme; les personnes ayant hacké des sites sensibles américains...). Darhf demande ce qu'il en sera en cas de fraude à la CNIE : « *quels moyens de protestation et de réparation seront à la disposition de la personne concernée ? La responsabilité de l'Etat sera-t-elle engagée ? Comment le préjudice sera-t-il estimé ?* ».

Tatoute remarque qu'il « *se trouvera toujours un ou plusieurs informaticiens chargés de développer des applications annexes à la carte qui ne respecteront pas la confidentialité voulue, comme ceux de la carte vitale qui ont fait passer des informations des usagers en clair par mail vers les services de comptabilité* »

Simix estime que le problème du vol de documents vierges reste posé et qu'il faut garantir la sécurité des documents au niveau de l'administration.

De façon générale, il est fait part de la **faiblesse d'un système ouvert comme l'internet**. Tatoute précise qu'il suffirait de « *diffuser un ver* » sur le réseau pour que le système soit attaqué. Beretta constate que même si le niveau de protection est élevé et implique des moyens financiers très importants pour tenter de le dépasser, il ne s'agit pas d'un obstacle insurmontable pour certains « *Etats voyous ou certaines multinationales* ». D'ailleurs, Beretta se demande quel est le dispositif qui va être mis en place pour contrôler les échanges de données entre Etats.

BJ soulève le problème des ordinateurs infectés par des programmes qui permettent de récupérer toutes sortes d'informations ou d'accéder au disque dur. A ses yeux, sans politique de sécurité valable au niveau des postes informatiques des personnes ayant à traiter des données à caractère personnel, la CNIE n'est pas envisageable. Phil13 insiste sur le problème de la sécurité du poste client : « *Même bien sécurisé, le système sera accessible à tous les ordinateurs familiaux des usagers qui, pour beaucoup, sont pleins de virus, spywares, etc.* ».

Richardrgf demande « *quels outils seront utilisés en France pour créer, gérer, accéder à la nouvelle carte ?* » et note que « *si l'on utilise Windows, autant dire tout de suite qu'il n'y aura jamais de vraie sécurité sur cette carte* ». Beretta estime que « *l'accessibilité et l'interopérabilité du système doivent être assurées. Les standards ouverts et les logiciels libres sont un moyen d'y parvenir* ».

→ Estimant qu'aucun système électronique ne peut être sécurisé à 100%, le ministère de l'intérieur propose de remplacer le terme d'« infalsifiable », dont il est fait mention dans le document de présentation du programme INES, par « *dont la falsification demanderait de tels moyens que cela deviendrait hors de portée des fraudeurs actuels et ne serait de toute façon pas rentable* ».

De plus, le ministère rappelle que la sécurité sera bien plus importante avec la CNIE qu'elle ne l'est aujourd'hui « *mettons que la carte actuelle assure 70-80% de sécurité. La*

nouvelle carte nous amènerait à 95% » (ce à quoi phil13 répond que « 1% d'erreur sur 60 millions de français cela fait 600.000 erreurs »).

Le ministère signale également que « *l'accès à chaque application nécessitera un niveau de sécurité donné (selon la confidentialité des informations échangées* » et que le citoyen pourra y accéder avec tout moyen garantissant ce niveau de sécurité.

II. Le coût de la carte

Une majorité d'internautes souhaite que **la carte soit gratuite**. Si elle devait être payante, Julesandolfi suggère qu'elle ne le soit que « *pour les personnes imposables sur les revenus* ».

De façon générale, les internautes évoquent le **coût de la carte pour la collectivité**. Eupalinos écrit que « *Même si le citoyen n'aura pas à payer directement la CNIE, il en supportera les frais indirectement via le budget de l'Etat et les impôts* » et évoque le « *lobbying* » de quelques sociétés spécialisées (« *Applied Digital Solutions et autres Bill Gates* »).

Simix évoque le **coût du matériel entourant la CNIE** (lecteur de carte à puce au domicile pour justifier de son identité sur internet, lecteur d'empreintes digitales ou rétiniennes pour éviter les problèmes liés à la perte du lecteur de carte...) pour constater que la mise en place d'une telle carte posera des problèmes de financement.

Enfin, Merlot note que mettre une photographie dans la puce « *nécessite une mémoire importante et donc augmente sérieusement le coût de la carte* ».

III. La création d'un organisme de contrôle ad hoc

Certains ont noté l'absence d'un véritable contre-pouvoir face au projet de CNIE. Or, à l'image de Zorclub42, ils estiment que « *la fiabilité du système doit absolument être garantie et surtout certifiée par un organisme indépendant* ».

Freez suggère qu'une « **commission spéciale soit instituée** (autre que celles existantes) qui devra être radicalement indépendante et avoir pour mission la surveillance des données et des personnes qui y ont accès et de toutes les opérations possibles à partir de ces données (...). Ses membres devront jouir des mêmes protections que les magistrats qui pourront garantir un peu contre les pressions. (...) Des organisations/associations de citoyens devront pouvoir être présentes dans cette commission et des citoyens tirés au hasard dans la population (...) et bénéficiant des mêmes garanties que des représentants du personnel ».

Necronick souligne que les membres d'une instance indépendante, pour qu'ils restent eux-mêmes indépendants, ne doivent pas jouir de « *privilèges (primes, immunités, etc.)* » pour que leur engagement ne soit pas « *dicté par un intérêt personnel* ».

IV. Les modalités pratiques

Une majorité d'internautes souhaite que **la carte soit facultative**.

En ce qui concerne le format de la carte, les messages souhaitent tous que ce soit un **format carte de crédit**.

En ce qui concerne le **vote électronique**, les internautes semblent, dans leur grande majorité, opposés à la possibilité de voter à domicile avec la CNIE (attaques contre le système trop présentes, atteinte à la confidentialité du vote, usurpation d'identité, le bureau de vote seul permet de s'assurer que le votant n'a pas subi de pression...). A cet égard, Franchick évoque la crainte des pressions exercées à la maison et des fraudes et Necronick estime que « *le vote n'est pas une démarche qui doit être simplifiée* ».

En ce qui concerne les **téléprocédures**, les avis sont moins tranchés, ces services semblant moins « sensibles » que le vote électronique. Les messages suggèrent généralement la mise en place de services de paiement avec les administrations (autant nationales que locales). Pesked se demande s'il ne serait pas possible d' « *intégrer dans la puce électronique une autorisation de prélèvement d'organes ou de tissus en vue d'une greffe et une indication de l'inscription sur les listes électorales* ».

→ Le ministère de l'intérieur a précisé qu'il pourrait être possible d'utiliser la CNIE pour prouver son identité dans une téléprocédure, au lieu d'avoir un login/mot de passe.

En ce qui concerne le **lieu de délivrance de la carte**, attilio71 privilégierait les services de police, qui sont d'après lui, « *plus sécurisants* ». De même, Julesandolfi estime que la carte « *devrait être délivrée dans les commissariats de police et/ou les brigade de gendarmerie selon leur compétence territoriale, par des personnels administratifs (ou actifs réformés) strictement habilités à cet effet et responsables devant la loi en cas de fraude avérée de leur part* ». Cet internaute estime également que des « *bornes en Mairie devraient permettre les mises à jour comme c'est le cas des cartes vitales actuelles* ».

Des questions sur les aspects pratiques de la carte ont également été faites :

- Quand le porteur de la carte décède, sa carte est-elle automatiquement invalidée ?
- Quand le porteur de la carte récupère sa carte qui a été perdue ou volée et qui a été invalidée, peut-il la faire revalider ?
- Les opérations de déclaration de perte, de vol ou de « revalidation » peuvent-elles se faire à distance ? (par exemple : événement produit dans les DOM alors que le porteur réside en métropole).

V. Des remarques sur le débat

Certains estiment que le débat devrait avoir une **portée** européenne car désormais les décisions sont prises au niveau européen (passeport biométrique et le Règlement de décembre 2004, titres de séjours et visas biométriques). Les problématiques posées se retrouvant dans les autres Etats membres, Pierre Rostaing estime que le débat ne devrait pas être uniquement national mais porté à un niveau européen (« *pourquoi à l'heure de l'Europe, penser franco-français, et ne pas penser ensemble ces problèmes...inévitablement communs?* »).

