

Le Forum des droits
sur l'internet

RAPPORT

Projet de carte nationale d'identité
électronique

SOMMAIRE

| | |
|---|-----------|
| INTRODUCTION | 4 |
| I. LES POINTS FORTS DU DÉBAT PUBLIC | 5 |
| A. – Sur les questions centrales | 5 |
| 1. – Sur la justification du projet | 5 |
| a) Lutter contre la fraude à l'identité..... | 5 |
| b) Lutter contre le terrorisme..... | 6 |
| c) Simplifier la vie du citoyen : une seule procédure pour la demande de deux titres (CNIE et passeport) et une accélération des renouvellements..... | 6 |
| d) Offrir aux citoyens les moyens de signer électroniquement ses transactions sur internet..... | 6 |
| 2. – Sur la protection de la vie privée..... | 7 |
| a) Sur les risques dans l'utilisation d'un fichier centralisé des empreintes digitales numérisées..... | 7 |
| b) Sur la maîtrise de la carte par son titulaire et sur les personnes habilitées à consulter les données stockées | 10 |
| c) Sur le risque de lecture, à distance et à l'insu du porteur, des données inscrites sur la carte | 11 |
| d) Sur la création d'un organisme de contrôle <i>ad hoc</i> | 11 |
| e) Sur l'utilisation du Répertoire national d'identification des personnes physiques (RNIPP)..... | 11 |
| 3. – Sur la biométrie | 12 |
| a) Des débats sur cette forme particulière d'identification par le biais d'une partie du corps 12 | |
| b) Des débats sur la fiabilité de la biométrie..... | 14 |
| c) Des débats sur l'opportunité des biométries choisies..... | 14 |
| d) Des débats sur le marché de la biométrie et le coût de la biométrie associée à la carte à puce | 15 |
| 4. – Sur la sécurité du système | 15 |
| a) Sur les certificats et la signature électronique..... | 16 |
| b) Sur l'emploi de la carte à puce..... | 16 |
| c) Des propositions pour améliorer la sécurité du système | 16 |
| d) La faille de sécurité au niveau de l'état civil | 17 |
| 5. – Sur les usages | 17 |
| a) Un intérêt très limité pour l'aspect « portfolio personnel »..... | 17 |
| b) Des confusions et des incompréhensions | 17 |
| c) Peu d'intérêt voire des interrogations quant aux fonctionnalités internet de la carte (certificat et signature électronique)..... | 18 |
| d) Quelques questions sur le contexte européen | 19 |
| 6. – Sur les mesures d'accompagnement | 19 |
| a) Le coût..... | 19 |
| b) Le caractère obligatoire | 20 |
| c) Le lieu et le mode de délivrance | 21 |
| B. – Sur les questions plus générales | 22 |
| 1. – La place de l'identité..... | 22 |
| a) La carte nationale d'identité électronique permettra utilement de sécuriser l'identité | 22 |
| b) Quelle gestion de l'identité à l'heure du numérique ? | 23 |
| 2. – Le rôle et la responsabilité de l'État | 24 |
| a) Quelle responsabilité pour l'État certificateur ?..... | 24 |
| b) L'intervention de l'État dans la sphère marchande..... | 24 |
| 3. – Le principe de précaution en matière de nouvelles technologies | 25 |
| 4. – La fracture numérique | 25 |

| | |
|--|-----------|
| II. ANALYSE CRITIQUE DU PROCESSUS DU DÉBAT..... | 26 |
| A. – Le débat est-il efficient ?..... | 28 |
| 1. – Le débat en chiffres..... | 28 |
| 2. – Une fonction d'alerte sur un sujet sensible..... | 28 |
| 3. – L'impact du débat sur le projet de carte nationale d'identité électronique..... | 28 |
| B. – Le débat public est-il fiable ?..... | 30 |
| III. ANALYSE ET RECOMMANDATIONS DU FORUM DES DROITS SUR L'INTERNET | 31 |
| A. – Les enjeux de sécurité sont essentiels aux yeux des Français mais les arguments avancés à l'appui du projet n'ont pas convaincu..... | 31 |
| 1. – Des études sur la fraude à l'identité..... | 31 |
| 2. – Un découplage avec le projet passeport..... | 31 |
| B. – La protection de la vie privée est une préoccupation majeure à laquelle le projet doit apporter des garanties complémentaires..... | 32 |
| 1. – Un nouveau pacte social doit être conclu entre l'État et le citoyen..... | 32 |
| 2. – Il convient de porter une attention particulière sur la mise en place d'un identifiant unique..... | 32 |
| 3. – Le projet de carte nationale d'identité électronique doit faire l'objet d'un contrôle global et permanent..... | 33 |
| C. – Des incertitudes à lever en termes de sécurité..... | 33 |
| 1. – Une évaluation de l'aspect lecture « sans contact » de la carte..... | 33 |
| 2. – L'articulation entre le projet INES et celui de dématérialisation de l'état-civil..... | 34 |
| D. – Une attente mitigée par rapport à une carte de services..... | 34 |
| 1. – Un faible intérêt pour une CNIE utilisable pour les téléprocédures administratives..... | 34 |
| 2. – Une réticence assez forte pour une carte « signeuse » pour les échanges marchands..... | 34 |
| E. – Des réticences sur le caractère payant et obligatoire de la carte nationale d'identité électronique..... | 34 |
| 1. – La carte doit être gratuite à la première délivrance..... | 34 |
| 2. – Un débat devant le Parlement sur le caractère obligatoire..... | 35 |
| F. – La sensibilité de l'enjeu territorial..... | 35 |
| G. – Le contexte européen..... | 35 |
| Conclusion..... | 35 |
| ANNEXES..... | 36 |
| Lettre de mission..... | 37 |
| Experts intervenus aux débats en ligne et en région..... | 39 |
| Comptes rendus des débats en régions et en ligne et les contributions des experts en ligne..... | 42 |
| Le sondage Ipsos/Forum des droits sur l'internet..... | 44 |

INTRODUCTION

Le projet de création d'une carte nationale d'identité électronique (CNIE) est un projet majeur. Il a pour objectif de renforcer la qualité et la sécurisation des titres d'identité, mais aussi d'offrir de nouveaux services aux citoyens en leur donnant les moyens de prouver leur identité sur internet et de signer électroniquement. Ce faisant, il devient un projet qui va changer une partie de la vie des Français. Le ministère de l'Intérieur a souhaité recourir à un projet de loi pour le mettre en œuvre.

Le Forum des droits sur l'internet a pris l'initiative de proposer au ministère de l'intérieur d'organiser un débat public sur ce projet afin de donner à toutes les sensibilités et à tous les points de vue la possibilité de s'exprimer. Le ministère de l'intérieur a ainsi officiellement mandaté le Forum à ce sujet en janvier 2005 (voir lettre de mission en annexe).

Pour répondre à cette mission, le Forum des droits sur l'internet a mis en place trois outils : un débat en ligne et un débat en régions qui ont duré quatre mois (début février à début juin 2005) ; plus de 3000 messages ont été postés et des manifestations publiques se sont tenues dans six villes ; par ailleurs, le Forum a invité des personnalités expertes à participer aux débats, soit dans les régions, soit en envoyant des contributions dans le débat en ligne.

Le Forum a souhaité également organiser un sondage sur le sujet. Avec l'institut IPSOS, il a ainsi recueilli l'opinion de 950 personnes, correspondant à un échantillon représentatif de la population et ces résultats orientent également les conclusions (voir sondage en annexe).

À partir de l'ensemble de ces contributions, le Forum des droits sur l'internet a élaboré le présent rapport. Le rapport a été adopté par le Conseil d'orientation du Forum dans sa séance du 14 juin 2005.

Ce rapport a pour objectif d'alimenter la réflexion des pouvoirs publics sur le sujet, dans la perspective du débat parlementaire.

* *
*

I. LES POINTS FORTS DU DÉBAT PUBLIC

A. – Sur les questions centrales

1. – Sur la justification du projet

Les enjeux et les changements induits par le projet de carte nationale d'identité électronique (caractère obligatoire et payant, base centralisée, biométrie, délivrance dans quelques mairies...) sont de la première importance. Les motivations d'un tel projet se doivent d'être clairement expliquées et convaincantes, les garanties largement développées, les aspects techniques et de sécurité fondés sur des travaux fiables et des études nombreuses. En effet, comme le précise Patrice Flichy, professeur de sociologie, « *en matière d'atteinte aux libertés publiques, les fantasmes peuvent parfois devenir réalité. Aussi est-il important de donner au citoyen le maximum de garanties et même plus que ce que les techniciens estiment sans doute nécessaire.* »¹

Tout le débat tourne en effet autour de l'équilibre à trouver entre protection des libertés individuelles et sécurité de l'identité et sur la façon dont le ministère de l'intérieur a pu faire comprendre aux Français participant aux débats sa vision et ses projets dans le domaine de l'identité nationale électronique sécurisée.

Or, comme le note Michel Elie, président de l'Observatoire des Usages de l'Internet, « *nous demandons encore à être convaincus par votre solution* »². Ces propos reflètent bien le sentiment qui s'est constamment exprimé tant en ligne qu'en régions. Alors que d'un côté les changements annoncés semblent bien réels, de l'autre, le projet semble lancé avec « *précipitation* »³ et avancé pour des raisons trop légères sans justification convaincante.

Le ministère de l'intérieur justifiait la mise en place d'une CNIE par le biais de quatre arguments :

a) Lutter contre la fraude à l'identité

La lutte contre la fraude à l'identité semble être une préoccupation majeure des Français puisqu'à la question « *dans le cadre de la lutte contre la fraude à l'identité, le ministère de l'intérieur envisage de remplacer la carte d'identité actuelle par une carte d'identité électronique comportant des données personnelles numérisées telles que empreintes digitales, photographie, voire iris de l'œil* », 74 % des sondés répondent favorablement et 25 % défavorablement.

Pour autant, et alors que cet argument semble fondamental voire justifier en lui-même la mise en place d'une carte nationale d'identité électronique, le ministère de l'intérieur ne dispose d'aucune donnée chiffrée précise à l'appui de cet argument ; aucune étude systématique n'a été conduite en France. Les chiffres avancés dans le débat par le ministère sur la fraude à l'identité ne s'appuient que sur des études étrangères (principalement américaines ou britanniques). À cet égard, beaucoup se sont demandé s'il est possible de se référer à des chiffres avancés dans des pays étrangers alors que les instruments et dispositifs d'identification qui y sont employés ne sont pas du tout les mêmes que ceux mobilisés en France (par exemple, pour les États-Unis, surtout le numéro de sécurité sociale et le permis de conduire et pour le Royaume-Uni, l'inexistence de carte nationale d'identité depuis 1952).

À cela le ministère de l'intérieur a répondu tout au long du débat que seuls les ministères des finances et des affaires sociales seraient à même d'établir le coût de la

¹ Contribution sur internet de Patrice Flichy, 13 avril 2005

² Message sur internet de Michel Elie, 17 avril 2005

³ Contribution de Martial Gabillard, débat de Rennes, 11 mai 2005

fraude et il a précisé que le Sénat a justement mis en place une mission d'information sur la nouvelle génération de documents d'identité et la fraude documentaire afin notamment de pouvoir établir des données chiffrées sur la fraude. Le ministère a cependant admis qu'il convenait de travailler sur ce point.

b) Lutter contre le terrorisme

De même, cet argument a peu convaincu et les questions ont été nombreuses : un tel dispositif permettra-t-il vraiment de repérer un primo-terroriste ? En quoi cela empêchera-t-il quelqu'un qui souhaite commettre un acte terroriste de ne pas obtenir, en toute légalité, une CNIE ? À cet égard, certains se demandent si l'on ne se sert pas des contraintes internationales sur le projet passeport (Règlement européen du 13 décembre 2004⁴ adopté dans un contexte de lutte contre le terrorisme afin d'améliorer le contrôle des passages aux frontières et de répondre aux exigences américaines) pour faire adopter la CNIE. Or, le débat a montré que si la France doit appliquer le règlement sur le passeport dans un bref délai, cette obligation ne concerne pas la carte d'identité nationale⁵. De plus, l'argument du terrorisme a surtout donné l'impression que la France subissait des pressions étrangères, européennes et surtout américaines.

Le ministère de l'intérieur a précisé que la fausse identité (ou l'usurpation) est souvent à la base du phénomène terroriste et qu'en ce sens, toute action destinée à rendre plus fiable l'identité des citoyens est un moyen de lutter contre les atteintes à la sécurité publique. En ce qui concerne l'articulation avec le projet passeport, le ministère a reconnu qu'aucune obligation ne concernait effectivement la CNI, même si le fait de coupler les deux procédures pouvait être utile et opportun au regard notamment de la compatibilité de la carte avec celles des autres États européens.

c) Simplifier la vie du citoyen : une seule procédure pour la demande de deux titres (CNIE et passeport) et une accélération des renouvellements

Cet argument est le seul où il a pu être reconnu un intérêt : mais cet intérêt a été estimé très réduit par rapport aux enjeux du projet.

d) Offrir aux citoyens les moyens de signer électroniquement ses transactions sur internet

Cet argument n'a finalement que peu intéressé les participants qui ne voyaient pas son utilité, voire ont exprimé des réticences à avoir accès, sur un même support, à des usages administratifs et à des usages commerciaux ou encore de pouvoir faire une transaction sur internet, réseau ouvert et pouvant présenter de nombreuses failles de sécurité.

À l'issue du débat, on peut estimer, que le ministère de l'intérieur n'a pas convaincu dans les arguments avancés pour justifier le projet de carte nationale d'identité électronique. C'est d'ailleurs ce que résume l'internaute Algair, qui estime que « *dans l'équilibre fondamental entre protection des libertés individuelles et sécurité de l'identité, actuellement rien ne me convainc de la nécessité d'accepter d'abandonner un peu de liberté au profit de plus de sécurité* ».