En ce qui concerne la publicité du débat, un grand nombre d'internautes regrette qu'il ne soit pas suffisamment connu et que, pour un débat qui se veut national, il n'y ait ni campagne de presse ni informations diffusées à la télévision (Eupalinos regrette que ce débat ne touche « *qu'une infime partie de la population. Quand nos présentateurs TV des trois premières chaînes parleront-ils de même?* »). Ce manque d'informations fait craindre à certains, comme Cogex ou Katwoman, que ce débat ne soit en fait qu'une « *pseudo-consultation* » et un prétexte, pour les pouvoirs publics, d'obtenir un assentiment populaire avant la mise en place de la CNIE.

* * *

SYNTHESE DES CONTRIBUTIONS DES INTERNAUTES SUR LE THEME « BIOMETRIE » DU 29 MARS 2005

La biométrie et la CNIE

Il ressort du débat qu'un certain nombre de contributeurs sont **contre l'utilisation de la biométrie** dans la CNIE **par principe** exprimant leurs peurs face à cette forme d'identification directement inscrite dans le rapport au corps et craignant des dérives futures.

D'autres sont également **contre la biométrie mais plus pour des raisons « pratiques et techniques »**. Pour Lohran, il semble « dangereux de stocker des données non révocables sur un dispositif matériel susceptible d'être dérobé ». Dans le même sens, rfid274 estime qu'il « ne faut pas mettre en dur dans un vecteur matériel des données non révocables, mais, par exemple, un certificat généré à partir des données biométriques, ce qui change tout. La carte perdue, on révoque le certificat, et on en régénère un nouveau à partir des données fondamentales stockées dans un serveur au ministère de l'intérieur ».

D'autres internautes citent l'exemple britannique où il est envisagé de passer d'une absence de carte d'identité à une carte de type biométrique (photo, empreintes digitales et iris de l'œil), suscitant une très vive controverse. Citant des extraits d'un récent rapport de la « London School of Economics & Political Science » publié sur ce sujet, lucmars évoque sa dimension internationale et les préconisations émises par l'Organisation Civile de l'Aviation Internationale et le Conseil de l'UE. A ce titre, cet internaute estime que les pouvoirs publics ne doivent pas avancer « l'argument d'obligations internationales, celles-ci ne requiert que la photo sur la puce et aucunement une base de donnée (même si cela diminue l'efficacité de la vérification et de l'identification). De plus, cela n'a trait qu'aux passeports ». Pour cet internaute, l'introduction d'autres données biométriques « et d'une base de données n'a d'autre justification que celle d'une politique intérieure, européenne ou nationale ».

Ce lien entre introduction de la biométrie et la mise en place d'une base de données centralisées des empreintes a également été évoqué par d'autres internautes. Ces derniers, qui ont souligné le fait que la délivrance des cartes d'identité actuelles s'accompagne déjà du relevé des empreintes digitales, se demandent si les inquiétudes liées à la mise en place de la biométrie ne sont pas uniquement dues au fait que le projet de CNIE prévoit de centraliser et de numériser des données déjà existantes. Et « ce n'est pas le fait de garder des cartes non électroniques qui va empêcher l'apparition de ces bases » relève pshunter.

Au contraire, certains contributeurs, à l'instar de Michel Lo, estiment qu'il y a « **des aspects positifs** » dans la biométrie comme « **le renforcement de la preuve de l'identité qu'on ne peut rejeter** », ce que confirme Richard qui se prononce en faveur des empreintes digitales estimant que cela permettra de résoudre davantage de crimes et délits.

D'autres internautes s'interrogent sur **le type de données biométriques utilisées**. Pingouin se demande ainsi si l'utilisation de l'iris de l'oeil comme donnée biométrique ne serait pas plus sûre que le recours à une empreinte digitale. Il est aussi demandé combien de doigts devront être numérisés ? 10cd29 rapporte à cet égard les difficultés pratiques qui peuvent surgir lors de tentatives de lecture d'empreintes digitales sur des personnes dont le doigt a été abîmé (exemple donné : les mains en contact prolongé avec une lessive à base de soude...).

De façon générale, **la plupart des messages sont interrogatifs** (pourquoi utiliser une

telle technique ? Pourquoi conserver la photo, dont la mise en place est onéreuse, dès lors qu'il est avancé que les empreintes digitales sont plus fiables ? Cette technique est-elle d'ailleurs réellement plus efficace en terme de sécurité ?)

* *

REPONSE DU MINISTERE DE L'INTERIEUR

Tout d'abord, **qu'entend-on par biométrie ?** La description du signalement portée sur les passeports intérieurs au XIX e siècle était une forme rudimentaire de biométrie. Le portrait d'identité photographique relève de la biométrie, or il date également (pour la technique) du milieu du XIXe siècle. Il faut également considérer, dans l'ordre chronologique, l'anthropométrie, les empreintes digitales, les empreintes génétiques...

Il convient donc de réaliser que la biométrie, dans sa grande diversité, n'est pas fondamentalement une invention récente, pas plus que son application aux papiers d'identité : l'Argentine a commencé à inscrire les empreintes digitales sur les cartes d'identité en 1905...

Ce qui choque certaines personnes, c'est que la biométrie, initialement appliquée aux malfaiteurs (anthropométrie développée par Bertillon dans les années 1880 pour l'identité judiciaire), soit généralisée à titre préventif. Cette réaction n'est pas nouvelle non plus : lorsque la préfecture de police a proposé en 1921 aux habitants du département de la Seine une carte d'identité avec empreintes, certains se sont indignés de voir les honnêtes gens traités comme des malfaiteurs. D'autres ont reconnu l'utilité de disposer d'un titre pratique et fiable (rappelons qu'à l'époque, en l'absence de carte d'identité, il fallait se débrouiller comme on pouvait lorsqu'on avait besoin de prouver son identité. Le recours à deux témoins est célèbre, ces témoins étant souvent de complaisance). On pourrait recopier dans ce forum certains articles de l'époque sans y modifier un mot.

Pourquoi utiliser de la biométrie alors ? Comme on s'en rend compte en lisant un passeport du XIXe siècle, un simple signalement physique (« taille 1m75, cheveux clairs, yeux marrons ») n'aide pas à garantir que le porteur du document est bien son propriétaire légitime. Cela ouvre la voie à de nombreuses fraudes par prêt ou vol de titre. Des techniques plus précises sont alors utilisées : apposition d'une photo, apposition des empreintes digitales par tampon encreur (pas très facile à contrôler), ou, comme dans le projet INES, inclusion des empreintes dans la puce de la carte (facile à contrôler). Nous voyons ici apparaître la première raison d'utilisation de la biométrie dans INES, **utilisation en mode « local » (dans le titre lui-même) : pouvoir garantir que le porteur du titre en est bien le titulaire.**

Mais cela ne suffit pas à garantir que ce titulaire correspond bien à l'identité déclarée. En effet, la biométrie en mode local n'empêche pas un fraudeur de se faire délivrer plusieurs titres sous plusieurs identités différentes, que ce soit pour échapper à la justice ou pour usurper des droits qu'il n'a pas. La seule parade consiste à conserver une base des éléments biométriques de chaque demandeur, et à vérifier

- lors de toute demande initiale pour un état civil donné, que les éléments biométriques ne correspondent pas à un autre état civil de la base ;

- lors de toute demande de renouvellement, que les éléments biométriques sont bien corrects.

La seconde raison de l'utilisation de la biométrie dans INES, **en mode centralisé (base biométrique), est donc de garantir qu'à une personne physique ne correspond qu'un seul état civil, et vice-versa.**

Remarquons que rien n'oblige que ces éléments centralisés soient les mêmes que ceux utilisés en mode local. On pourrait par exemple envisager (à titre théorique, 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), et que la base pour les contrôles des demandes de titre ne contienne pas les empreintes digitales, mais un autre élément, l'iris de l'œil par exemple.

Le couplage de la biométrie et de l'informatique change ainsi la donne par rapport au XIXe siècle. L'informatique permet certes de constituer des bases des éléments biométriques (ce point-là n'est pas nouveau : il y avait plusieurs millions de fiches anthropométriques à la préfecture de police en 1893), mais surtout d'automatiser les recherches et comparaisons. C'est pourquoi une mise en œuvre d'un système d'identification biométrique doit s'accompagner **de garanties très précises pour éviter toute dérive**. En ce qui concerne le projet INES, des garanties seront mises en place par un projet de loi qui sera **soumis au Parlement après avis de la CNIL** :

- Seules les autorités habilitées (police, gendarmerie, douanes) auraient accès aux empreintes stockées dans la puce de la carte, à l'exclusion de toute autre administration et de tout autre organisme public ou privé ;
- Seules les autorités habilitées (police, gendarmerie, douanes) auraient accès aux empreintes stockées dans la base, et uniquement sous contrôle judiciaire ;
- Les accès aux bases seront journalisés afin de prévenir tout abus, les peines pour les accès non autorisés seraient aggravées.
- Les vérifications lors des demandes de titre seraient effectués de manière automatique, sans que l'agent puisse accéder à la base.

Pour en venir à la motivation des choix techniques, rappelons que parler de « biométrie » en général n'a aucun sens et que les **différentes techniques présentent différents degrés de maturité**.

- La reconnaissance de l'iris apporte une grande fiabilité, mais elle présente l'inconvénient de révéler par la même occasion des informations sur l'état de santé de la personne.
- Les empreintes digitales, utilisées depuis plus d'un siècle, sont également une technique fiable et éprouvée, facile d'emploi de surcroît. Il est là aussi nécessaire de distinguer entre des prises d'empreintes à usage policier (empreintes prises « roulées » sur les 10 doigts, pour obtenir un maximum d'informations) et celles à usage d'identité (empreintes prises à plat, sur seulement le nombre de doigts nécessaire pour éviter toute confusion en fonction de la taille de la population visée). Le projet INES vise évidemment la seconde catégorie.
- La reconnaissance faciale, plus récente, est beaucoup moins fiable, bien que des progrès rapides soient envisageables.
- L'empreinte génétique (ADN) est sans doute la technique la plus fiable si elle est correctement mise en œuvre, sauf dans le cas des vrais jumeaux.
- Mentionnons pour mémoire la reconnaissance vocale, la dynamique de la signature manuscrite, et des formes modernes d'anthropométrie (reconnaissance de la forme de la main, de l'oreille, etc).

Rappelons aussi que l'usage d'une technique biométrique doit faciliter et accélérer les

contrôles (pensons notamment aux aéroports), mais **en aucun cas remplacer le contrôleur humain** : il s'agit d'une aide à la décision. Si le contrôle biométrique est positif, la personne (le voyageur) peut passer en cinq secondes. Si le contrôle biométrique est négatif ou impossible, on retombe dans la procédure actuelle. Mais comme l'existence d'un taux d'erreur est reconnu, le fait que le contrôle soit négatif n'est pas une condamnation automatique : des procédures de vérification doivent être prévues. De même pour les personnes ne pouvant pas être traitées par le système (cas des mains abîmées, voire des personnes amputées). C'est pour cela qu'il ne serait pas sain d'installer des portiques biométriques complètement automatisés : il ne sauraient pas traiter les erreurs ou les exceptions, et seraient vulnérables à certains types de fraude que la présence d'un contrôleur humain permet d'empêcher.

En ce qui concerne les contraintes internationales, il convient de séparer les différentes strates :

- Au niveau mondial, l'OACI impose un passeport contenant une puce avec la photographie numérisée, les autres éléments biométriques étant optionnels.

- Au niveau européen, le règlement du 13 décembre 2004 reprend les dispositions de l'OACI et impose comme autre élément biométrique les empreintes digitales. Il prévoit un dispositif pour réserver la lecture de ces empreintes aux autorités habilitées, et un autre pour empêcher tout accès à la puce à l'insu du porteur.

Le but de ces dispositions est de permettre de s'assurer au passage d'une frontière que le porteur d'un passeport en est bien le titulaire : il s'agit donc d'un usage de biométrie en mode local (tel que présenté plus haut). Mais si les États souhaitent s'assurer lors de l'émission d'un titre que le demandeur n'en détient pas déjà un autre sous une autre identité, ils ont besoin en outre d'avoir une base centralisée nationale (voir plus haut).

- Aucune disposition internationale ne s'applique pour le moment aux cartes d'identité. Toutefois, celles-ci servent aussi de document de voyage : il serait donc pratique et logique qu'elles intègrent les fonctionnalités prévues pour le passeport (y compris le dispositif pour réserver la lecture de ces informations aux autorités habilitées, et celui pour empêcher tout accès à la puce à l'insu du porteur).

Mais la carte d'identité ne sert pas qu'aux contrôles aux frontières : on en a également besoin pour retirer un recommandé à la poste, pour passer un examen ou un concours, ou pour déposer des demandes d'allocation. Elle doit donc rester utilisable par le postier, l'examineur, ou le fonctionnaire, qui, rappelons-le, n'auront pas accès aux données stockées dans la puce (empreintes notamment). C'est pourquoi elle devra conserver (sous un format carte bancaire plus pratique) un aspect traditionnel et permettre de voir nom, prénoms, photo, date de naissance, etc, comme aujourd'hui.

Enfin, le projet INES prévoit une séparation totale des éléments biométriques et des fonctionnalités d'administration électronique (authentification du titulaire en ligne et signature électronique) : aucune application, ni publique, ni privée, n'aura accès ni à la photo, ni aux empreintes digitales. L'administration électronique s'appuiera exclusivement sur le code secret.

* * *

SYNTHESE DES CONTRIBUTIONS DES INTERNAUTES SUR LE THEME « VIE PRIVEE » DU 22 AVRIL 2005

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

De nombreuses interrogations et critiques portent sur la mise en place d'une base d'empreintes digitales numérisées et sur les risques qui peuvent en découler. Deux types de risques sont principalement évoqués : le risque de croisement de fichiers et de fichage des individus ainsi que celui d'une évolution future de l'usage de la base.

A titre liminaire, Pierre Piazza rappelle, en tant qu'historien, que « *la constitution de bases de données centralisées contenant des informations relatives aux demandeurs de cartes d'identité a constamment été au coeur des préoccupations des autorités* » depuis 1921. Il note également qu'avec « *l'émergence des débats sur l'informatisation de la carte d'identité à partir du début des années 1980, les tentatives de création de fichiers centralisés de données nominatives par le ministère de l'Intérieur font l'objet des critiques les plus virulentes* ».

a. Le risque de croisement de fichiers et d'un fichage des individus

De nombreux messages ont porté sur le risque de croisement de fichiers et de fichage des individus.

Constatant que les fichiers existant actuellement sont décentralisés, Phil13 ou encore CECE craignent qu'une base centrale touchant toute la population ne conduise à terme à un fichage généralisé des individus. Constatant que les interconnexions de fichiers existent depuis déjà longtemps, Neoxon estime que la véritable question est celle de l'encadrement de ces interconnexions et des consultations des données.

Pingouin fait remarquer qu'avec le système entourant actuellement la carte d'identité il y a moins de risque d'interconnexions car, aux termes du décret d'octobre 1955 instituant la carte nationale d'identité : « *les données sont normalement conservées par l'émetteur de la carte (mairie)* » et le texte (article 12) « *précise clairement que les informations nominatives contenues dans le système de gestion informatisée ne peuvent faire l'objet d'aucune interconnexion avec un autre fichier ni d'aucune cession à des tiers* ».

Pour Beretta tout est « *un problème de finalité (...)* : si la biométrie a pour unique finalité d'associer un titre à son porteur qu'elle est l'utilité d'un fichier central des empreintes si ce n'est une vaste opération de police ? Il existe sûrement des solutions techniques permettant de s'assurer qu'une même personne physique n'a qu'une identité sans constitué de base d'empreintes (je pense notamment aux ZKS, Zero-Knowledge Systems) ». Il précise que « *s'il apparaissait qu'un fichier centralisé était la seule solution à un problème technique* » il faudrait alors « *que ce fichier ne soit pas réversible, cad qu'il soit possible de demander l'empreinte d'une personne en fonction de son nom mais pas le nom d'une personne en fonction de son empreinte. Si le fichier n'a pas de vocation policière cela devrait suffire à détecter la fraude ou les identités multiples* ».

b. Le risque d'une évolution possible de l'usage de la base

De nombreuses interrogations portent sur le risque d'une évolution possible de l'usage de la base par les pouvoirs publics : élargissement du contenu de la base à d'autres données ou de l'accès à d'autres agents, voire changement de régime - spectre du retour d'un régime du type vichyste...