Ce déficit d'explication a par ailleurs contribué à nourrir des craintes et à brouiller les enjeux. Ainsi, pour certains comme les internautes Minas et Zébulon, la mise en place

⁴ Règlement (CE) n° 2252/2004 du Conseil européen du 13 décembre 2004 « *établissant des normes pour les éléments de sécurité et les éléments biométriques intégrés dans les passeports et les documents de voyage délivrés par les États membres* ».

⁵ L'article 1 alinéa 3 du règlement exclut la carte d'identité de son champ d'application : « *Le présent règlement s'applique aux passeports et aux documents de voyage délivrés par les États membres. Il ne s'applique pas aux cartes d'identité délivrées par les États membres à leurs ressortissants.* »

de la CNIE émane d'une volonté de « *flicage* » du gouvernement ou fait suite aux peurs « *sécuritaires développées par les américains* » depuis les attentats du 11 septembre 2001. D'autres, n'y voient qu'une question d'argent et une pression des industriels (fabrication des puces, des cartes, des lecteurs, marché de la biométrie etc.). Ce déficit d'explication a également entraîné des confusions ou des erreurs. En effet, beaucoup ont estimé que la présentation du projet entraîne la confusion par le mélange des genres (projet destiné à la lutte contre le terrorisme, contre la fraude à l'identité, à développer la signature électronique, à des utilisations individualisées au moyen d'un « *portfolio personnel* »...). D'autres ont confondu les étiquettes RFID de la grande distribution avec l'interface radio de la carte d'identité ou ont cru que la carte servirait de moyen de paiement.

Cette impression générale de confusion est renforcée par le manque de coordination qui a été noté entre différents projets qui semblent néanmoins liés : CNIE, carte de vie quotidienne, dématérialisation de l'état-civil.

2. – Sur la protection de la vie privée

À titre liminaire il convient de préciser que l'aspect « *vie privée* » est celui qui a donné lieu au plus grand nombre d'échanges. Ces échanges ont exprimé des interrogations, des craintes mais aussi des erreurs voire des propagations de rumeurs ; certains ont pu par exemple dire que la CNIE serait « *un premier pas vers une puce sous-cutanée implantée chez tous les Français* ». Comme le remarque Pierre Trudel, professeur à l'Université de Montréal⁶ : « *Il demeure troublant de constater à quel point les risques de dérives semblent dominer les débats lorsqu'il est question d'outils et de procédés qui concernent l'identification des personnes (...) Rituellement, on exprime des préoccupations sur le potentiel liberticide des technologies de l'information. (...). La plupart des craintes à l'égard de l'usage des technologies de l'information concernent les opérations de surveillance policière.* »

De façon générale, beaucoup d'intervenants ont estimé que le passage de l'identité papier à l'identité électronique recèle un certain nombre de dangers en termes de protection de leur vie privée : la CNIE 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* ». À cet égard, de nombreuses discussions ont eu lieu entre les internautes. À 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'État qui mettrait en place un tel principe.

En revanche, pour d'autres participants, la mise en place d'une carte nationale d'identité électronique ne suscite pas de craintes particulières et permettrait de sécuriser utilement l'identité.

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

De nombreuses interrogations et critiques ont porté sur la mise en place d'une base centrale et sur les risques qui peuvent en découler. Pour Pierre Piazza, historien de la carte d'identité et chargé de recherche à l'Institut National des Hautes Études de Sécurité⁷, « *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*

⁶ Contribution sur internet de Pierre Trudel, 11 mai 2005.

⁷ Pierre Piazza, *Histoire de la carte nationale d'identité*, Paris, Odile Jacob, 2004.

tentatives de création de fichiers centralisés de données nominatives par le ministère de l'intérieur font l'objet des critiques les plus virulentes »⁸.

À cet égard il est très intéressant de comparer les résultats du sondage avec les impressions générales et réactions telles qu'issues du débat public. À la question : « *le ministère de l'intérieur prévoit de constituer un fichier informatique national des empreintes digitales. Laquelle de ces deux opinions se rapproche le plus de la vôtre ?* », 75 % des sondés répondent que c'est « *une bonne chose car cela permettra de lutter plus efficacement contre les fraudes* ». 23 % estiment que « *c'est une mauvaise chose car cela constitue une atteinte à la liberté individuelle* ».

Le débat a montré que, parmi ceux qui s'interrogent sur la mise en place d'une base centrale, deux types de risques ont principalement été évoqués : le risque de croisement de fichiers et de fichage des individus (à cet effet, beaucoup ont d'ailleurs proposé des schémas alternatifs à une base centrale) ainsi que celui d'une évolution future de l'usage de la base.

1) Le risque de croisement de fichiers et de fichage des individus

Constatant que les fichiers actuels sont décentralisés, certains 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, d'autres estiment que la véritable question est celle de l'encadrement de ces interconnexions et des consultations des données.

Pour d'autres encore, comme l'internaute Beretta, tout est « *un problème de finalité : si la biométrie a pour unique finalité d'associer un titre à son porteur quelle est l'utilité d'un fichier central des empreintes si ce n'est une vaste opération de police ? (...)* Si le fichier n'a pas de vocation policière cela devrait suffire à détecter la fraude ou les identités multiples ». De nombreux internautes vont d'ailleurs dans ce sens, Zorglub 42 se demande s'il est vraiment nécessaire, en fonction de l'objectif recherché, de mettre en place un fichier centralisé ; 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 AAA propose « *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* ». Enfin, l'internaute Alice propose un même type de scénario qui empêche de retrouver l'identité d'une personne à partir de ses données biométriques. Cet internaute précise que ce scénario protégerait davantage les données personnelles (empêcherait tout passage d'une base à l'autre et l'utilisation des données pour une autre fin que celle pour laquelle elles ont été collectées) mais que son unique finalité serait de gérer la fraude au renouvellement et d'assurer une délivrance sans doublon de cartes. Enfin, comme Alice le précise « *cette approche paraît robuste au détournement de finalité par contre, elle a un inconvénient structurel : elle ne permet pas d'identifier des victimes de catastrophes ou des amnésiques, et ne permet pas de lever le doute dans le cas où la biométrie est ou a été rendue illisible... Mais il faut savoir ce que l'on veut.* »

De plus, lors du débat de Lyon, il a été proposé deux alternatives au projet :

1. Il a été suggéré d'abandonner le projet de CNIE en renforçant la sécurité de l'actuelle carte nationale d'identité, en la rendant obligatoire et en sécurisant et informatisant l'état-civil. De façon générale, il a d'ailleurs été souligné que, quel que soit le projet retenu par le Gouvernement, sans informatisation de l'état-civil, le projet INES risque d'avoir des failles.

⁸ Message sur internet de Pierre Piazza, 13 avril 2005.

2. Plutôt que d'instaurer une carte d'identité électronique avec une base centralisée d'empreintes digitales numérisées, il a été proposé de créer une CNIE sans base centrale où les données numérisées seraient uniquement dans la puce de la carte. Ce scénario a rencontré un certain écho et de nombreux intervenants ont ainsi souhaité, à l'instar d'Éric Caprioli⁹, que les données biométriques soient uniquement dans la puce et qu'une base centrale ne soit pas mise en place. Meryem Marzouki, présidente de l'association IRIS (Imaginons un Réseau Internet Solidaire) a présenté¹⁰ un schéma alternatif qu'elle considère acceptable. Dans ce schéma, qui se rapproche, pour partie, de celui susmentionné, la CNIE ne doit qu'authentifier le porteur (la personne est bien celle qu'elle prétend être), à l'exclusion de toute possibilité d'identification d'un individu anonyme parmi une population ; la puce ne doit donc servir qu'à authentifier la carte comme étant un document non falsifié. IRIS estime également que la carte ne devra comporter aucun élément biométrique (cf. l'Italie, qui a développé une carte électronique où les empreintes digitales sont facultatives ; la Belgique propose une carte sans biométrie mais avec base centrale), que la photographie ne devra pas figurer sous forme numérisée dans la puce, mais uniquement de manière visible sur la carte pour identification par un contrôleur humain et qu'enfin il ne devra pas y avoir de constitution de base de données centralisée à l'image par exemple de l'Italie où la carte fonctionne sans base centrale.

Cette solution fait écho aux remarques de François Giquel, vice-président de la Commission Nationale de l'Informatique et des Libertés, qui a rappelé¹¹ qu'il existe d'autres scénarios pour la mise en place d'une CNIE en Europe. C'est le cas en Italie (carte sans base centrale et avec biométrie) ou encore en Belgique (carte sans biométrie mais avec base centrale car ce pays dispose d'un Registre national de la population).

De façon générale, le ministère a estimé que cette alternative ne répondrait pas à l'objectif du projet qui est de lutter contre la fraude à l'identité : seule une base centrale des empreintes permettrait d'éviter la délivrance à une même personne de titres sous plusieurs identités différentes ou à plusieurs personnes d'un titre sous une même identité. En revanche, le ministère de l'intérieur a proposé, dans le débat sur internet, une alternative en termes de biométrie en envisageant (à titre théorique, car cela ne figure pas dans le projet INES) que la puce de la carte contienne les empreintes (qui sont faciles à vérifier lors d'un passage de frontière), mais que la base centrale ne contienne pas les empreintes digitales, mais un autre élément biométrique comme l'iris de l'œil.

2) Le risque d'une évolution possible de l'usage de la base

À l'instar de Michel Tubiana¹², président de la Ligue des droits de l'Homme ou encore de Meryem Marzouki¹³, de nombreux intervenants ont noté les risques d'une évolution possible de l'usage de la base par les pouvoirs publics via un élargissement de l'accès à d'autres agents (cf. élargissement du nombre d'agents ayant accès au fichier du Système de Traitement des Infractions Constatées – STIC) ou un élargissement du contenu de la base à d'autres données. L'hypothèse la plus noire d'un changement de régime – spectre du retour d'un régime du type vichyste – a même été évoquée.

⁹ Contribution sur internet d'Éric Caprioli, 1^{er} juin 2005.

¹⁰ Contribution de Meryem Marzouki, débat de Lille, 27 avril 2005.

¹¹ Contribution de François Giquel, débat de Paris, 11 avril 2005.

¹² Contribution de Michel Tubiana, débat de Paris, 11 avril 2005.

¹³ Contribution de Meryem Marzouki, débat de Lille, 27 avril 2005.

b) 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 sa carte et dans les fichiers. Certains, comme Le Guet, souhaitent 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* ». Darhf souhaite que « *L'État 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?). Beretta et Zorclub42 se demandent « *Qui habilite qui ? Qui surveille la piste d'audit ?* ».

À ces interrogations, le ministère de l'intérieur a répondu :

1) En ce qui concerne l'accès du citoyen aux données contenues dans la puce et dans la base

L'accès au contenu de la puce se fera par le biais d'un accès direct, probablement à partir de bornes installées dans les lieux de délivrance des titres. De plus, le titulaire de la carte, en saisissant son code PIN, pourra donner accès aux administrations qui en auraient besoin dans le cadre des téléprocédures administratives.

En revanche, l'accès du citoyen au contenu de la base se fera par le biais d'un accès indirect, ce mode d'accès étant celui réservé aux fichiers gérés habituellement par le ministère de l'intérieur. Un accès direct ne peut être envisageable car, outre les données d'état-civil et biométriques, la base contiendra le « *journal* » des consultations de la base réalisées par les agents habilités.

2) En ce qui concerne l'accès des agents aux données contenues dans la puce et dans la base

L'accès aux données de la puce sera « *hiérarchisé* » selon le caractère confidentiel des informations contenues. Pour les empreintes digitales, seules les forces de police pourront les lire, à des fins de contrôle d'identité et ce dans le cadre de l'article 78-2 du code de procédure pénale.

L'accès à la base se fera de la façon suivante :

* le système sera géré par des agents habilités (agents chargés de la délivrance des titres, mairies et préfectures). Ces agents se contenteront de rentrer les données pour la délivrance des titres. Ils n'auront un accès à la base qu'en mode écriture, et limité aux données alphanumériques (nom, prénoms etc...) et à la lecture de la photo. Ils ne pourront ni consulter les empreintes digitales, ni lire les données personnelles d'un autre individu.

* Seules la police et la gendarmerie auront accès à la base des données biométriques, dans le cadre que fixera le projet de loi (possibilité réservée aux seuls officiers de police judiciaire sous le contrôle du parquet, à des fins de vérification d'identité et dans les conditions prévues par l'article 78-3 du code de procédure pénale). Ces consultations seront tracées (elles feront l'objet d'un « *journal* » qui retracera les interrogations faites).

c) 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. Certains se sont opposés à son principe même qui conduit à un contrôle de masse quantitatif et automatique des individus, assimilés à « *du bétail* ». Plus globalement, 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. « *L'identification « sans contact » aggravera encore le flicage, puisqu'on pourra être contrôlé sans même qu'on le sache* » dit, par exemple, Fanchick. L'association IRIS¹⁴ estime à cet égard que la lecture de la puce ne doit pas se faire sans contact.

Lors des débats le ministère a, par la suite, justifié ce choix en expliquant que le « sans contact » de la carte se conjuguerait avec les applications passeport (qui comportera également une puce sans contact insérée dans le livret), serait plus facile à utiliser (lors de contrôles de masse dans des aéroports par exemple) et s'userait moins.

d) 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.

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 et Freez proposent également « *la création d'une autorité administrative indépendante* » qui aurait « *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.* »

e) Sur l'utilisation du Répertoire national d'identification des personnes physiques (RNIPP)

Le projet prévoit que l'état-civil soit dématérialisé pour que les actes puissent être transmis directement et de manière sécurisée entre mairies de naissance et mairies de délivrance du titre. Pour ce faire, il serait prévu de permettre une consultation du Répertoire national d'identification des personnes physiques (RNIPP), tenu par l'INSEE, afin de valider si les données d'état-civil communiquées par la personne qui souhaite la délivrance d'un titre correspondent à celles enregistrées dans le RNIPP au niveau de la filiation.

Pour certains, utiliser le RNIPP semble logique dès lors que l'on utilise un circuit et une base existante et fiable. Pour d'autres, au contraire, cette solution a un impact symbolique fort et est porteur d'un certain nombre de craintes. C'est ce qu'ont exprimé des syndicats de l'Insee par le biais d'une lettre ouverte à leur directeur général¹⁵. Dans cette lettre, ils estiment que la participation de l'Insee à la constitution d'un fichier national d'identité n'a pas de précédent : il y a actuellement une séparation entre les fonctions statistiques et les fonctions de gestion policière de la population et l'usage du

¹⁴ Débat de Lille, 27 avril 2005.

¹⁵ Lettre ouverte du 17 mai 2005 des syndicats nationaux CGT, CFDT, SUD, CGT-FO, CGC, CFTC de l'Insee au Directeur général de l'Insee intitulée « *L'Insee n'a pas vocation à être une annexe du ministère de l'intérieur !* », message sur internet du 1^{er} juin 2005.

RNIPP comme une des sources pour constituer ou vérifier un fichier de police serait une rupture majeure (utilisation d'informations sur la filiation, problème de confiance...).

Plus généralement et d'un point de vue strictement historique, Pierre Piazza¹⁶ rappelle que ce n'est pas la première fois que l'utilisation du RNIPP est envisagée : notamment entre « 1946 et 1951, des rencontres sont organisées entre des fonctionnaires du ministère de l'intérieur et des représentants de l'INSEE. Il est alors prévu de recourir au Répertoire général d'identification constitué sous l'Occupation pour identifier chaque demandeur de la nouvelle « carte nationale d'identité » dont la création est envisagée. Cependant, ce sont, principalement, des « divergences de points de vue » sur la question de l'identification des Français musulmans d'Algérie qui aboutissent à l'abandon de ce projet.

3. – Sur la biométrie

La mise en place d'identifiants biométriques suscite de nombreux débats.

a) Des débats sur cette forme particulière d'identification par le biais d'une partie du corps

La biométrie¹⁷ est apparue comme étant un sujet sensible qui fait débat car il touche directement au rapport au corps. Gérard Dubey¹⁸, sociologue à l'Institut National des Télécoms, estime ainsi, à partir d'enquêtes et entretiens menés sur ce thème, que face à l'introduction de la biométrie, certains semblent vouloir dire : « C'est une part de moi que je laisse, donc je ne veux pas que mon intimité soit comme ça perdue sans que je sache ce qui va en être fait ». Il estime que ceci révèle autre chose que la crainte d'être fiché ou enregistré sur une base de donnée : « la question est plutôt que devient l'individualité, ce qu'il y a de singulier en chacun, une fois numérisé ? »

Ce questionnement fait écho au fait que dans les débats beaucoup ont estimé que, même si l'on a toujours eu recours à la biométrie, la grande différence réside actuellement dans l'introduction de l'informatique qui multiplie la puissance de cette technique d'identification. Comme l'exprime Yannick Comenge¹⁹, docteur en Biochimie, cette « rencontre entre biométrie et informatique est perturbante ». De plus, l'utilisation de la biométrie est assimilée par certains à une méthode de police principalement utilisée pour « fichier » les délinquants : l'internaute 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 État policier ».

À ce titre, le projet INES de numériser les empreintes digitales et la photographie suscite de nombreux débats.

Certains ont estimé, à l'instar de Bernard Didier²⁰, Directeur du développement des affaires à la division sécurité de Sagem, que parce qu'elle permet de mesurer le vivant et d'identifier les individus de façon performante, seule la biométrie permet de s'assurer que lors de la délivrance d'un titre celui-ci est délivré à la bonne personne. C'est d'ailleurs ce que confirment des internautes comme Michel Lo qui estime qu'il y a « des aspects positifs » dans la biométrie comme « le renforcement de la preuve de l'identité qu'on ne peut rejeter » ou encore Richard qui se prononce en faveur des

¹⁶ Message sur internet de Pierre Piazza, 13 avril 2005.

¹⁷ Analyse des caractéristiques biologiques d'une personne, destinée à déterminer son identité de manière irréfutable. La biométrie repose sur le principe de la reconnaissance de caractéristiques physiques (empreintes digitales, l'iris de l'œil, forme de la main, la voix etc.) qui sont censées offrir une preuve irréfutable de l'identité d'une personne puisqu'elles constituent des caractéristiques biologiques uniques qui distinguent une personne d'une autre et ne peuvent être associées qu'à une seule personne.

¹⁸ Contribution de Gérard Dubey, message sur internet du 22 mars 2005.

¹⁹ Message sur internet du 19 mars 2005.

²⁰ Contribution de Bernard Didier, débat de Paris, 11 avril 2005.

empreintes digitales estimant que cela permettra de résoudre davantage de crimes et délits. De plus, pour Emmanuel-Alain Cabanis²¹, professeur de médecine et président de la Société de Biométrie Humaine, la rencontre entre la biométrie et l'électronique permet paradoxalement de mieux protéger l'identité de l'individu. C'est ce qu'il appelle le « *paradoxe de la liberté* » : le fait de pouvoir être connu, identifié avec certitude permet à un être humain de garantir son identité et ainsi d'être libre car démontrer son unicité, c'est, pour lui, affirmer sa différence vis-à-vis des autres.

L'introduction de la biométrie a fait l'objet d'enquêtes sociologiques. Les sociologues Gérard Dubey²² et Xavier Guchet²³ estiment ainsi, d'après leurs travaux portant sur la biométrie aux Aéroports de Paris et dans des cantines scolaires, que l'introduction de cette technique s'accompagne d'« *une forme d'atonie sociale, une quasi-absence de réaction de la part des usagers vis-à-vis de la mise en place de ces dispositifs* », voire une « *quasi-acceptation* ».

Gérard Dubey explique ceci par le fait qu'il est « *très rare que les usagers sachent comment fonctionnent ces dispositifs et tout aussi rare qu'ils cherchent à le savoir. En fait il n'y a quasiment pas de discours sur ces techniques, de distance critique. Certains évoquent parfois le spectre de Big Brother, d'une tracabilité ou d'un flicage, mais pour la majorité, ces techniques n'évoquent rien de particulier. On évoque parfois leur côté pratique, plus sûr, dans un monde qui est ressenti comme l'étant de moins en moins* ». Cette « *acceptation sociale ne doit pas pour autant dissimuler les contradictions et les tensions qu'elle engendre* ». Il note enfin que l'introduction de la biométrie n'entraîne pas de « *profonds bouleversements* », de changements radicaux et immédiats dans la façon de se représenter l'individu mais ce serait plutôt par une « *analyse minutieuse et patiente des petites peurs, des inquiétudes exprimées par les usagers sur le mode imaginaire, que l'on peut s'approcher des dangers propres à ces dispositifs, de leurs véritables enjeux sociétaux* ». Or, il estime que ceci ne peut se quantifier facilement et mériterait « *d'être approfondi et confirmé par d'autres études* ».

Xavier Guchet²⁴ estime que cette introduction relativement indolore de la biométrie auprès des individus ne signifie pas pour autant que la requalification biométrique de l'identité est sans problème : il reconnaît qu'il est impossible, en l'état, de savoir si la biométrie sera bien acceptée à l'échelle d'une population et recommande à cet effet une analyse précise des usages. Il précise également que la biométrie n'est pas un outil neutre au service de problématiques purement techniques, elle est aussi un instrument de pouvoir car elle s'accompagne de rapports de force et de changements qui modifient la nature même du pouvoir qui s'exerce sur les gens. Ce thème est apparu fortement dans le contexte scolaire où la biométrie inaugure un nouveau type de pouvoir et de contrôle social qui ne passe plus forcément par les surveillants traditionnels mais s'appuie sur d'autres relais.

Le rapport de mars 2005 de la London School of Economics & Political Science²⁵ ainsi que l'étude de la Commission européenne sur les incidences des techniques biométriques d'avril 2005²⁶ confirment cette impression. L'étude de la Commission insiste d'ailleurs sur la nécessité de veiller à faire accepter les applications biométriques par les citoyens, en leur expliquant clairement la finalité et les limites de ces applications.

²¹ Contribution d'Emmanuel-Alain Cabanis, débat de Rennes, 11 mai 2005.

²² Contribution sur internet de Gérard Dubey, 30 mars 2005.

²³ Contributions sur internet de Xavier Guchet, 30 mars 2005 et dans le débat de Marseille du 25 mai 2005.

²⁴ Contribution de Xavier Guchet, débat de Marseille, 25 mai 2005.

²⁵ The Identity Project. An assessment of the UK Identity Cards Bill & its implications, London School of Economics & Political Science, Londres, Mars 2005.

²⁶ Biométrie aux frontières : évaluation des impacts sur la société, étude réalisée par le Centre commun de recherche de la Commission européenne, à la demande de la Commission des libertés et des droits des citoyens, de la justice et des affaires intérieures du Parlement européen, avril 2005.

b) Des débats sur la fiabilité de la biométrie

Quelle fiabilité pour la biométrie ? Pourquoi utiliser l'empreinte digitale plutôt que l'iris de l'œil alors que cette dernière technique semble plus fiable pour certains ? Les questions des internautes s'interrogeant sur les types de biométrie utilisés et leur fiabilité ont été nombreuses. Pingouin se demande ainsi si l'utilisation de l'iris de l'œil ne serait pas plus sûre que le recours à une empreinte digitale. 10cd29 rapporte 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...). 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 Ielou 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. » Certains, lors du débat de Rennes, ont d'ailleurs confirmé ces propos et évoqué l'exemple d'un chercheur japonais qui a fabriqué avec de la gélatine de vraies-fausse empreintes digitales qui ont leurré 11 des 15 systèmes biométriques testés.

Sur ce point, le ministère de l'intérieur a assuré qu'il existe des moyens de se prémunir de ce type de manœuvre par l'acquisition de matériels suffisamment pointus et fiables. En outre, toute utilisation des titres lors des contrôles aux frontières, ou des contrôles d'identité, se fait et demeurera sous le contrôle d'un agent. Le ministère met en avant le facteur humain qui est, à ses yeux, une sécurité supplémentaire contre l'utilisation de fausses empreintes.

c) Des débats sur l'opportunité des biométries choisies

Certains, comme Emmanuel-Alain Cabanis, soulignent que l'on peut éventuellement recueillir des informations médicales à l'occasion d'une identification par l'iris de l'œil (l'iris peut changer de couleur avec l'absorption de certains médicaments) ; cependant, reprenant des chiffres avancés dans le rapport du député Cabal²⁷, il estime que les empreintes sont plus fiables que l'iris.

De l'autre, Bernard Didier²⁸ a précisé que les empreintes bénéficient de plus d'un siècle d'expérience par les pouvoirs publics français en matière de lutte contre la criminalité. Il précise qu'il s'agit d'une technique fiable, maîtrisée et ayant acquis une certaine maturité industrielle. En revanche, il estime que l'iris de l'œil fait l'objet d'une technologie plus jeune sur laquelle on ne dispose pas assez de recul. Il a également précisé²⁹ que la technologie de l'iris « *offre un potentiel plus élevé de détection des fraudeurs (FAR), mais les rejets à tort sont plus importants (...)* Les temps de transaction sont de même très longs car il est procédé à plusieurs tentatives de reconnaissance en cas de rejet. »

²⁷ Christian Cabal est intervenu lors du débat de Lille. Député, il a présenté en juin 2003 un rapport sur la biométrie au sein de l'Office Parlementaire d'Évaluation des Choix Scientifiques et Technologiques. Ce rapport parlementaire précisait que le FAR (« *False Acceptation Rate* », c'est-à-dire le taux qui détermine la probabilité pour un système de « reconnaître » une personne qui normalement n'aurait pas dû être reconnue) est plus fort pour les empreintes digitales (0,008 %) que pour l'iris (0,0001 %). De même, le FRR (« *False Rejection Rate* », le taux qui détermine la probabilité pour un système donné de ne pas « reconnaître » une personne qui normalement aurait dû être reconnue) est plus fort pour les empreintes digitales (2,5 %) que pour l'iris (0,25 %). La reconnaissance faciale est la moins fiable (respectivement 0,45 % pour le FAR et 17 % pour le FRR).

²⁸ Contribution de Bernard Didier, débat de Paris, 11 avril 2005.

²⁹ Message sur internet de Bernard Didier, 31 mai 2005.

d) Des débats sur le marché de la biométrie et le coût de la biométrie associée à la carte à puce

Un certain nombre de personnes ont évoqués des aspects de politique industrielle nationale qui expliqueraient, plutôt que les performances respectives de chaque biométrie, les choix retenus. Par exemple, Yves Bismuth³⁰ a estimé que le choix d'utiliser les empreintes digitales comme élément de biométrie a également été fait pour des raisons économiques parce qu'une entreprise française, Sagem, a une position dominante dans ce domaine et que d'autres choix technologiques (iris de l'œil) dépendent de brevets américains. À cela Bernard Didier a souhaité répondre³¹ que Sagem « ne réduit pas sa position de leader à la seule technologie de l'empreinte digitale. Elle maîtrise depuis plus de deux ans les deux autres technologies de référence que sont la reconnaissance du visage et de l'iris. Cette maîtrise s'est traduite par l'obtention des deux plus importantes références mondiales en la matière. »

Pierre Piazza rappelle³² que certains, comme le député européen danois Ole Sorensen, font valoir que les coûts financiers liés la généralisation des dispositifs biométriques risquent d'être exorbitants au regard des bénéfices que les citoyens pourraient en retirer. Meryem Marzouki estime que le marché de la biométrie et de la carte à puce présente de très forts potentiels économiques et que, de l'avis de tous les acteurs industriels, il est encore seulement en émergence.