Beretta cite ainsi l'exemple de l'élargissement progressif des fichiers d'empreintes génétique, initialement restreint aux seuls criminels sexuels. Il veut également des

« garanties quant à la non extension et la non prospection de nouvelles données biométriques autres que celles choisies initialement ».

A cet égard, antiNOM estime que *« lorsqu'on est en possession d'une base de données, la logique veut qu'on les exploite pour faire des statistiques, afin d'en tirer des probabilités. Ma question au gouvernement est donc la suivante: Qui peut nous garantir qu'il ne sera fait aucun "scoring" avec nos données centralisées? »*

Galimatias note qu'une CNIE *« où une technologie de haut niveau serait utilisée est immédiatement un moyen de mieux surveiller (le punir n'est alors jamais loin) et à terme, c'est à dire au bout du temps où ces outils seront suffisamment banalisés pour être "naturels", ils permettront de passer tout naturellement à une l'implantation d'une puce d'identification ».*

Partant du constat que l'article II-68 du Traité établissant une constitution pour l'Europe *« traite du respect de l'intégrité des données personnelles et de la vie privée »*, Asterix se demande si, *« à moyen terme »*, ces principes seront toujours respectés car une CNIE *« pourrait (...) réunir (...) des données sur sa santé, sur sa situation familiale ou ses orientations politiques, sexuelles ou religieuses, d'où un réel danger pour la démocratie et les libertés ».*

2. Sur le fait que le projet ne risque pas de porter atteinte au respect de la vie privée

En revanche, pour d'autres internautes, la mise en place d'une telle base ne s'accompagne pas de craintes particulières ; au contraire, elle est même, parfois, légitimée.

Ainsi, Pesked estime que *« la protection de la liberté individuelle est justement une cause essentielle qui ne supporte pas d'être décrédibilisée par des productions comme "entre insécurité et respect de ma protection individuelle, je préfère l'insécurité. Il vaudrait mieux, selon moi, que les véritables défenseurs des libertés individuelles (ceux qui font passer le pragmatisme avant l'idéologie) accompagnent le projet de CNIE plutôt que de s'y opposer avec des argumentaires fallacieux ».*

De même, doutre *« ne comprends pas cette phobie d'être fiché »*. Il *« trouve très bien que les services de l'Etat puisse bénéficier d'un répertoire à jour de chaque individu : les empreintes digitales puis les empreintes génétiques seront une avancée fabuleuse pour la résolution de crimes et délits ».*

Dan47 note que *« pour un quidam qui mène une vie normale, sans commettre d'illégalité, la carte ne va pas lui poser de problème métaphysique grave. Le contrôle de la maréchaussée lui paraîtra d'un banal affligeant. Pour ma part celui qui peut me suivre au jour le jour et savoir mon mode de vie c'est mon banquier. La simple lecture des relevés de ma carte bleue en dit plus que tout autre contrôle... Comme quoi tout est relatif. On accepte tout de son banquier, rien de la maréchaussée! Problème de choix ».*

Martd propose que soit créée *« une base de données dans laquelle le n° INSEE sera saisi obligatoirement, ce dernier doit être attribué dès la naissance puisqu'il nous accompagnera durant toute la vie, les célibataires pourront se marier ou divorcer, ce numéro lui ne changera jamais. Toutefois, il ne doit pas apparaître sur la CNIE mais doit correspondre à un numéro matricule dédié par informatique ».*

Rappelant que *« nous ne sommes pas aux Etats-Unis »* mais *« bien en France »* et supposant que la mise en oeuvre de la CNIE *« est faite en toute transparence et que sa fiabilité est confirmée, que les personnes habilitées ne sont pas corruptibles »*, Zorglub42

choisit volontairement de « *forcer le trait* » en se demandant si la mise en place d'une telle carte pose de réels problèmes en termes de respect de la vie privée.

Il se demande ainsi : « *En quoi consiste la CNIE ? (...) à un simple fichage. Et alors ? Mes empreintes digitales sont stockées dans une base qui contient plusieurs dizaines de millions d'entrées. Allez, noircissons le trait: mon identification unique permet à l'Etat de faire le lien avec les fichiers des cartes grises, des interdits bancaires, des casiers judiciaires, des impôts, etc. Jusque là, ça m'est bien égal! Si l'Etat veut tout savoir sur moi, c'est déjà faisable, la CNIE ne fait qu'accélérer les choses et les rendre disponibles aux agents habilités* ». En ce qui concerne le risque de « *flicage par l'Etat* » il rajoute que si « *l'Etat utilise les informations existantes, y ajoute d'autres informations sur nos préférences, nos habitudes, nos opinions pour nous classer dans certaines catégories et nous soumettre à une répression quelle qu'elle soit* » ceci serait « *contraire à notre Constitution. Si l'Etat en arrive à ces dérives, comme disait un autre membre de ce forum, c'est possible avec ou sans CNIE* ».

En revanche, Zorclub42 précise que si le système CNIE est « *une véritable passoire* » et que « *des individus ayant des objectifs différents de ceux de l'Etat s'emparent de nos informations (Falsification d'identité, fraude, etc.) : là ça me pose problème* ».

3. Sur les données qui doivent être contenues dans la carte

Sur ce point, les avis divergent et les propositions sont nombreuses.

Richardrgf estime que la carte ne devrait contenir qu'un minimum d'informations (nom, prénom, adresse, sexe, couleur des yeux et, éventuellement, empreintes digitales), « *il faut interdire tout ajout d'autres informations et faire en sorte que cette puce soit limitée en capacité et autorisation d'écriture au strict nécessaire* ».

Certains, comme Le guet et Michel Elie, partagent cet avis.

Le guet propose que les renseignements « *primaires* » soient réduits au minimum.

Michel Elie souhaite que la CNIE ne comporte « *que des informations concernant l'état civil du porteur : nom, âge, nationalité et le moyen de les authentifier : photo, empreintes digitales* »

Merlot remarque que le lieu de naissance et la date de naissance n'entrent pas dans l'identité et peuvent porter préjudice à la personne concernée. « *Il faut donc un système qui garantisse que chaque CNI est unique* ». Pour lui, « *ce système est composé des noms, prénoms et n° de la carte* » ; il précise que « *l'adresse ne fait pas partie de l'identité, qu'elle peut être variable au cours de la vie de la carte et qu'elle n'est d'aucune utilité sur le visuel* » et demande à quoi peut « *servir la photo numérisée dans la puce puisqu'il est prévu d'y inclure les empreintes digitales qui sont beaucoup plus fiables* ».

Enfin, Zorclub42 estime que « *si la CNIE est mal conçue, son vol permettrait à une personne malveillante d'accéder d'un seul coup à peu près tout ce qui est dessus. Les documents actuels sont multiples, et cela est un avantage* ».

Julesandolfi propose que la puce de la carte contienne « *outre la photo et l'empreinte digitale de son porteur, la nationalité, les renseignements du domicile et d'état civil sans filiation pour ne pas heurter ceux qui n'en ont pas, et en tenant compte des ex-départements français d'Algérie tels 91-Alger, 92-Oran, 93-Constantine, etc, et NON PAS ALGERIE comme c'est le cas actuellement ce qui crée de sérieux problèmes aux passages des frontières notamment aux USA* ». Courtois « *rapatrié d'Algérie né avant 1962* » précise que son « *passport indique comme lieu de naissance la mention DZ* » et se demande « *quelle mesure est-il envisagé de prendre pour éviter de mentionner mon lieu de naissance par les lettres DZ* » sur sa future carte nationale d'identité électronique.

Au contraire, Flapi estime qu'il serait « *dommage de se priver d'unifier sur un même support plusieurs fonctions, uniquement parce que certaines d'entre elles ne sont pas*

accessibles à tout le monde » et jpg33700 qu'il « est temps de réduire le nbre de paperasses à fournir avec l'instauration d'un document électronique passe-partout. Il existera toujours des abus, mais ils finissent toujours par être dénoncés ».

Jjf évoque le fait que *« l'assurance maladie s'achemine vers une gestion des droits en ligne (projet « Sesam-Vitale en ligne ») »* et qu'ainsi *« Vitale 2 n'aura plus de données administratives ou de santé dans sa puce »*. Au vu du coût de la carte Vitale 2, il se demande si la France, à l'instar d'autres pays européens, ne devrait pas intégrer un volet santé et social sur la CNIE et rappelle qu'il est également prévu que la carte Vitale 2 assure également des fonctions d'authentification et de signature électronique.