Bernard Didier a précisé que le surcoût d'une carte lié à la biométrie représente environ 20 % du coût total. Ceci reviendrait à une estimation de 2 à 4 euros par personne. Hubert Vigneron, président de la section « Carte à puce » du Gixel (Groupement des industries électroniques qui rassemble Axalto, Gemplus, Sagem, Thalès) et Directeur Marketing Stratégique chez Axalto³³ a, quant à lui, annoncé que le marché de la carte à puce dans ses applications d'administration électronique est prometteur puisqu'il est estimé à 60 millions de cartes au niveau mondial en 2005 et plus de 100 millions en 2006 (selon IDC). Cela ne représente toutefois qu'une faible part des cartes à microprocesseur dans le monde (1,7 milliard en 2005 dont 1,2 en téléphonie mobile). Aujourd'hui l'industrie française de la carte fournit 60 à 70 % du marché mondial. À cet effet, Hubert Vigneron estime que l'intérêt des industriels français est de permettre l'émergence de standards internationaux tout en capitalisant sur une implémentation nationale de référence ; c'est pourquoi le Gixel travaille également avec les allemands.

4. – Sur la sécurité du système

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. De façon générale, beaucoup rejoignent l'avis de Sylvain Gombault, enseignant à l'École Nationale Supérieure des Télécommunications de Bretagne et membre du projet SERES (Sécurité des réseaux et des applications réparties) et estiment que « le fait d'utiliser internet comme réseau de transport n'est jamais neutre pour la sécurité d'un système. Il expose les postes clients aux dangers d'internet comme les vers et les virus, et il devient difficile, voire impossible, de garantir un niveau de sécurité de chacun des postes compatible avec la manipulation des données à caractère personnel contenues dans la carte INES. »³⁴

³⁰ Contribution d'Yves Bismuth, débat de Lyon, 31 mars 2005.

³¹ Message sur internet de Bernard Didier, 31 mai 2005.

³² Contribution sur internet de Pierre Piazza, 7 mars 2005.

³³ Contribution de Hubert Vigneron, débat de Lille, 27 avril 2005.

³⁴ Message sur internet de Sylvain Gombault, 7 juin 2005.

a) 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 « *INES présente des garanties suffisantes. Je peux confirmer que du fait de la longueur des clés proposées la carte INES est actuellement inviolable. Il faudra qu'elle le reste et l 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...* » 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 « *États voyous ou certaines multinationales* ».

Cela reflète un constat général : l'échange d'information « sensible » sur un réseau ouvert comme internet est potentiellement dangereux car le risque d'attaques et de failles de sécurité est réel.

b) Sur l'emploi de la carte à puce

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

À ces réserves, il a été répondu que les cartes à puce sont beaucoup plus sécurisées que tout autre support. Olivier Chavrier, Directeur de la division identité et sécurité de Gemplus a rappelé³⁵ qu'un système sécurisé à 100 % n'existe pas. Pour autant, il estime que l'introduction des cartes à puce a renforcé la sécurité. En effet, introduites dans les années 1990 pour le paiement, elles ont permis une diminution de 80 % des fraudes au paiement bancaire alors que, dans le même temps, les volumes de paiement augmentaient de 120 %. De plus, la carte associée à un code PIN permet une sécurité accrue dans l'accès aux données. Dans ce cadre, une carte d'identité électronique fondée sur une carte à puce et de la signature électronique permettra une authentification sécurisée sur le net. Enfin, si l'on veut davantage de garanties sur la sécurité d'un système, il convient que celui-ci fasse l'objet d'une évaluation par des laboratoires indépendants puis de certification par un autre organisme.

c) Des propositions pour améliorer la sécurité du système

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)* ».

Pour l'internaute toto37 : « *il pourrait être envisagé de former un groupe d'experts, reconnus et mandatés par les différentes parties prenantes pour valider cette*

³⁵ Contribution d'Olivier Chavrier, débat de Marseille, 25 mai 2005.

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

Enfin, faisant écho aux débats intervenus sur le thème de la vie privée (possibilité de lecture à l'insu du porteur), 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* ». Beretta, comme bien d'autres, 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).* »

d) La faille de sécurité au niveau de l'état civil

Le projet INES prévoit que la procédure de délivrance des titres soit sécurisée, en amont, par la mise en œuvre d'un processus d'échange direct des données d'état civil entre services source (la mairie de naissance) et services chargés de la délivrance des titres. Les citoyens n'auraient donc plus à prendre contact avec leur mairie de naissance pour obtenir un extrait de naissance mais l'échange d'information se ferait directement entre les mairies concernées. Pour ce faire, un projet, conduit par le ministère de la justice, prévoit de dématérialiser les actes de l'état civil afin de mettre en œuvre un système d'échange d'informations entre services. Le déploiement des deux projets doit contribuer à conférer une sécurisation supplémentaire aux documents d'identité délivrés.

Cependant, certains ont noté, notamment lors des débats de Lyon et de Paris, que le projet de carte nationale d'identité électronique ne semble pas s'articuler avec celui de dématérialisation de l'état-civil ; qu'il est donc un peu illusoire de renforcer la sécurisation des titres si, dans le même temps, les données d'état-civil sur lesquels ils se fondent, ne sont pas entièrement fiables ; qu'à ce titre, il risque d'y avoir des failles de sécurité.

5. – Sur les usages

a) Un intérêt très limité pour l'aspect « portfolio personnel »

L'aspect portfolio personnel consiste à permettre aux titulaires, s'ils le souhaitent, de stocker, à titre personnel, des informations complémentaires dans la carte. Ceci pourrait permettre, par exemple, de remplir plus facilement des formulaires à partir d'informations que l'on porterait toujours sur soi (ex : permis de conduire, numéro fiscal, etc.). Il ressort du débat que cette fonctionnalité de la carte n'intéresse pas les intervenants même si son aspect « *espace mémoire* » serait une « *avancée intéressante* » pour l'AMGVF³⁶.

b) Des confusions et des incompréhensions

Un certain nombre de confusions ou d'incompréhensions ont pu être notées. Ainsi, certains ont eu peur que toutes les actions de la vie courantes apparaissent (« *liste des habitudes de consommation* ») ou que la CNIE ne soit une carte de paiement. Beaucoup ont pensé également que la CNIE accueillerait les données de santé, voire serait fusionnée avec la carte Vitale. Sur ce point, le ministère de l'intérieur a régulièrement

³⁶ Message sur internet de l'Association des Maires de Grandes Villes de France, 18 mai 2005.

répondu que les données de santé et à caractère sanitaire et social ne seront pas dans la CNIE, qu'une telle disposition serait, en tout état de cause, inconstitutionnelle.

c) Peu d'intérêt voire des interrogations quant aux fonctionnalités internet de la carte (certificat et signature électronique)

Le ministère de l'intérieur, dans son dossier de présentation du projet INES, précise que la CNIE pourra donner accès à des téléprocédures administratives et permettra de s'identifier de façon certifiée sur internet auprès de sites marchands³⁷.

Certains ont été intéressés par les nouveaux services qu'offre la carte. L'internaute RC note que « la CNIE offre beaucoup d'avantages : elle remplace les certificats électroniques qui sont nécessaires à la réalisation des formalités administratives comme TELETVA (et qui coûtent 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 qu'elle 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-à-dire nous) de faciliter les démarches administratives » (vicoleboss).

Cependant, de façon générale, l'intérêt pour les téléprocédures administratives est limité. De plus, les internautes Franchick ou Necronick estiment que certains actes citoyens, comme la possibilité de voter électroniquement par le biais de la CNIE, ne doivent pas être rendus possibles du fait des risques : risques d'attaques contre le système, atteinte à la confidentialité du vote, usurpation d'identité...

De plus, certains ont fait part de leurs inquiétudes sur le fait que la carte permette d'authentifier un accès, voire de signer électroniquement, auprès de sites marchands. 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. Cyril Rojinsky³⁸, avocat, estime ainsi qu'il convient d'insister sur le fait qu'un « titre national d'identité, électronique ou non (...) matérialise, signe pour ainsi dire l'identité strictement légale de chacun. Sous prétexte de simplification, de réduction du nombre de cartes dont nous pouvons disposer, le projet d'une carte unique intégrant des applications commerciales viendrait pervertir le rôle même de l'État à cet égard ». Pour d'autres, comme l'association IRIS³⁹, la CNIE ne doit pouvoir faire l'objet d'aucune autre utilisation. Les certificats de signature électronique et autres utilisations individuelles doivent être complètement dissociés de la carte, de son support et de sa gestion.

D'autres, comme l'avocat Thierry Piette-Coudol⁴⁰, se demandent : « Quel besoin d'une identification forte pour les téléprocédures ? D'autant que l'anonymat de l'agent public correspondant pourrait, lui, être respecté, "si des motifs intéressant la sécurité publique ou la sécurité des personnes le justifient" (art. 4 de la loi n°2000-321 du 12 avril 2000 relative aux droits des citoyens dans leurs relations avec les administrations). » Il se demande également : « Pourquoi une "identification certifiée" (...) pour une transaction électronique privée ? En somme, si le commerce repose depuis l'antiquité sur la confiance, le commerce électronique devrait-il reposer sur l'authentification forte et les mesures biométriques ? »

³⁷ Dossier de présentation du ministère de l'intérieur du 1^{er} mars 2005 : le bloc « identification certifiée » permettrait d'accéder à des téléprocédures publiques ou privées via un code PIN et « le bloc "signature électronique" de signer électroniquement des documents authentiques, soit à l'intention d'une e-administration, soit pour toute transaction électronique privée ».

³⁸ Contribution sur internet de Cyril Rojinsky, 7 mars 2005.

³⁹ Contribution de Meryem Marzouki, débat de Lille, 27 avril 2005.

⁴⁰ Contribution sur internet de Thierry Piette-Coudol, 7 mars 2005.

Daniel Kaplan, délégué général de la Fondation Internet Nouvelle Génération (FING)⁴¹ estime également que le développement d'une carte « signeuse » est potentiellement dangereux. En effet, parce que la CNIE bénéficiera d'un statut officiel et qu'elle proposera un dispositif très fort d'authentification, elle risque d'inciter un grand nombre d'acteurs à se reposer sur elle pour leurs relations avec des tiers (clients, fournisseurs...) même si ce niveau d'authentification n'est pas nécessaire.

D'une manière générale, la plupart des intervenants ont souhaité une variabilité de l'authentification en fonction de l'usage.

d) Quelques questions sur le contexte européen

Le contexte européen a fait l'objet de peu de questions. Les questions ont principalement porté sur l'interopérabilité (la carte sera-t-elle « lisible » à l'étranger ?) et l'articulation entre le projet français et ceux de nos voisins européens. À cet effet, Michel Elie⁴² souhaite une généralisation la carte « à l'espace européen » et que la carte devienne « un document d'identité unique applicable au moins à toute personne résidant en Europe communautaire ». Dans cet esprit, certains se sont demandé quel est l'intérêt de développer une carte nationale dans un contexte européen et s'il ne fallait pas mieux concentrer ses efforts sur un projet de carte d'identité électronique européenne. À leurs yeux, le projet devrait avoir une portée européenne car désormais les décisions sont prises au niveau européen (passeport biométrique et Règlement de décembre 2004, titres de séjours et visas biométriques). Les problématiques posées se retrouvant dans les autres États membres, l'internaute 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 ? »).

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

6. – Sur les mesures d'accompagnement

a) Le coût

Pour de nombreux intervenants, le projet de CNIE va coûter cher. Ils se demandent concrètement combien va coûter le projet dans son ensemble ; l'annonce faite par le Ministre de dépenser 205 millions d'euros par an en a choqué certains « en ces périodes de restrictions budgétaires » ; mais ils se demandent aussi qui va payer la carte : la collectivité ou l'individu lui-même.

À cet égard, les contributions rappellent que l'actuel CNI papier est gratuite, la rendre payante serait mal perçue, les nouveaux services proposés ne le justifiant pas. D'une façon générale, le souhait se porte sur la gratuité de la carte (important en termes d'acceptation et d'insertion surtout pour les catégories défavorisées). Si elle devait être payante, l'internaute Julesandolfi suggère qu'elle ne le soit que « pour les personnes imposables sur les revenus ». 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'État et les impôts ». 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 rétinienne 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. Lors du débat de Bordeaux, Patrick Nouvel⁴³, Directeur commercial domaine identitaire de Thalès, a précisé que si la carte proposait des services associés, le secteur privé y

⁴¹ Contribution de Daniel Kaplan, débat de Marseille, 25 mai 2005.

⁴² Message sur internet de Michel Elie, 8 avril 2005.

⁴³ Contribution de Patrick Nouvel, débat de Bordeaux, 8 mars 2005.

trouverait une source de revenus et, de ce fait, pourrait prendre en charge une partie des coûts.

D'autres intervenants seraient favorables au paiement de la carte en cas de renouvellement de papier ou de perte. Christian Cabal⁴⁴ a d'ailleurs estimé, en tant que parlementaire, qu'il serait intéressant de songer à ne rendre la carte payante que dans ces deux situations.

À l'idée de savoir combien coûtera au final une CNIE pour l'utilisateur, Hubert Vigneron précise⁴⁵ que le prix d'une carte dépend de nombreux facteurs et que les prix annoncés englobent souvent plusieurs éléments (le prix de fabrication de la carte, le coût de son émission, et le coût du système – ou son amortissement). Dans les projets traités par Axalto, la partie carte représentait de 30 à 50 % du total du projet. Il a précisé que les cartes actuellement développées coûtent entre 10 € en Belgique (proche du prix de revient car le prix de revient d'une carte est toujours à un chiffre) et 35 £ au Royaume-Uni en passant par des coûts moyens (Italie : 25 à 30 €). Hubert Vigneron a enfin précisé que la carte d'identité électronique en Finlande coûte 40 € mais que, du fait de son caractère non obligatoire, elle ne se vend pas et se développe peu.

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

b) Le caractère obligatoire

Ce point a fait débat : certains ont annoncé que si la carte n'est pas obligatoire elle ne sera jamais adoptée largement (cf. Finlande carte de 40 euros pas obligatoire) et dès lors ne servira pas. À cet effet, il est intéressant de voir les résultats du sondage : à la question « *quelles opinions se rapprochent le plus de la vôtre ? La future carte d'identité électronique devrait être obligatoire car cela garantit une réelle diminution des fraudes ou facultative comme c'est le cas actuellement de la carte d'identité ?* », 69 % des sondés répondent que c'est « *une bonne chose car cela permettra de lutter plus efficacement contre les fraudes* ». 30 % estiment que « *c'est une mauvaise chose car cela constitue une atteinte à la liberté individuelle* ».

Il a été rappelé que le projet INES rend obligatoire la détention d'une CNIE mais conserve la liberté du mode de preuve⁴⁶. Il a aussi été remarqué que, même si le fait de porter une CNIE en permanence sur soi ne pourra être imposé, on ne pourra plus se prévaloir de ne pas avoir une carte d'identité.

De plus, beaucoup craignent que la carte ne devienne à terme obligatoire dans les faits pour la plupart des échanges avec l'administration, voire avec le secteur privé. En effet, comme le précise Thierry Piette-Coudol⁴⁷, avocat, « *la facilité de pouvoir utiliser le certificat embarqué dans la carte pourrait entraîner une utilisation systématique apportant ainsi aux relations électroniques un niveau d'authentification qui n'est pas nécessairement demandé par le Droit* ». Ce faisant, un tel niveau d'authentification

⁴⁴ Contribution de Christian Cabal, débat de Lille, 27 avril 2005.

⁴⁵ Contribution d'Hubert Vigneron, débat de Lille 27 avril 2005.

⁴⁶ L'article 78-2 du Code de procédure pénale, qui dispose que l'on peut « *justifier, par tout moyen, de son identité* », s'appliquera toujours.

⁴⁷ Contribution sur internet de Thierry Piette-Coudol, 1^{er} mars 2005.

risque, dans les faits, d'entraîner une forme de pression sociale. Cette préoccupation est très présente dans les débats. De même, Annie Blandin, maître de conférences à École Nationale Supérieure des Télécommunications de Bretagne⁴⁸, rappelle que l'identification de haut niveau fournie par l'État risque d'être utilisée à tout propos sous la pression éventuelle de destinataires imposant le recours aux certificats de la CNIE. Ces craintes font logiquement écho à celles exprimées dans la partie 5. c selon lesquelles la carte pourrait devenir un standard quasi obligatoire pour tous les usages de la vie quotidienne.

D'une manière plus générale, la grande majorité des intervenants aux débats se sont opposés très clairement au caractère obligatoire de la carte. Ils estiment qu'il y a là non seulement un risque de fracture technologique (ceux qui ne savent pas se servir des usages) mais surtout une rupture avec la « tradition » républicaine française. En effet, comme le rappelle Pierre Piazza⁴⁹, le principe du caractère facultatif de la carte a été affirmé sous la Troisième République, réaffirmé à la Libération et jamais remis en cause par les différents gouvernements successifs, jusqu'à nos jours.

Enfin, le ministère de l'intérieur a précisé que la carte sera obligatoire à partir de la majorité, soit à l'âge de 18 ans (pour rappel, la carte d'identité électronique sera obligatoire en Belgique à partir de 12 ans).

c) Le lieu et le mode de délivrance

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

Sur ce point, les avis ont été partagés. Jean Péringuey⁵⁰, en tant que président d'une communauté de communes où les mairies ont 400 habitants en moyenne a rappelé que les citoyens sont très attachés à une carte nationale d'identité électronique délivrée dans un service de proximité et il estime que la mise en place de la CNIE ne doit pas diminuer l'offre de services publics locaux. Pour beaucoup de maires ruraux, la délivrance d'une carte nationale d'identité est souvent le moyen d'entretenir des liens avec leurs administrés. À cet égard, de nombreuses réserves ont été exprimées sur le fait, qu'en milieu rural, la carte soit délivrée par le biais d'une borne itinérante (station d'acquisition) allant dans chaque mairie.

Alain Risson⁵¹, en tant que responsable du groupe de travail « Nouvelles technologies » de l'Association des maires de France, a exprimé ses craintes quant à l'apparition de « *supers mairies* » seules à même de pouvoir délivrer les cartes. Il se demande si le plus simple ne serait pas que le nombre de « *super-mairies* » soit « *ramené, pour des raisons purement financières, à quelques centaines, ces super-mairies pouvant être alors parfaitement suppléées par les sous-préfectures qui sont au nombre de quelques centaines aussi...* »⁵².

⁴⁸ Contribution d'Annie Blandin, débat de Rennes, 11 mai 2005.

⁴⁹ Message sur internet de Pierre Piazza du 13 avril 2005.

⁵⁰ Contribution de Jean Péringuey, débat de Bordeaux, 8 mars 2005.

⁵¹ Contribution d'Alain Risson, débat de Lyon, 31 mars 2005.

⁵² Message sur internet d'Alain Risson, du 18 avril 2005.

L'Association des Maires des Grandes Villes de France⁵³ s'interroge finalement sur le rôle de la mairie dans la chaîne de traitement des CNIE et à l'étendue de ses responsabilités : « *Les mairies auront-elles la possibilité ou le devoir de demander des pièces justificatives supplémentaires en cas de dossiers litigieux ; aura-t-elle le rôle que joue la préfecture actuellement ? Le contentieux administratif ne risque-t-il de s'accroître pour les villes ?* ». L'AMGVF se demande également ce qu'il est prévu en termes organisationnels pour « *l'adaptation des locaux pour garantir la confidentialité des opérations, l'organisation de l'attente (...) la formation du personnel...* ».

Un point plus ponctuel a été discuté : celui des photographies d'état-civil. Les nouvelles modalités de photographie (il est prévu que l'utilisateur n'amène plus de photos d'identité, celles-ci seront prises sur place par les agents équipés en matériel de photographie numérique) posent problème à l'Association pour la Promotion de l'Image⁵⁴. Tout en proposant un système qui permettrait de numériser les photos remises par les usagers (photos réalisées par des professionnels), cette association estime que le système proposé dans le cadre d'INES est « *contraignant pour l'utilisateur* » (« *absence de liberté de choix de leur photo d'identité et de choix du prestataire réalisant leur photo d'identité* »), « *contraignant pour l'administration* » (« *La prise de photo d'identité est une activité professionnelle à part entière, qui suppose une expérience et une formation spécifiques* ») et « *lourd et complexe* » (« *Les communes les plus importantes devront recourir à des compétences externes en engageant des formateurs ou des professionnels, et les plus petites communes ne pourront disposer des compétences spécifiques ou des moyens d'engager des formateurs sur ce système* »).

B. – Sur les questions plus générales

1. – La place de l'identité

Le projet INES prévoit la création, par l'État, d'une identité nationale électronique sécurisée ; ce faisant il fait également évoluer les relations des citoyens avec le concept même d'identité. Le débat a donc tourné autour du postulat suivant : comment trouver un juste équilibre entre d'un côté « *la légitimité dans une démocratie de disposer d'un moyen de s'assurer de façon aussi sûre que possible de l'identité des personnes* »⁵⁵ et de l'autre le droit à l'anonymat. De manière générale, les participants au débat se sont demandé dans quelle mesure on doit protéger davantage son identité à l'heure du numérique.

a) La carte nationale d'identité électronique permettra utilement de sécuriser l'identité

Les débats ont régulièrement rappelé que cette volonté de sécuriser l'identité s'inscrit également dans un contexte actuel de fraude et d'usurpation à l'identité sur les réseaux. L'avocat Thierry Wickers⁵⁶ a rappelé qu'une entreprise américaine (ChoicePoint) s'est récemment fait voler 145 000 « identités » (numéros de sécurité sociale, permis de conduire...) de clients dont elle avait la charge. Les débats en ligne ont rappelé l'affaire de « phishing »⁵⁷ de mai 2005 où des banques françaises furent victimes de cette escroquerie ; à cette occasion le ministère de l'intérieur a d'ailleurs estimé que si les internautes utilisaient leur CNIE pour se connecter à leur banque, cette technique de

⁵³ Message sur internet de l'Association des Maires des Grandes Villes de France, 18 mai 2005.

⁵⁴ Message sur internet de l'Association pour la Promotion de l'Image, 15 mars 2005.

⁵⁵ Contribution de Michel Elie, message sur internet du 8 avril 2005.

⁵⁶ Contribution de Thierry Wickers, débat de Bordeaux, 8 mars 2005.

⁵⁷ Contraction des termes anglais *ishing* (« pêche ») et *phreaking* (« piratage des lignes téléphoniques ») : escroquerie qui consiste à envoyer un courriel usurpant une identité pour obtenir des données personnelles. Le 27 mai 2005, quatre banques françaises ont été victimes de ce type de fraude : un courriel usurpant leur identité demandait au client de se connecter vers un faux site bancaire afin d'obtenir de ce dernier des données confidentielles (codes d'accès, numéro de compte).

fraude disparaîtrait. C'est pourquoi certains, comme Emmanuel-Alain Cabanis⁵⁸, ont pu dire que le recours à l'électronique protège notre identité en faisant en sorte qu'on ne la confonde pas avec celle de notre voisin ou celle d'un usurpateur intentionnel (cf. le « *paradoxe de la liberté* » évoqué partie 3.a.).

b) Quelle gestion de l'identité à l'heure du numérique ?

Face à ces changements, il a souvent été rappelé dans les débats que la gestion de l'identité à l'ère du numérique doit être observée avec la plus grande prudence. Yves Bismuth⁵⁹ estime ainsi, en tant qu'avocat, que la loi pourrait instaurer un « *Habeas Data* » qui protégerait officiellement les droits du citoyen à l'ère du numérique et notamment son identité.

Daniel Kaplan, quant à lui, note⁶⁰ que les relations humaines reposent depuis toujours sur une part de confiance souvent prépondérante. Dans certains cas, le fait de ne pas exiger de preuve d'identité peut même constituer le ciment d'une relation forte et durable, le signe d'une confiance réciproque. Si le recours a priori commode à la CNIE contribue à faire basculer ces relations de l'informel au formel, de la confiance à la sécurité, cela peut avoir des conséquences sur les relations sociales. Trop sécuriser une relation enlève paradoxalement de la confiance.

C'est ce que confirme et développe Gérard Dubey⁶¹ qui remarque que « *la notion même d'identité numérique doit être au cœur de toute réflexion sur la biométrie. Ces techniques sont censées donner plus de confort aux usagers, protéger contre la fraude et faciliter les contrôles. On insiste moins sur le fait qu'elles vont se traduire, comme tout processus d'automatisation, par la suppression de médiations sociales ou humaines. Or, on le sait, la disparition progressive de la présence humaine renforce le sentiment d'insécurité. Ce qui est fragilisé, plus profondément, ce sont les rapports de confiance sans lesquels il n'existe pas de société.* » À ses yeux la question est donc « *de savoir ce que signifie et ce que change le fait de déléguer à des automatismes le soin de définir l'identité, à commencer par sa traduction en langage numérique* ». Il note enfin que « *l'intolérance contemporaine à la fraude, à l'erreur, au risque de falsification (...) ne doit pas faire oublier qu'il n'y a d'identité réelle que sociale, sujette au changement, et la définition de l'identité civile n'échappe pas à cette règle. L'identité comporte nécessairement des marges d'incertitude ou d'indétermination qui constituent autant de sources d'erreurs potentielles et d'occasions de fraude. À moins d'en livrer une image extrêmement dégradée ou appauvrie, l'identité civile ne recouvre donc jamais l'identité réelle, mais doit au contraire refléter en partie cette indétermination* ».

De plus, beaucoup se sont demandé dans quelle mesure la volonté de certifier l'identité ne va pas à l'encontre du droit à l'anonymat. À cet égard, Bruno Villalba⁶², maître de conférences à Lille II, a rappelé que l'anonymat est un droit et qu'un espace où il n'y a plus d'anonymat possible est un lieu où il n'y a plus d'espace privé. De même, Jean-Jacques Lavenue⁶³, professeur de droit à Lille II, estime qu'avec la mise en place d'une identité certifiée apparaît le risque que le bénéfice de l'anonymat, le droit à l'oubli, voire à la dissimulation, disparaissent. Il insiste sur la nécessité de veiller à ce que la sécurité ne devienne pas une idéologie et à cet égard rappelle les propos de Benjamin Franklin : « *Quiconque est disposé à abandonner une partie de sa liberté au nom d'une prétendue sécurité, ne mérite ni l'une ni l'autre.* »

⁵⁸ Contribution d'Emmanuel-Alain Cabanis, débat de Rennes, 11 mai 2005.

⁵⁹ Contribution d'Yves Bismuth, débat de Lyon, 31 mars 2005.

⁶⁰ Contribution de Daniel Kaplan, débat de Marseille, 25 mai 2005.

⁶¹ Contribution de Gérard Dubey, message sur internet du 22 mars 2005.

⁶² Débat de Lille, 27 avril 2005.

⁶³ Contribution de Jean-Jacques Lavenue, débat de Lille, 27 avril 2005.