4. Sur la maîtrise de la carte par son titulaire et sur les personnes habilitées à consulter les données stockées.

Beaucoup ont souhaité savoir quelle maîtrise aura le citoyen sur les données inscrites sur la carte et dans les fichiers.

Ainsi Le guet souhaite que toutes les informations de la puce puissent être lues et effacées par le titulaire, que le chargement d'autres informations ne soit possible qu'avec son autorisation expresse et que celui-ci sache exactement quelles sont les informations qui peuvent être consultées par un tiers.

De même Michel Elie estime que *« la cnie ne doit pas pouvoir être lue sans le consentement explicite de son porteur (...). Seul le porteur peut affirmer qu'il reconnaît pouvoir être identifié au moyen de cette carte »*. Pour lui, *« la cnie devrait seulement constituer la clé du système de protection et d'accès aux informations personnelles ; elle ne serait en quelle que sorte que la partie émergée d'un système de protection et d'accès aux informations personnelles. Elle autoriserait le porteur ou une personne habilitée à consulter et/ou modifier les données personnelles le concernant selon son niveau d'habilitation »*.

Darhf souhaite que *« L'Etat n'ait accès à des données privées sur le citoyen qu'avec son propre consentement ou celui de la justice (indépendante) dans les affaires relevant de la sécurité »*.

D'autres se demandent quelles garanties seront apportées sur les personnes pouvant accéder aux données : quels seront ces agents, de quels droits et de quelles façons auront-ils accès aux données, quelle habilitation aura un agent de mairie par rapport à un magistrat ou un policier ?...).

Certains comme Beretta et Zorclub42 se demandent *« Qui habilite qui ? Qui surveille la piste d'audit ? »*. Freez se demande où seront stockées *« l'ensemble des données pour les vérifications nécessaires et sous la responsabilité de quelle administration? »*.

Il est souvent souhaité que l'accès aux données par des personnes habilitées fasse l'objet d'un traçage et que cet accès se fasse *« au vu et au su des porteurs de carte »*.

Par ailleurs, pour Beretta, *« on ne saura de toute façon pas qui aura accès à ces fichiers. Une empreinte embarquée destinée au contrôle automatisé de mon titre de visu avec un agent habilité (une co-authentification pourrait être une bonne fonction d'ailleurs : une identification mutuelle du contrôleur et du contrôlé car le système ne doit pas être à sens unique) je n'ai rien contre, mais mes informations biométriques bien rangées et bien exploitables qui se baladent dans les divers services ministériels, ses sous traitants et autres : non »*.

5. Sur le risque de lecture, à distance et à l'insu du porteur, des données inscrites sur la carte.

Le dossier de présentation du programme INES précise que *« la consultation des données d'identité (photo et empreintes) par les autorités habilitées se fera sans contact »*. La notion de *« sans contact »* a fait l'objet de nombreuses craintes.

Même si certains estiment que la carte d'identité électronique ne présente aucun danger et permet de meilleures garanties en carte de porte ou de vol, la perception générale est qu'il y a un risque, qu'à l'insu du porteur, la puce sans contact puisse être lue à distance et qu'elle permette un traçage des porteurs de carte.

De nombreux messages ont ainsi évoqué le risque que la puce sans contact permette une lecture à distance des données inscrites sur la carte (« *L'identification « sans contact » aggravera encore le flicage, puisqu'on pourra être contrôlé sans même qu'on le sache* » Fanchick) et que cela entraîne également un traçage des porteurs de carte. S'agissant plus précisément du traçage, certains internautes ont rappelé qu'un tel traçage existe déjà (téléphone portable, carte bancaire). Gonzague rappelle les nombreuses réticences exprimées au moment de l'apparition de la carte bancaire dans les années 1970 pour une utilisation aujourd'hui largement acceptée.

En revanche, d'autres estiment qu'il s'agit, dans ces cas là, d'un traçage choisi (« *Etre « tracé » reste pour l'instant en grande partie un choix* » cirspec).

A l'instar du message de cirspec (« *si le dispositif était de très courte portée, une puce « ordinaire » donnerait toute satisfaction* »), le souhait général est d'en limiter la portée à quelques centimètres (l'exemple du pass Navigo mis en place par la Ratp a été mentionné).

6. Sur la création d'un organisme de contrôle ad hoc

Certains ont noté l'absence d'un véritable contre-pouvoir face au projet de CNIE et dénoncent la difficulté pour la CNIL de remplir ce rôle.

Beretta se demande si le projet de CNIE « *ne devrait pas être l'occasion d'une remise à plat du système de protection des données privées et des communications ?* ».

Zorglub42 estime que « *la fiabilité du système doit absolument être garantie et surtout certifiée par un organisme indépendant* ».

Banjo trouve qu'il pourrait être opportun de « *créer un nouvel organisme indépendant chargé de réguler les transferts de données qui seront inscrites sur la carte* ».

Vincemdk propose également « *la création d'une autorité administrative indépendante sur le modèle de la CNIL dont plusieurs membres seraient tirés au sort parmi la société civile, comme la Justice peut le faire pour les jurés d'assises?* ».

Dans le même esprit, Freez suggère qu'une « *commission spéciale soit instituée (autre que celles existantes) qui devra être radicalement indépendante et avoir pour mission la surveillance des données et des personnes qui y ont accès et de toutes les opérations possibles à partir de ces données (...). Ses membres devront jouir des mêmes protections que les magistrats qui pourront garantir un peu contre les pressions. (...) Des organisations/associations de citoyens devront pouvoir être présentes dans cette commission et des citoyens tirés au hasard dans la population (...) et bénéficiant des mêmes garanties que des représentants du personnel* ».

Enfin, Necronick souligne que les membres d'une instance indépendante, pour qu'ils restent eux mêmes indépendants, ne doivent pas jouir de « *privileges (primes, immunités, etc.)* » pour que leur engagement ne soit pas « *dicté par un intérêt personnel* ».

* *

REPONSE DU MINISTERE DE L'INTERIEUR

Sur les risques dans l'utilisation d'un fichier centralisé des empreintes digitales numérisées

De façon générale, l'article 34 de la Constitution indique qu'il revient à la loi de fixer les règles concernant les garanties fondamentales (dont relèvent la protection de la vie privée et l'interconnexion des fichiers).

La loi de base est celle qui a institué la CNIL, loi du 6 janvier 1978 modifiée en août 2004 qui définit le concept de données personnelles ou nominatives, les modalités de traitement et de protection. Chaque texte législatif ou réglementaire instaurant un traitement de données rappelle les principes et doit justifier les finalités du traitement et son caractère strictement nécessaire au regard du principe de proportionnalité. L'accès aux données d'un fichier ou d'un système de traitement doit être justifié (c'est ce qui est prévu dans le projet de loi INES). Les données peuvent être consultés par des "tiers autorisés" après accord de la CNIL.

Le projet présenté respectera toutes ces exigences conformément à l'avis que donnera la CNIL. On peut dire dorénavant et déjà qu'aucun lien ne sera possible avec les données relatives à la santé, la sécurité sociale, le fisc... ou le casier judiciaire. En outre, aucune de ces informations ne sera portée dans la carte.

Le projet INES a pour unique but de fiabiliser l'identité des citoyens, en garantissant le lien entre un individu et son identité par l'intermédiaire de ses empreintes digitales. Ainsi, les citoyens seront protégés contre l'usurpation de leur identité par un autre individu. De même, un individu cherchant à se prévaloir de plusieurs identités (y compris fictives) sera détecté par le système.

Aucune interconnexion avec un autre fichier n'est envisagée. Les accès aux fichiers INES seront strictement encadrés par la future loi INES dont le projet sera bientôt déposé. Les sanctions pour les dérives éventuelles seront renforcées.

Sur le fait que le projet ne risque pas de porter atteinte au respect de la vie privée

Le fait que la carte soit acceptée par toutes les administrations, les services financiers et commerciaux, signifie juste qu'ils la reconnaissent comme preuve d'identité. Exemples: au guichet d'une administration, pour retirer une lettre recommandée, pour ouvrir un compte en banque... Mais ils n'obtiennent AUCUNE autre information que celle relative à l'identité, c'est à dire les informations qui aujourd'hui sont inscrites sur la CNI. L'apport d'INES est de diminuer les risques de fraude à l'identité en certifiant le lien entre un individu et son identité.