Arnaud Belleil⁶⁴, du groupe « Identité Numérique » de la FING, propose une « option » pour concilier sécurité de l'identité et protection de l'anonymat qui serait de faire en sorte que la CNIE « ne soit pas systématiquement une carte d'identité mais, pour certains usages, uniquement une carte d'habilitation. On pourrait imaginer bien des cas de figure où le porteur de la carte aurait juste besoin de prouver qu'il est majeur, qu'il est de nationalité française, qu'il possède des droits (...) ou qu'il n'est pas déchu de certains droits (...) sans avoir pour autant à justifier de son identité. »

2. – Le rôle et la responsabilité de l'État

a) Quelle responsabilité pour l'État certificateur ?

Dans le cas où l'État remplit le rôle d'autorité de certification, beaucoup se sont demandé, à l'instar d'Annie Blandin⁶⁵ ou d'Éric Caprioli⁶⁶, dans quelle mesure il sera responsable de la fiabilité du procédé. Pour ce dernier, l'État sera responsable de la fiabilité du procédé de signature électronique (outil de signature et certificat). Il estime de plus que l'on pourrait limiter la valeur d'usage du certificat : pour toute transaction au-delà d'une certaine somme le certificat ne serait plus valable. La responsabilité de l'État ne serait ainsi engagée que dans le cadre de cette somme (transaction de 10.000 euros par exemple).

D'autres ont estimé que la responsabilité de l'État ne doit être liée qu'à la délivrance des certificats et pour une durée limitée.

D'autres encore proposent que l'État développe une politique de certification dans laquelle sa responsabilité serait décrite exhaustivement.

b) L'intervention de l'État dans la sphère marchande

Certains se demandent dans quelle mesure cette mainmise de l'État sur l'activité de certification ne va pas nuire à un marché privé qui a déjà du mal à décoller ou si, au contraire, c'est le seul moyen d'instaurer la confiance dans ce domaine.

Pour certains, l'État, qui serait son propre certificateur, entrerait en concurrence avec des prestataires de services de certification (PSC). Et il disposerait d'un avantage en termes de moyens et de confiance. Annie Blandin⁶⁷ estime ainsi que le risque n'est pas nul de voir émerger un monopole de la certification qui fausserait la concurrence sur ce marché. Elle note qu'avec cette intervention directe « *ès qualité sur le marché dit de la confiance, on est ici à contre-courant de la tendance actuelle qui consiste à exclure un nombre croissant d'activités du champ de la sphère publique lorsqu'elles sont de nature économique* ». À l'inverse, des internautes comme Beretta notent que « *l'État 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* ».

Au contraire, d'autres craignent que si l'État n'investit pas dès maintenant dans le domaine de la certification, il devra acheter au prix fort des certificats aux entreprises privées spécialisées, voire laisser l'offre de certificats venir uniquement du secteur privé. À ce titre, Martial Gabillard⁶⁸ estime que si l'État ne développe pas une offre dans le domaine de l'administration électronique et des certificats, le secteur privé risque de s'emparer de ce domaine. Il précise que le secteur de l'administration en ligne doit rester le fait de la puissance publique afin d'éviter une privatisation rampante des services qu'offre l'État et une remise en cause consécutive des exigences de service public.

⁶⁴ Contribution d'Arnaud Belleil, message sur internet du 3 mars 2005.

⁶⁵ Contribution d'Annie Blandin, débat de Rennes, 11 mai 2005.

⁶⁶ Contribution d'Éric Caprioli, débat de Marseille, 25 mai 2005.

⁶⁷ Contribution d'Annie Blandin, débat de Rennes, 11 mai 2005.

⁶⁸ Contribution de Martial Gabillard, débat de Rennes, 11 mai 2005.

3. – Le principe de précaution en matière de nouvelles technologies

Un grand nombre de participants aux débats ont souhaité que soit menée une réflexion sur le principe de précaution appliqué aux technologies de l'information et de la communication. Ces technologies devraient pouvoir faire l'objet d'actions de prévention pour faire face à des risques éventuels de dérives dans leur utilisation, à l'instar de ce qui a été mis en place pour l'environnement.

4. – La fracture numérique

Sur ce point trois remarques principales ont été énoncées lors des débats.

Tout d'abord, avant de développer, voire de généraliser, une carte nationale d'identité électronique, certains rappellent qu'il convient de prendre en compte le 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.).

Ensuite, d'autres rappellent le risque de « fracture territoriale » entre les territoires desservis par l'internet haut débit et les autres mais surtout entre ceux qui bénéficieront de lieux de délivrance et ceux qui n'auront la carte que par le biais de stations d'acquisition mobiles. Il y a là, pour beaucoup, un risque de rupture dans le fonctionnement des services publics locaux.

Enfin, dans le cas où la CNIE serait obligatoire et payante, des risques de « fracture sociétale » entre ceux qui auront les moyens financiers et les autres sont soulignés. De façon générale, et comme cela a été rappelé par l'internaute danyd44, il y a une crainte de la marginalisation de ceux qui sont les « *ni-ni (ni urbains, ni jeunes)* » et de « *déshumanisation* » des relations avec l'administration.

II. ANALYSE CRITIQUE DU PROCESSUS DU DÉBAT

Organiser un débat public n'est pas une chose nouvelle en France. En effet, il existe la Commission Nationale du Débat Public⁶⁹ qui est chargée d'organiser un débat public sur les objectifs et caractéristiques principales des grandes opérations d'aménagement ou d'équipement d'intérêt national. De plus, de nombreuses consultations publiques (par exemple, actuellement est menée une « Consultation publique sur le service public des communications électroniques ») ou consultations nationales sont régulièrement mises en place (cf. sur la laïcité, sur l'école etc.). De même sur internet, le Gouvernement avait mis en place en 1999 une « Consultation publique sur l'adaptation du cadre législatif de la société de l'information » préparant la Loi sur la Société de l'Information. Depuis, il existe www.forum.gouv.fr, espace de discussion proposé par le gouvernement sur des sujets de société (réforme de l'état et service public, avenir de l'Europe, famille...).

Cependant, le Forum des droits sur l'internet a souhaité mettre en place une forme de débat à la fois innovante et complémentaire.

Innovante tout d'abord dans les modalités de la consultation publique. Le Forum des droits sur l'internet a souhaité conjuguer différentes façons de consulter les Français et de toucher divers types de population. Les débats en ligne et en régions, la mobilisation des experts, l'organisation du sondage ont permis de cerner au plus près les attentes des français.

Innovante surtout du fait du positionnement du Forum des droits sur l'internet. Il ne s'agit en effet pas d'une consultation organisée par les pouvoirs publics eux-mêmes au soutien d'un projet mais d'un processus plus neutre mis en œuvre par un organisme situé à la confluence des pouvoirs publics, des entreprises et des utilisateurs. Le but du Forum est de recueillir l'avis des français, leurs interrogations et propositions ; il est aussi d'animer un processus interactif entre les français et le ministère qui conduit celui-ci à expliquer, clarifier, identifier les points de blocage, le cas échéant, à modifier son projet. Le projet INES a ainsi été questionné, débattu et amendé avant même sa présentation en Conseil des ministres et auprès des institutions compétentes (CNIL, Conseil d'État, Parlement...).

Le débat public mis en œuvre par le Forum n'est donc pas une photographie de l'avis des français sur le projet mais une dynamique aidant à la prise de décision.

Innovante enfin par rapport aux autres pays. Très peu ont mené des consultations avant de mettre en œuvre une CNIE et aucun n'a organisé de débat similaire au nôtre. Deux pays ont néanmoins mené quelques consultations : le Canada et le Royaume-Uni.

Ainsi, au Canada, le « débat » autour d'un projet de CNIE s'est matérialisé par un colloque de deux jours précédé d'un sondage, le tout organisé par le Gouvernement sans véritable débat contradictoire. Le ministère fédéral de la citoyenneté et de l'immigration a envisagé de rendre obligatoire une carte d'identité avec indications biométriques mais n'a pas encore statué sur l'émission d'un tel document. Auparavant, ce ministère avait organisé un forum de deux jours sur le sujet (« *Biométrie, incidences et applications pour*

⁶⁹ La loi du 2 février 1995 relative à la protection de l'environnement, dite loi « Barnier », crée la Commission Nationale du Débat Public (CNDP). La loi du 27 février 2002 relative à la démocratie de proximité transforme la CNDP en une autorité administrative indépendante, garante du débat public, élargit son domaine de compétence et diversifie ses modes d'intervention : elle impose que les projets importants soient connus du public et confirme le principe que la CNDP organise un débat public sur l'opportunité, les objectifs et caractéristiques principales des grandes opérations d'aménagement d'intérêt national de l'État, des collectivités territoriales, des établissements publics et des personnes privées.

la citoyenneté et l'immigration », les 7 et 8 octobre 2003 à Ottawa). Avant que ne s'ouvre ce forum, un sondage avait été réalisé. Il portait sur l'éventuelle instauration d'une carte nationale d'identité électronique. À la question « *compte tenu, d'une part des avantages possibles au niveau de la sécurité, d'autre part du risque possible pour la liberté, est-ce une bonne idée d'introduire une carte nationale d'identité électronique ?* » 57 % des canadiens ont répondu positivement et 30 % négativement. Il ressort du sondage que la majorité des Canadiens estiment que l'utilisation frauduleuse de documents d'identification constitue un problème. Ils sont favorables au recours à la biométrie et à la mise au point d'une nouvelle carte d'identité mais dans l'optique où celle-ci serait délivrée de manière facultative. Les préoccupations portent principalement sur le respect de la vie privée, le coût élevé de la mise en œuvre, la capacité des criminels à contrer la technologie ou encore la possibilité que le gouvernement utilise abusivement ces renseignements personnels.

Au Royaume-Uni, le « débat » a également été mené uniquement par le Gouvernement par le biais d'auditions, de consultations et de sondage. Mais il a été souvent reproché à Tony Blair de ne pas avoir organisé de véritable débat national indépendant pouvant apporter la contradiction (seuls les experts ont véritablement été consultés). Ainsi, en juillet 2002, le Gouvernement a lancé une consultation sur la fraude à l'identité (jusqu'en janvier 2003). Un résumé a été rendu public le 11 novembre 2003, date à laquelle le projet pour une carte d'identité électronique a été annoncé. D'avril à juillet 2004, le Gouvernement a lancé un « *consultation paper* » (« *Legislation on Identity Cards – A consultation* ») auprès de nombreux organismes, syndicats etc. Sur les 5000 personnes et organisations qui ont répondu, 4200 se sont réellement exprimées. 60 % d'entre elles se sont prononcées pour l'instauration d'une carte nationale d'identité électronique. De plus, un sondage a été commandé : il indique que 80 % de la population est favorable à la CNIE mais seulement 50 % se déclare prêt à payer pour en disposer. Enfin, un site d'information a été ouvert sur le site du Home Office (<http://www.homeoffice.gov.uk/comrace/identitycards>). Parallèlement, et devant l'absence de véritable débat sur un sujet aussi fondamental, une forte campagne a été lancée contre le projet : 5000 courriels ont été envoyés contre l'instauration d'une carte nationale d'identité électronique (sur identitycards@homeoffice.gsi.gov.uk) et l'opposition s'est fédérée autour de www.no2id.net et www.privacyinternational.org. Le projet de loi devrait être adopté prochainement, la carte serait alors déployée progressivement dès 2008 puis à terme rendue obligatoire.

En outre, la démarche du Forum des droits sur l'internet est complémentaire de celle que mènent d'autres instances. Ainsi la Commission Nationale de l'Informatique et des Libertés rendra son avis en temps voulu sur le projet de loi, après avoir mené ses travaux d'expertise. De même, la commission des bis du Sénat a mis en place une « mission d'information sur la nouvelle génération de documents d'identité et la fraude documentaire » en février 2005 ; elle devrait rendre prochainement ses travaux. Les conclusions du débat public peuvent aider ces instances dans leurs travaux, bien qu'elles poursuivent des objectifs différents.

Ces deux caractéristiques du débat public organisé par le Forum étant soulignées, deux questions légitimes peuvent être posées quant au processus engagé :

- Le débat est-il efficient, c'est-à-dire, a-t-il été suivi d'effet ?
- Le débat public est-il fiable, c'est-à-dire, ses conclusions sont-elles dignes de foi ?

A. – Le débat est-il efficient ?

1. – Le débat en chiffres

Le débat sur internet a reçu 3060 contributions soit plus de 50 % des taux de fréquentation habituels des forums en ligne de ce type. Le débat en régions a compté une présence moyenne de 100 personnes par débat dans six villes avec une présence allant de 70 personnes à Bordeaux à 205 à Paris, soit plus de 600 personnes en régions.

Le Forum des droits sur l'internet a également souhaité faire intervenir des experts à même d'éclairer le grand public et d'alimenter ainsi le débat par leurs connaissances et leurs réflexions sur le sujet. Des avocats, des chercheurs, des universitaires, des sociologues, des représentants de la société civile travaillant sur les notions d'identité numériques sont ainsi intervenus, soit sur le forum de discussion, soit lors de manifestations en régions. Ces contributions ont fait l'objet de nombreux commentaires de la part des internautes et de discussions en régions. Cinquante experts ont ainsi participé au débat (liste complète des experts en annexe).

2. – Une fonction d'alerte sur un sujet sensible

Le débat a permis de faire connaître aux Français le projet INES et les nombreux changements qu'il allait apporter dans la vie de tous les jours, de questionner utilement le ministère de l'intérieur et de proposer des recommandations qui viendront nourrir la réflexion gouvernementale et les débats parlementaires qui auront lieu par la suite.

Le débat a ainsi eu le mérite d'alerter l'opinion sur ce sujet. Le projet de carte nationale d'identité électronique a d'ailleurs progressivement été l'objet de prises de position de la part de nombreuses associations dont c'est naturellement le rôle. Ainsi, la Ligue des Droits de l'Homme, le Syndicat de la magistrature, le Syndicat des avocats de France), l'association IRIS (Imaginons un réseau Internet solidaire), l'intercollectif DELIS (Droits et libertés face à l'informatisation de la société) et l'Association française des juristes démocrates ont, le 26 mai, rendu public une pétition exigeant le retrait total et immédiat du projet INES. De son côté, le collectif « Souriez vous êtes filmés » a envoyé, le 21 mai 2005, une « *Lettre ouverte aux maires de France. Exprimez votre désaccord sur le projet de carte d'identité électronique à votre maire* ». Les syndicats CGT, CFDT, SUD, CGT-FO, CGC, CFTC de l'INSEE ont rédigé, le 9 mai 2005, une « *Lettre ouverte au Directeur général de l'Insee : l'Insee n'a pas vocation à être une annexe du ministère de l'intérieur !* ». L'association des Maires des Grandes Villes de France a envoyé un message sur le fond du projet le 12 mai 2005 et de nombreux autres organismes ou associations se sont exprimés par la suite.

Ces prises de position se sont d'ailleurs souvent faites dans le débat en ligne ou en régions, soit directement (« Souriez vous êtes filmés », lettre ouverte des syndicats nationaux de l'Insee, AMGVF, AMF, FING, APRIL, Club de l'Hyper-République, FNTC, Association photographes...), soit indirectement par le biais d'alertes des internautes ou de communications en régions (pétition de la LDH, SM, SAF, IRIS, DELIS et AFJD).

3. – L'impact du débat sur le projet de carte nationale d'identité électronique

Ce débat a-t-il eu un impact sur le projet de carte nationale d'identité électronique ? Dans quelle mesure le ministère de l'intérieur va-t-il en tenir compte ? Ce débat n'est-il pas en fait qu'un prétexte, pour les pouvoirs publics, d'obtenir un assentiment populaire avant la mise en place de la CNIE ? Quelle est la crédibilité pour ce débat alors que le ministre de l'intérieur a rendu public ses orientations et que le projet a reçu l'aval du Premier ministre avant même la fin des débats ? Toutes ces questions ont été régulièrement posées lors des débats.

D'autres personnes ont également regretté que le processus de débat ne soit pas suffisamment connu et que, pour un débat de portée nationale, 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 le débat n'ait été qu'une « *pseudo-consultation* ».

Le Forum des droits sur l'internet reconnaît qu'aucun moyen ne lui a été alloué pour faire connaître le débat auprès du grand public ; il s'en est d'ailleurs régulièrement plaint auprès du ministère.

En revanche, il a pu être constaté que les débats en région ont toujours bénéficié d'une très large couverture presse : le sujet, quand il est connu, intéresse !

En outre, c'est dans le débat que le ministère de l'intérieur a choisi de préciser divers éléments du projet, comme l'accès indirect à la base, les modes de lecture des données sur la carte, les modes de délivrance... C'est aussi au cours du débat que le ministère a reconnu les insuffisances dans le projet ou les points qui méritaient réflexion : l'absence de chiffres sur la fraude à l'identité, l'articulation avec le projet de dématérialisation de l'état-civil, le manque de lien entre les projets passeport et CNIE... Le processus de débat a donc, dans sa fonction clarificatrice, eu des impacts.

Il a même, dans quatre cas, conduit à des changements concrets du projet CNIE :

1) L'aspect portfolio enlevé

Le ministère proposait un bloc « *portfolio personnel* »: cette fonction optionnelle devait permettre de stocker des informations complémentaires dans la carte, soit pour faciliter des transactions électroniques (par exemple stocker de manière « exportable » nom, prénom et adresse pour remplir des formulaires), soit pour remplacer d'autres papiers (ex : numéro de permis de conduire, numéro fiscal, etc). Les gens ont montré dans le débat soit une opposition, soit peu d'intérêt. Au cours du débat, le ministère de l'intérieur a annoncé son souhait de retirer cette fonctionnalité du projet.

2) Le « sans contact » reconsidéré et plus sécurisé

Les nombreux débats sur le « sans contact » ont montré qu'il est impératif pour le ministère de fournir des preuves sur la sécurité de cette fonctionnalité avant de valider son utilisation. Dans les débats en région le ministère a précisé que tous les États s'interrogent sur la possibilité d'utiliser cette technologie et a reconnu qu'elle ne serait introduite en France pour la carte nationale d'identité électronique que si les études montrent qu'il n'y a pas de risque de capture des informations à l'insu du porteur, et selon les normes qui permettront de s'en assurer. Dans le débat en ligne, de nombreuses propositions ont été faites (cage de Faraday/étui métallique) et reconnues utiles par le ministre de l'intérieur, qui va reconsidérer cet aspect du système.

3) Une proposition de schéma alternatif prise en considération par le ministère.

Aux propositions concernant une gestion différente de la base d'empreintes, le ministère a estimé possible de suivre l'une d'entre elle (décrite dans le rapport par les internautes Alice et Zorclub42...) tout en précisant que ce choix était lié à la finalité même du projet.

4) Introduction de mesures de traçabilité de consultation des données de la carte.

Le ministère a souhaité étudier les suggestions issues du débat sur le traçage des contrôles de carte pour éviter les abus, que ce soit par une « boîte noire » dans le lecteur, ou par inscription dans la puce. Le ministère a également pris en considération la possibilité pour le citoyen de vérifier sur un serveur l'habilitation des personnes l'ayant contrôlé.

B. – Le débat public est-il fiable ?

Le débat a rassemblé un grand nombre de personnes : plus de 600 présentes en régions, plus de 3 000 contributions sur internet. À titre d'exemple, le sujet qui a connu le plus de succès sur le site institutionnel <http://www.forum.gouv.fr> (« Réforme de l'État : Quel service public pour demain ? ») a reçu 1908 contributions. Les citoyens ont entendu parler de l'existence du débat par la presse qui en a fait un large écho, ou par les moyens d'information mis en place par le Forum, relayés par les pouvoirs publics (site du Premier ministre, de l'ADAE, de la CNIL...) et l'univers associatif, qui s'est progressivement mobilisé sur ces enjeux.

De plus, les contributions reçues furent de qualité. En effet, il semble que l'on ait souvent eu affaire à des « citoyens-experts » car les personnes « contributrices » se sont avérées être bien informées, alertées quant aux enjeux du projet de CNIE et posant des questions pertinentes. Les échanges qui sont intervenus étaient le plus souvent de haute qualité. Cependant, des propos erronés, voire des rumeurs, ont parfois pu être présents (le fait que la carte puisse être lue à plusieurs centaines de mètres, l'existence prochaine d'une puce sous cutanée...). Il se dégage une grande homogénéité entre les réactions/contributions dans les débats en ligne et celles qui se sont exprimées en régions. Beaucoup de propositions concrètes ont pu être faites. Certaines sont d'ailleurs reprises dans le présent rapport. De plus, les « experts » qui se sont exprimés ont apporté de nouveaux éléments et ont utilement éclairé le projet dans le domaine qui est le leur. Enfin, de nombreux organismes et associations sont intervenus directement dans le débat en ligne ou en régions (cf. LDH, IRIS, AMGVF, FING, APRIL, FNTC...), permettant d'analyser certains points du projet au regard de leurs préoccupations spécifiques.

Enfin, le fait d'avoir mené des débats et commandé un sondage a permis de combiner divers outils en associant une approche à la fois qualitative et quantitative du sujet. Ce faisant, le Forum a obtenu des résultats larges et complets sur l'état de l'opinion. En effet, les appréciations qualitatives apportées par les débats en ligne ou en régions (public averti, contributeurs parfois revendicatifs, débats de qualité...) ont été complétées par les résultats quantitatifs d'un sondage (appréciation neutre d'un échantillon représentatif de la population, soit 950 personnes a priori moins sensibilisées à ces questions).

À ce titre on peut donc estimer que le débat public est fiable et a couvert, par une approche plurielle, un large éventail d'opinions.

III. ANALYSE ET RECOMMANDATIONS DU FORUM DES DROITS SUR L'INTERNET

Compte tenu des enseignements du débat en ligne et en région mais également des indications du sondage, le Forum des droits sur l'internet formule aux pouvoirs publics les analyses et recommandations suivantes.

À titre liminaire, on constate deux choses :

D'une part, que ce **débat sur la carte d'identité électronique est un débat qui intéresse les Français** : ils se sont mobilisés tout au long du débat public et, au vu du sondage, sont peu à ne pas avoir d'opinion sur ce sujet majeur.

D'autre part, en raison de l'impératif de sécurité, le sondage montre que les Français sont, pour les trois quarts, favorables au projet de carte d'identité électronique⁷⁰.

Cependant, en contrepoint à cette tonalité globalement positive, les débats en ligne et en région ont fait remonter des réticences très fortes sur certains aspects du projet. Le gouvernement et le Parlement devront répondre à celles-ci s'ils souhaitent poursuivre le déploiement du projet dans un climat de consensus. Les propositions ci-après ont l'objectif d'y contribuer.

A. – Les enjeux de sécurité sont essentiels aux yeux des Français mais les arguments avancés à l'appui du projet n'ont pas convaincu

Si le sondage IPSOS et le débat public, dans une certaine mesure, ont montré que les Français sont sensibles aux enjeux liés à la sécurisation de leur identité, le débat a aussi montré que les arguments avancés par le ministère de l'intérieur justifiant le projet INES n'ont pas véritablement convaincu. Les raisons sont apparues minces, voire inadaptées, la plupart du temps mal comprises. En particulier la fraude à l'identité, présentée comme un argument majeur n'a pas pu être clairement chiffrée et le lien avec le projet de passeport électronique est apparu artificiel et même contre-productif.

1. – Des études sur la fraude à l'identité

Il semble difficile d'envisager un tel projet sans avoir de données chiffrées sur la fraude à l'identité en France.

Le Forum des droits sur l'internet recommande que soit réalisée une étude rigoureuse visant à mesurer l'ampleur réelle de la fraude à l'identité en France.

2. – Un découplage avec le projet passeport

Le débat a montré que si la France est tenue par les dispositions européennes visant à adopter un passeport biométrique dans un bref délai, ces textes et l'urgence de transposition qui leur est liée, ne s'appliquent pas à la carte d'identité nationale.

⁷⁰ Il est intéressant de rapprocher ce résultat de celui, quasiment similaire, d'un autre sondage réalisé en août 2002 par la SOFRES pour le Forum des droits sur l'internet sur une question très proche : « *Seriez-vous favorable ou opposé à ce que l'État délivre aux personnes qui en font la demande une carte d'identité électronique sécurisée (carte à puce) qui pourrait leur servir dans l'accomplissement de toutes leurs démarches administratives sur Internet (identification, signature, paiement en ligne) ?* » 73 % des sondés avaient répondu favorablement, 25 % négativement. Le sondage est disponible sur : <http://www.foruminternet.org/telechargement/documents/sdq-admelec-res-020924.pdf>

En outre, le couplage des deux procédures a donné l'impression que la France, sur un domaine régalien, subissait des pressions étrangères (européennes et surtout américaines).

Au regard des enjeux et de l'impact du projet INES, le Forum des droits sur l'internet **recommande que sa mise en œuvre ne soit pas couplée avec le projet passeport.**

B. – La protection de la vie privée est une préoccupation majeure à laquelle le projet doit apporter des garanties complémentaires

Une majorité des contributions enregistrées au cours du débat public concernent la protection de la vie privée. Au-delà du débat théorique sur le changement de société que susciterait la CNIE, elles s'inquiètent tant des dérives éventuelles dans l'utilisation de la base centrale par l'administration que d'un rapprochement entre fichiers publics et privés. Concernant la base centrale, de nombreux débats ont porté sur sa finalité précise. Des internautes ont estimé que si le projet se limitait à lutter contre la fraude à l'identité (gérer la fraude au renouvellement et assurer une délivrance sans doublon de cartes), un autre scénario de base, plus protecteur en termes de protection des données, serait alors possible (voir partie 2. a. 1. du rapport).

De façon générale, la relative incompréhension des objectifs du projet conduit à renforcer la sensibilité des individus sur les aspects liés à la protection de leur vie privée.

1. – Un nouveau pacte social doit être conclu entre l'État et le citoyen

Le projet de CNIE est l'occasion pour l'État de préciser les relations qu'il souhaite entretenir avec le citoyen dans un contexte de déploiement de l'administration électronique. À un contrôle accru des titres et de l'identité individuelle doit correspondre une possibilité accrue de maîtrise par le citoyen des données qui le concernent dans les téléprocédures administratives. Cette réciprocité est un gage d'équilibre et de confiance.

Dans la mesure où la carte nationale d'identité électronique donne accès à des téléprocédures administratives, le Forum des droits sur l'internet **recommande que le citoyen ait un accès en ligne, gratuit et permanent, à ses dossiers administratifs et au suivi de l'état d'avancement de sa démarche.**

2. – Il convient de porter une attention particulière sur la mise en place d'un identifiant unique

Le projet INES prévoit que la CNIE permettrait de conjuguer, sur un support unique, des finalités différentes comme le contrôle d'identité et l'accès à des téléprocédures administratives. Ceci pourrait conduire à ce que les individus soient identifiés de façon unique et centralisée quel que soit l'usage. Cette perspective d'identifiant unique serait un changement significatif avec le principe de pluralité des identifiants sur lequel l'administration électronique s'est fondée jusqu'à présent.

Le Forum des droits sur l'internet **appelle l'attention des pouvoirs publics sur la cohérence entre l'identification unique et centralisée, telle que prévue dans le projet INES, et le principe de pluralité des identifiants utilisé actuellement dans le cadre de l'administration électronique.**

3. – Le projet de carte nationale d'identité électronique doit faire l'objet d'un contrôle global et permanent.