Sur les données qui doivent être contenues dans la carte

Les informations contenues dans la carte seront **les mêmes que celles figurant sur l'actuelle CNI**, c'est à dire :

- Le nom.
- Le prénom.
- La date de naissance.
- Le lieu de naissance
- Le sexe.
- La taille.
- L'adresse.
- La photographie.

La date de naissance et le lieu de naissance font partie de l'identité de la personne, elles permettent d'éviter les confusions entre homonymes.

A ces informations, **s'ajouteront uniquement les empreintes digitales de deux doigts** pour garantir le lien entre le porteur de la carte et l'identité déclarée.

La puce ne contiendra en aucun cas des informations relatives à la vie privée du titulaire. En tout état de cause, afin de respecter les libertés des citoyens, **la puce ne contiendra pas:**

- Des informations médicales.
- Des informations bancaires.

- Le numéro INSEE du titulaire.
- Son appartenance religieuse, ethnique, etc.
- Son appartenance à un syndicat ou à un parti politique

Elle ne comportera pas, non plus, « d'historique » sur la vie de celui-ci (liste des contraventions qu'il aurait éventuellement eu, etc.).

La CNIE demeurera un document d'identité et rien d'autre.

Il ne se substituera pas aux autres titres et documents (permis de conduire, carte d'électeur...). Si les citoyens expriment le souhait de stocker sur la Cnie les éléments leur permettant de ne pas transporter quotidiennement d'autres documents (on pense au permis de conduire), il leur sera possible (et non obligatoire) de faire inscrire le numéro du dit document afin que, par exemple lors d'un contrôle routier, les forces de l'ordre puissent consulter la base des permis de conduire et vérifier que l'individu en est bien titulaire. Il s'agit bien de simplifier la vie du citoyen en lui évitant de porter sur lui plusieurs documents.

Cet ajout éventuel d'autres informations dans un espace « portfolio » a été envisagé. Il s'agirait exclusivement d'informations administratives enregistrées uniquement à la demande du porteur. Si cette idée ne répond pas à un besoin de la population, elle ne sera pas mise en œuvre.

Sur la maîtrise de la carte par son titulaire et sur les personnes habilitées à consulter les données stockées

Lors de la délivrance de la carte en mairie, le titulaire pourra consulter, pour vérification, les données personnelles contenues dans la puce. En outre il est prévu de permettre au titulaire de lire ses données personnelles tout au long de la vie du titre quand il le désirera, dans des lieux dédiés (et donc sécurisés). Pour l'instant aucune solution n'a été retenue mais l'on peut penser aux mairies où seront délivrés les titres.

Les informations personnelles (à part celles contenues, si le citoyen le souhaite, dans le portfolio) ne pourront être lues que par les autorités habilitées (services de police, gendarmerie, douanes, etc...) et pour des fins strictement encadrées (contrôle d'identité, vérification d'identité, franchissement des frontières

Les commerçants ne pourront pas lire le contenu de la puce.

Ils pourront en revanche s'assurer de l'authenticité du titre par un moyen plus sécurisé qu'aujourd'hui (contrôle visuel) avec la fonction d'authentification de la carte.

Concernant les outils d'administration électronique, ils ne pourront être mis en œuvre par le titulaire qu'en utilisant un code secret.

Sur le risque de lecture, à distance et à l'insu du porteur, des données inscrites sur la carte

Il ne faut pas confondre les étiquettes RFID, faites, comme toute étiquette, pour être lues facilement, avec des puces sans contact comme celles prévues dans la carte INES.

Le projet de carte prévoit que l'accès sans contact à la puce (accès uniquement à identité/photo/biométrie) :

- 1) nécessite un code pour accéder à au bloc « identité/photo », ce code se déduit des éléments imprimés sur la carte et nécessite donc de tenir la carte en main. Il s'agit d'un mode d'accès identique à celui retenu pour les passeports du monde entier par les différents Etats mettant en œuvre les titres biométriques.
- 2) nécessite un autre code et un matériel spécifiques pour accéder aux empreintes. Ce code et ce matériel seront réservés aux services de contrôle européens pour

les contrôles d'identité et les passages aux frontières. Il s'agit d'un mode d'accès identique à celui retenu pour les passeports européens (règlement européen du 13/12/04).

Aucun autre accès sans contact n'est prévu.

Il ne sera donc impossible d'effectuer des identifications à distance et sans consentement du citoyen.

SYNTHESE DES CONTRIBUTIONS DES INTERNAUTES SUR LE THEME « SECURITE » DU 27 MAI 2005

1. Sur la fiabilité des outils biométriques et électroniques

De nombreux messages notent que la sécurité d'un système informatique ne peut être établie que pour une durée limitée et que, de toute façon, un système ne peut être sécurisé à 100% (pour **stefloft** « aucun système est inviolable, sinon cela se saurait », pour **holylvier** « aucun système n'est infaillible » etc.).

De plus, **truc12** s'interroge sur la « pérennité » d'un système informatique. A ses yeux, un système supposé fiable « impose de mettre en place dès (sa conception) les moyens de gérer les exceptions ou anomalies qui auront lieu entre le moment où les premières faiblesses seront constatées et le moment où leurs parades seront mises en place et les moyens de le faire évoluer ». Si ce postulat est respecté il craint paradoxalement que « cette course à la technique » n'entraîne « des dérives de coût importantes ». De la même façon, **Rikouman** rappelle que « si on tient compte de la vitesse à laquelle avancent les technologies, votre puce sera obsolète dans moins d'une dizaine d'années. Qu'est-ce que cela signifie ? Que l'Etat va se lancer dans une course en perfectionnant les documents d'identité et en y ajoutant de plus en plus d'éléments (aujourd'hui les empreintes digitales, demain l'iris de l'oeil, ensuite l'ADN) ».

D'autres messages notent que l'introduction de l'informatique peut intrinsèquement apporter des éléments intéressants et novateurs pour l'être humain mais qu'en revanche il convient de veiller attentivement à la façon dont on utilise cet outil. Pour beaucoup, le problème n'est donc pas l'informatique mais ce qu'on en fait. Ainsi, **Zorglub42** déclare être « rassuré sur la fiabilité technique » du projet mais pas sur « la sécurité du système, incluant les hommes et les procédures. Et là, on retombe dans le fameux débat qui peut déraper facilement sur le flicage ! ».

De façon générale, et comme le souligne **john c** « le présent débat aura permis de souligner notamment les inquiétudes des internautes sur le "sans contact" (beaucoup de confusion cependant avec les puces RFID utilisées notamment pour la gestion des stocks de marchandises) et sur les données biométriques inscrites sur la carte ».

a. Les outils biométriques

Pour beaucoup, l'utilisation de la biométrie est assimilée à une méthode de police principalement utilisée pour « ficher » les délinquants. **Eupalinos** explique ainsi sa méfiance vis-à-vis de cette technologie « parce que la biométrie est un processus policier et que sa généralisation serait la consécration d'un Etat policier ».

Pshunter estime que « le vrai problème de la biométrie est sa relative non-fiabilité (il est assez facile de tromper un lecteur d'empreintes digitales) mais surtout sa non-révocabilité ». Il rejoint à cet égard **lelou** qui relate les propos écrits en 2003 par l'un des responsables actuels de la Direction centrale de la sécurité des systèmes d'information (DCSSI) pour qui la biométrie « a au moins deux limites : ce n'est pas une méthode confidentielle et c'est une méthode rigide. L'authentification par empreintes ne remplacera pas un login/mot de passe car une empreinte n'est pas un secret : c'est exploitable : on laisse 20 traces de doigt/jour exploitables (...). De plus il existe de nombreuses techniques permettant de passer outre les mécanismes de sécurité reposant en tout ou partie sur la biométrie (exemple en mai 2002, un chercheur japonais fabrique avec de la gélatine de vraies-fausses empreintes digitales qui ont leurré 11 des 15 systèmes biométriques testés) ». A cet effet, **Flag** se demande « Que dois-je craindre finalement si mes empreintes digitales sont récupérées par quelqu'un ? Que peut-il en faire ? ».

D'autres estiment que l'emploi de la biométrie sécurise et facilite le processus. Ainsi **Jeando** estime que « *Le système optique couplé à une reconnaissance digitale semble le plus pratique, et le plus rapide, pour les aéroports. (...) Surtout que les cartes on peut les oublier, se les faire voler, se les faire falsifier, entrer sans papiers, avoir des faux papiers etc. Tandis que sa pupille, ses doigts, son sang on les a sur soi ! Pas de crainte de se les faire voler !* ».

b. La carte à puce

La falsification du support carte à puce a souvent été évoquée. A l'instar de **Tetchawet** ils estiment ainsi que « *l'on sait tous aujourd'hui avec quelle facilité une carte à puce peut être falsifiée, que ce soit une carte téléphonique ou un carte de paiement* ».

Beaucoup se posent également des questions. Ainsi, **Holyvier** se demande « *sur combien de bits est codée la clé d'accès aux protocoles de lecture et d'écriture de la puce ? La puce est-elle activée selon un protocole RFID ?* ». **Flag** se demande « *si la puce est accessible aux tiers, comment garantir que les clés de cryptage ne finiront pas par être connues de tous ?* » et « *dans 10 ans, que vaudront les algorithmes de cryptage choisis en 2005 ?* ». **AAA** se demande « *Comment éviter les fausses cartes pour tous ceux qui vérifieront l'identité d'une personne sans pouvoir accéder à la puce ? (...) Comment le commerçant qui vérifie l'identité pour accepter un chèque saura-t-il que la carte est fausse ? Comment le service de sécurité privé d'une grande entreprise pourra-t-il savoir qui est effectivement entré dans ses locaux malgré un contrôle d'identité à l'entrée ?* ».

2. Sur la lecture sans contact des données de la carte

A l'instar de **John c**, beaucoup se demandent si « *le "sans contact", dont on nous dit que la portée sera extrêmement faible, est dans ce cas vraiment nécessaire ?* » ; partagent cette interrogation et, comme lui, ne saisissent « *pas très bien son intérêt, d'autant plus que cette fonctionnalité suscite sans doute le plus de désapprobation* ».

En effet, la perception générale a été qu'il y a un risque qu'à l'insu du porteur la puce sans contact puisse être lue à distance. Certains, comme **oncleo** pensent même « *qu'il suffira simplement de placer discrètement des bornes de lecture partout où on l'aura décidé pour savoir qui passe à proximité* ». D'autres font des amalgames entre les puces RFID (*Radio Frequency Identification*) et celle contenue dans la carte.

A chaque fois, des précisions et des réponses ont pu être apportées.

Ainsi, **Beretta** a rappelé que l'introduction du « *sans contact dans le passeport électronique est principalement du a des raisons pratiques, la lecture sans contact a d'incontestable avantage (...)* : plus de problème de contact oxydés ou dégradés, de lecteurs encrassés, d'usure mécanique, une vitesse de traitement globalement plus rapide ».

Au ministère de l'intérieur qui précise qu'il « *ne faut pas confondre les étiquettes RFID, faites, comme toute étiquette, pour être lues facilement et à longue distance (répondant à la norme ISO 15693, " RFID vicinity ")*, avec des puces sans contact comme celles prévues dans la carte INES répondant à la norme ISO 14443 " proximity " dont l'émission est limitée à quelques centimètres », **Beretta** répond que « *la portée de ces deux normes dépend principalement de l'environnement et de la puissance de la base inductive, ces données ne sont que des références en utilisation normale en aucun cas elle ne peuvent couvrir toutes les situations* ».

De même, au ministère qui affirme qu'il « *sera donc impossible d'effectuer des identifications à distance et sans consentement du citoyen* », **Beretta** poursuit en estimant « *qu'il y a trop peu de données pour dire que le schéma de protection est de facto sur, je ne suis pas spécialiste en cryptanalyse mais j'aimerais bien avoir l'avis d'expert indépendant quant a ce standard et les attaques envisageables. Dans l'état actuel du projet dire que quelque chose est impossible est très présomptueux* ».

Certains ont précisé qu'il existe des moyens techniques d'empêcher une lecture sans contact des données.

Abadie note ainsi que « *tout système de lecture à distance par induction peut être neutralisé simplement en enfermant la carte à lire dans une enveloppe métallique (du papier d'aluminium fait déjà l'affaire dans 95% des cas)* ». **Beretta** confirme ce point : « *l'utilisation d'un étui métallique peut être jugé un brin paranoïaque mais c'est la seule protection absolument fiable qui rend la fonction de lecture de dialogue à distance inopérante (...). C'est un peu extrême comme solution mais c'est une double protection, dans un étui métallique qui fera office de cage de Faraday, la carte ne peut plus être alimentée en énergie (pas d'induction possible et la carte n'est pas autonome)* ». Beretta se demande enfin si « *la proposition de l'ICAO de protéger la carte dans un étui métallique sera appliquée ?* ».

Face à ces propositions de protection technique, **ann** se demande « *serais-je suspect si je place ma carte contre deux plaques métalliques formant une cage de Faraday, et que ma carte n'est ainsi pas lisible sur les terminaux de la police ?* ».

Même si **holylvier2** a estimé que « *cette technique n'est pas efficace sur toutes les puces : MBBS a développé un système RFID unique permettant de lire/écrire de l'information à travers le métal ou dans un environnement métallique. Le système opère à une fréquence de 125 kHz et est basé sur un TAG passif n'exigeant aucune source d'énergie embarquée* », **Mad_Donkey et toto36** estiment qu'il se trompe. Pour **Mad_Donkey** « *la norme 14443 ne fonctionne pas du tout à cette fréquence mais à 13.56Mhz ; de plus la cage Faraday va aussi bloquer le champ magnétique et non seulement les communications radio donc la puce ne sera pas alimentée donc elle ne fonctionnera pas* ». **Toto36** indique qu'il est spécifiquement prévu que les puces MBBS puissent être lues à travers du métal mais que ceci est « *une technologie unique pour fonctionner là où les autres ne fonctionnent pas. (...) La plupart des puces RFID sont perturbées par le métal (...) et quelques puces d'un type particulier arrivent à surmonter ce handicap. Il faut donc exiger et vérifier que les puces de la CNIE ne soient pas des puces MBBS pour que le boîtier métallique ait tout son intérêt !* ».

3. Sur les certificats et la signature électronique

Certains font a priori confiance à la sécurité d'un système fondé sur de la signature électronique. Ainsi, pour **AAA** « *ce n'est pas le caractère asymétrique de la crypto utilisée qui rend les cartes robustes ou pas, c'est bien la longueur de la ou des clés utilisées pour les protéger. Les "yes cards" sont le résultat de l'ineptie du GIE carte bancaire qui n'a pas voulu rallonger la taille des clés dès qu'elles ont été craquées. Il est vrai que la leçon a été retenue et que de ce point de vue INES présente des garanties suffisantes. Je peux confirmer que DU FAIT DE LA LONGUEUR DES CLES proposées la carte INES est actuellement inviolable. Il faudra qu'elle le reste et il faut donc utiliser des clés plus longues que le strict nécessaire* ».

En revanche, d'autres, comme **Fabien Petitcolas** estiment qu'en ce qui concerne la signature électronique, « *l'authentification se fait jusqu'au niveau de l'ordinateur utilisé pour la signature. Le lien entre cet ordinateur et (le contenu du message) reste incertain... Résultat vous pouvez signer quelque chose de différent de ce que vous croyez signer, sans même vous en rendre compte* ».

Réagissant aux précisions du ministère de l'intérieur qui précise que la carte à puce aura une « *signature électronique " sécurisée " évaluée au niveau " EAL 4+ " sur le profil de protection " SSCD " (secure signature creation device)* » **Beretta** estime qu'un niveau annoncé de EAL 4+ est « *insuffisant, je pense qu'un niveau 5 serait un minimum un 6 serait souhaitable, même si évidemment cela impliquera un surcoût et du plus de temps/retard* ». Cet internaute précise que « *les cartes déjà évalués par la SSI ne sont que très rarement évalués au delà du niveau EAL4+ (niveau bâtard d'évaluation créé*

par complaisance avec les fabricant de carte pour ne pas les obliger a suivre un processus d'évaluation long et nécessitant la divulgation a l'organisme de certification des mécanismes sous-jacent du système) ».

Partant du constat que d'un côté « *la fraude sur Internet (...) repose sur des identifiants statiques numérisables et reproductibles, tels que les numéros de carte bancaire, les identifiants et les mots de passe* » et que, de l'autre, « *les données biométriques sont des données statiques numérisables et reproductibles* », **pachat** estime que « *la sécurité sur Internet (...) repose sur les token (jeton) signature PKI avec une clé privée unique et imprévisible assurant une authentification forte, qui associée à des protocoles de sécurité (SSL) assure la meilleure sécurité pour une transaction* ». Or, à ses yeux, le programme INES « *ne présente d'avantage que pour le ministère de l'intérieur français, il peut s'avérer dangereux pour les citoyens qui l'utiliseraient pour sécuriser leur transaction sur Internet* ».

Certains se posent des questions au niveau du marché de la signature électronique et pensent, à l'instar de **Beretta**, que l'Etat ne voulant « *pas faire d'ombre aux promoteurs ou principaux metteurs en oeuvre du projet, les entreprises seront toujours fortement encouragé a acheter des certificats auprès des sociétés privés qui seront derrière la technologie de la CNIE* ». Cet internaute estime que « *l'Etat en matière de signature électronique et de cryptage ne fait que le minimum syndical, remplir le vide laissé faute de rentabilité par le secteur privé en évitant soigneusement de concurrencer ce dernier.* ». **Arena** se demande ainsi « *qui seront les tiers de confiance et les tiers horodateurs ? des acteurs privés ? (...) je dis oui a la carte électronique, je dis non a la signature électronique, principe de précaution* ».

A l'inverse d'autres, à l'instar de **truc12**, estiment que l'intervention de l'Etat dans ce domaine risque de fausser la concurrence et se demandent également si une opération signée électroniquement sera « *opposable par l'administration à un administré ou sera t elle une simple indication ? En d'autres termes, une défaillance quelconque (...) du système sera-t-elle à charge de l'administré ou de l'administration ?* » et « *dans une utilisation administrative ou commerciale, quelle sera la responsabilité de l'Etat en cas de litige?* ».

Zorglub42 note que l'Agence pour le développement de l'administration électronique a publié PRIS version 2 qui élabore des schémas pour avoir des solutions de signatures électroniques utilisables dans le cadre de la dématérialisation des procédures administratives : « *Ces travaux devraient permettre aux particuliers d'acheter des certificats à des prestataires du secteur privé. Cela sous-entend-t-il que le certificat sera obtenu après vérification de l'identité à l'aide du bloc identité de la CNIE ? Comment ce certificat sera chargé sur la CNIE ?* ».

Concernant la lecture de la carte à puce par les ordinateurs familiaux, **phil13** note « *le manque ENORME de sécurité sur les ordinateurs familiaux (et même ordi de sociétés) pleins de petits spy très curieux, sans parler des 300 nouveau virus découvert quotidiennement par les sociétés spécialisées* ».

4. Des propositions et autres scenarii pour améliorer le système

Un certain nombre de propositions ont été formulées pour améliorer le système de sécurité tel qu'il est présenté actuellement dans le projet.

A titre liminaire, **gacb** estime fondamental que « *l'électronique soit bien maîtrisé* » pour cela cet internaute estime que le projet de CNIE ne peut être mis en place sans « *un cahier des charges rigoureux et de haut niveau, le verrouillage des bases de données, un maximum de contrôles (c'est fait !), un cryptage maximum, des équipements de la*

meilleure qualité et des investissements appropriés (et de préférence européens... partageons les coûts avec nos voisins) ».

Zorglub42 estime qu'il « *faudrait au moins garantir une certaine confiance dans l'utilisation du système (hommes et procédures)* » et, à ce titre, se demande si l'on « *pourrait évoquer la possibilité d'une certification BS7799 ou équivalent ?* ». A propos de la certification BS7799, **Beretta** précise « *que cette certification n'est pas franchement destinée à un organe d'Etat (elle est par exemple inapplicable à un commissariat de police)* ». Cet internaute estime quant à lui que « *l'ouverture des standards et une architecture ouverte sont des gages de transparence* ».

Des scénarios alternatifs ont également été proposés soit en terme de fichier des empreintes digitales numérisées, soit en termes d'architecture globale du système d'authentification.

Zorglub 42 et **toto36** se demandent s'il est vraiment nécessaire, en fonction de l'objectif recherché, de mettre en place un fichier centralisé.

Ainsi, **Zorglub 42** se demande « *d'un point de vue technique, pourquoi stocker les empreintes et non pas un scellement (checksum) pour comparaison ?* » Il précise que « *si le but du fichier est de « lutter contre l'usurpation d'identité : (...) un simple fichier de signature/hash/checksum des empreintes suffirait* ».

De même **toto36** note que « *pour vérifier l'existence de carte d'identité, un tel fichier est inutile. Il suffit de le remplacer par une procédure d'interrogation à distance des fichiers locaux existants. Cette procédure peut être accélérée par des mécanismes comme ceux décrits par antinom le 23/04 ou AAA le 18/05* ».

AAA propose en effet « *un fichier central de gestion des cartes sans lien avec l'identité en clair du porteur. Le seul lien serait un hash d'une empreinte biométrique pour éviter les fraudes. La gestion des cartes permettrait de savoir si une carte est valide, perdue, volée... Le hash permettrait d'éviter qu'un même individu puisse avoir deux cartes avec des identités différentes* ».

AntiNOM quant à lui, partant du constat qu'il y a « *peu de probabilité pour que deux personnes puissent se ressembler physiquement ET digitalement ET être nés au même endroit ET de parents qui sont eux aussi nés au même endroit* », propose « *que chaque paramètre débouche sur un ID (gabarits physiques et données du livret de famille), et qu'il soit créé un ID unique par combinaison de ces ID + l'ID du commissariat + l'ID de l'agent en charge du dossier. Ce N° serait donc unique, et plus complet que le n° de SS* ». Il poursuit en précisant que « *l'ID obtenue serait cryptée par deux clés: le code secret du détenteur et un autre code géré par un central "d'autorisation". C'est cet ID crypté qui apparaîtrait dans la base de donnée centrale et dans la puce. Pour l'authentification ponctuelle, l'agent devra s'identifier auprès du central, afin d'avoir accès au 2ème code. La réponse de la base de donnée serait "oui, cet n°ID existe, il a été généré au commissariat untel. Pour en savoir plus, se connecter à ce commissariat" (...). La base de données ne contient que des N° ID incompréhensibles sans les deux codes. Les données biométriques sont décentralisées. Elles ne sont pas directement codées sur la cartes: elles sont intrinsèques à l'ID qui fait foi* ».

En ce qui concerne la consultation des données par les agents habilités, **holyvier2** propose que le « *"matériel spécial"* » soit « *équipé d'un système comparable à une sorte de boîte noire qui garderait la trace de l'heure, de la date des identifiants des CNIe consultées et des identifiants des personnes habilitées ayant procédé à l'identification* ».

Vis-à-vis de cette proposition, le ministère de l'intérieur a annoncé que « *les spécifications de ce matériel ne sont pas arrêtées à ce jour; votre suggestion est intéressante et devra être étudiée. (d'où l'intérêt de ce débat: on peut encore prendre en compte les bonnes idées)* ».

Enfin, **toto37**, estimant que « *tous les experts en sécurité diront qu'il faut d'abord examiner la sécurité de l'ensemble du système pour ensuite répartir les fonctions de*

sécurité entre les différents composants du système », rappelle que le SCSSI (services centraux de la sécurité des systèmes d'information) recommande l'utilisation d'EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité) qui est une méthode/étude d'appréciation et de traitement des risques relatifs à la sécurité des systèmes d'information. Cet internaute ajoute néanmoins que « pour éviter de publier tous les résultats d'une telle étude, ce qui pourrait porter atteinte à la sécurité de l'ensemble, il pourrait être envisagé de former un groupe d'experts, reconnus et mandatés par les différentes parties prenantes pour valider cette étude EBIOS et informer leurs mandants des conclusions à retenir (...). Ces experts valideront également les cibles de sécurité (fonctions et niveau d'assurance) des éléments devant subir une évaluation selon le schéma national de certification conformément à l'ISO 15408".

A cet égard, **Beretta** propose également que soit mené une « étude indépendante de la CNIE par des chercheurs ».