Face aux enjeux du projet de CNIE, face aux craintes liées à la protection de la vie privée et de l'introduction de la biométrie et aux doutes quant à la sécurité du système, un contrôle fort et effectif a été souhaité. Ce contrôle devra non seulement s'effectuer en amont du déploiement de la carte (études...) mais aussi de façon continue pour prévenir d'éventuelles dérives (un élargissement de l'accès de la base à d'autres agents ou des usages de la base au-delà de ceux initialement prévus...).

Le Forum des droits sur l'internet estime fondamental que l'aspect contrôle soit étudié et mis en œuvre en même temps que le déploiement du projet. À cet effet, le Forum **recommande un contrôle global et permanent du système sous la responsabilité de la CNIL**⁷¹. Pour ce faire, cette institution devra disposer de moyens juridiques et financiers nécessaires pour contrôler, de façon effective, le dispositif. Il conviendra notamment de voir dans quelle mesure l'actuelle loi Informatique et Libertés permet d'assurer de telles missions. Une partie du financement du programme de la carte nationale d'identité électronique pourrait être affectée à cette fonction de contrôle.

C. – Des incertitudes à lever en termes de sécurité

De nombreux intervenants ont noté que, si le projet INES allait sans nul doute renforcer la sécurité des titres d'identité, celle-ci devait être étudiée de façon globale, à tous les stades d'élaboration et d'usage de la carte. En particulier, en amont, l'articulation du projet avec la gestion de l'état-civil est apparue critique, tout comme en aval, les aspects « sans contact » de la carte (risque de lecture à l'insu du porteur) et les usages sur internet (réseau ouvert sujet à de nombreuses attaques et failles de sécurité).

1. – Une évaluation de l'aspect lecture « sans contact » de la carte

Les nombreux échanges sur le « sans contact » ont montré qu'il est impératif de fournir des preuves de la sécurité de ce canal avant de pouvoir valider son utilisation.

L'aspect « sans contact » de la carte ayant fait l'objet de nombreuses craintes, **le Forum des droits sur l'internet recommande que cette technologie ne soit introduite en France pour la carte nationale d'identité électronique que si les études montrent qu'il n'y a pas de risque de capture des informations à l'insu du porteur, et selon les normes qui permettront de s'en assurer.**

⁷¹ Le contrôle devra répondre aux objectifs suivants :

1) En amont du déploiement du projet de carte d'identité électronique :

- Réaliser une expertise sur l'architecture du système dans le domaine de la sécurité informatique.
- Mener une étude sur l'acceptabilité de la biométrie afin de connaître, à une grande échelle, l'appropriation individuelle qui sera faite de cette technique.
- Mener des études sur l'impact du projet sur la vie privée (*les pouvoirs publics pourraient prendre exemple sur les procédures d'évaluation de la conformité d'un projet ou d'une technologie aux exigences générales de protection de la vie privée mises en place au Canada dans le cadre du « Personal Information Protection and Electronic Documents Acts ».* Cette « démarche d'évaluation d'impact sur la vie privée » permet d'identifier les risques d'atteinte à la vie privée des projets gouvernementaux et privés, de traiter les non conformités etc. Ces éléments sont ensuite présentés aux autorités décisionnaires et au public).

2) À partir de la mise en œuvre d'une carte d'identité électronique :

- Contrôler de façon permanente le fonctionnement de la base, les agents qui y ont accès et les motifs d'accès ainsi que le journal des consultations. Ceci pour permettre la rectification des informations et prévenir toute évolution possible de l'usage de la base.
 - Recevoir les réclamations des particuliers.
 - Assurer une évaluation permanente du système sous tous ses aspects (sécurité, protection des données, sociologique, financier) ainsi qu'une veille juridique, scientifique et technologique.
 - Rendre compte de son activité par le biais de la publication d'un rapport spécifique qui devra notamment se préoccuper des évolutions constatées et des incidences des mesures prises et envisagées.
- Pour remplir cette mission nouvelle La CNIL pourrait associer, dans un souci d'adjonction des compétences, des représentants de la société civile et du secteur privé.

2. – L'articulation entre le projet INES et celui de dématérialisation de l'état-civil

Le projet INES prévoit que la procédure de délivrance des titres soit sécurisée en amont par la mise en œuvre d'un processus d'échange direct des données d'état-civil entre mairie de naissance et mairie de délivrance des titres. La conjugaison de ces deux démarches devrait contribuer à conférer une sécurisation supplémentaire aux documents d'identité. Pour ce faire, un projet, conduit par le ministère de la justice, prévoit de dématérialiser les actes de l'état civil.

À cet égard, certains ont noté qu'à ce jour il semble que le projet de CNIE ne s'articule pas avec celui de dématérialisation de l'état-civil, chaque ministère ayant son propre calendrier. Or, il apparaît que sans une informatisation concomitante de l'état-civil, le projet de CNIE risque d'avoir des failles de sécurité.

Le Forum des droits sur l'internet, regrettant le manque de coordination entre les projets du ministère de la justice et de l'intérieur, **recommande que la délivrance d'une carte nationale d'identité électronique ne soit mise en place que lorsque l'informatisation de l'état-civil sera achevée, sinon la délivrance des cartes risque d'avoir des failles de sécurité.**

D. – Une attente mitigée par rapport à une carte de services

1. – Un faible intérêt pour une CNIE utilisable pour les téléprocédures administratives

Même si certains participants au débat, et notamment des représentants de collectivités locales, ont exprimé leur intérêt pour une carte combinant des fonctions d'identification et d'accès à des téléprocédures administratives, les réactions ont majoritairement montré un faible intérêt pour cette orientation.

Il conviendra, si cette orientation devait être confirmée, de mener une campagne énergique d'explication, soulignant l'articulation de la carte nationale d'identité électronique avec les cartes locales déjà existantes ou en projet.

2. – Une réticence assez forte pour une carte « signeuse » pour les échanges marchands

Si le projet INES n'est pas entièrement clair sur la possibilité d'utiliser ou non les certificats de la carte sur des sites marchands, une relativement forte opposition s'est dégagée sur cette idée qui conduit à combiner, sur un même support, des usages régaliens et marchands.

E. – Des réticences sur le caractère payant et obligatoire de la carte nationale d'identité électronique

1. – La carte doit être gratuite à la première délivrance

Dans le cas où le Parlement décide de rendre la carte nationale d'identité électronique payante, le Forum des droits sur l'internet **recommande qu'elle soit gratuite à la première délivrance mais payante en cas de perte ou de renouvellement.**

2. – Un débat devant le Parlement sur le caractère obligatoire

Ce point a fait débat : certains ont annoncé que si la carte n'est pas obligatoire elle ne sera jamais adoptée largement et ne servirait pas dans les faits ; le sondage semble confirmer cette opinion. Cependant, la très grande majorité des intervenants au débat se sont opposés au caractère obligatoire estimant que celui-ci serait une rupture avec une tradition républicaine.

Le Forum des droits sur l'internet **recommande au Parlement d'étudier l'éventualité du caractère obligatoire de la carte avec la plus grande attention. L'hypothèse d'une carte nationale d'identité électronique obligatoire représenterait, dans l'esprit des traditions républicaines d'un pays comme la France, un changement de première importance.**

F. – La sensibilité de l'enjeu territorial

Le projet prévoit, en raison du coût, mais aussi pour des raisons de sécurité et de charge de travail pour les petites collectivités, de concentrer l'émission et la délivrance de la nouvelle carte sur quelques centaines de mairies. Cette décision suscite beaucoup de controverses, tant auprès des collectivités locales qui veulent toutes garder le lien privilégié avec les citoyens que constitue la délivrance de la carte, qu'auprès des individus très attachés à une offre de service public répartie sur l'ensemble du territoire.

À cet égard, la solution d'une borne itinérante (station d'acquisition) allant dans chaque commune rurale n'apparaît pas comme une véritable réponse.

De plus, des problèmes de formation des agents municipaux, d'équipements des mairies en matériels ou encore organisationnels (l'adaptation des locaux pour garantir la confidentialité des opérations, l'organisation de l'attente etc.) se posent.

Compte tenu des enjeux liés à l'aménagement du territoire, le Forum des droits sur l'internet estime que **la délivrance en mairie de la carte nationale d'identité électronique mérite une large concertation avec les élus et leurs représentants** afin que puisse être trouvée une solution de consensus.

G. – Le contexte européen

La carte nationale d'identité est reconnue comme document de voyage dans un certain nombre de pays (les pays membres de l'Union Européenne mais aussi l'Islande, la Norvège, ou encore la Suisse et la Turquie). Le projet doit permettre à la carte nationale d'identité électronique de pouvoir être acceptée par ces pays.

Le Forum des droits sur l'internet **insiste sur le fait que la CNIE devra impérativement être acceptée dans tous les pays où elle sert déjà de document de voyage. Pour ce faire, des travaux d'harmonisation avec les normes et standards adoptés en la matière et d'interopérabilité avec les autres pays devront être menés.**

Conclusion

Le projet de CNIE est un projet majeur qui peut modifier la vie des français et le rapport qu'ils entretiennent avec l'État. Malgré leur forte sensibilité aux enjeux de sécurité qui conduit plus des trois-quarts d'entre eux à se déclarer favorables au projet de carte nationale d'identité électronique, le débat public a mis en lumière de fortes réticences sur certains points. Dès lors, le ministère doit revoir le projet afin de répondre à celles-ci s'il souhaite poursuivre son déploiement dans un climat de consensus.

| |
|----------------|
| ANNEXES |
|----------------|

- Lettre de mission
- Liste des experts intervenus aux débats en ligne et en région
- Liens vers les comptes rendus des débats en régions et en ligne et les contributions des experts en ligne
- Sondage commandé par le Forum des droits sur l'internet

LETTRE DE MISSION



MINISTÈRE DE L'INTÉRIEUR,
DE LA SÉCURITÉ INTÉRIEURE ET DES LIBERTÉS LOCALES

LE MINISTRE

Paris, le – 6 JAN. 2005

Madame la Présidente,

Le programme INES a été élaboré pour apporter aux citoyens à la fois plus de sécurité et plus de facilités dans leurs relations avec l'administration :

- plus de sécurité, face à la fraude documentaire qui prend des proportions croissantes (immigration illégale, fraude aux prestations sociales, escroqueries diverses), et dont le coût pour la Nation tout entière devient alarmant ; et face au terrorisme qui profite des lacunes des systèmes actuels pour se jouer des contrôles.
- plus de facilités, en réformant et en unifiant les procédures actuelles de demandes de titres, et en proposant d'autres usages nécessaires à la vie quotidienne des Français.

Ce programme doit également respecter des contraintes internationales concernant l'introduction, dans un délai court, de la biométrie dans les titres de voyage.

.../...

Madame Isabelle FALQUE-PIERROTIN
Présidente du Forum des droits sur l'internet
6, rue Déodat de Séverac
75017 PARIS

Des interrogations légitimes peuvent naître dans l'opinion publique sur un tel projet. Aussi, compte tenu de ces éléments, je souhaiterais que vous puissiez organiser un débat public sur l'ensemble de ces enjeux, afin d'informer l'opinion sur ce dossier et de recueillir les avis et les propositions des citoyens.

Ce débat se déroulerait sous deux formes :

- d'une part, un débat en ligne avec modérateur, ouvert sur le site internet du Forum des droits sur l'internet ;
- et d'autre part, des débats régionaux grand public dans plusieurs villes de France.

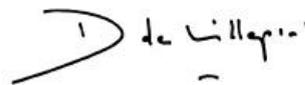
La période 1^{er} février – 30 avril 2005 paraîtrait la plus favorable.

Si cette coopération rencontre votre adhésion, le ministère de l'intérieur de la sécurité intérieure et des libertés locales se chargerait de l'annonce publique dans le cadre de son point de presse. Les préfetures de région assureraient l'organisation matérielle des débats en région, et le ministère prendrait en charge les frais de déplacement. Un agent du programme INES coopérerait avec le Forum pour la modération et l'animation conjointes du débat en ligne.

La direction de programme INES fixera avec vous les modalités pratiques de préparation et de lancement de ce débat, et notamment le choix des sujets à aborder et leur traitement.

Je tiens à vous remercier tout particulièrement de cette opération conjointe entre le Forum et le Ministère.

Je vous prie d'agréer, Madame la Présidente, l'expression de mes sentiments les meilleurs.



Dominique de VILLEPIN

| |
|--|
| EXPERTS INTERVENUS AUX DÉBATS EN LIGNE ET EN RÉGION |
|--|

Cinquante experts sont intervenus dans le débat en ligne ou en régions :

Contribution de l'**Association des Maires de Grandes Villes de France**

Contribution de l'**Association pour la Promotion et la Recherche en Informatique Libre (APRIL)**

Thierry **AUTRET**, Expert Sécurité, Groupement des Cartes Bancaires

Arnaud **BELLEIL**, Directeur Associé de Cecurity.com et Co-animateur du groupe « Identité Numérique » de la Fondation Internet Nouvelle Génération (Fing).

Yves **BISMUTH**, Avocat, Président d'honneur de l'Association Française du Droit de l'Informatique et de la Télécommunication

Annie **BLANDIN**, maître de conférences à École Nationale Supérieure des Télécommunications de Bretagne

Christian **CABAL**, Député et auteur d'un rapport sur la biométrie au sein de l'Office Parlementaire d'Évaluation des Choix Scientifiques et Technologiques

Emmanuel-Alain **CABANIS**, Professeur de médecine et Président de la société de Biométrie Humaine

Éric **CAPRIOLI**, Avocat et membre de la délégation française auprès des Nations Unies sur les questions de commerce électronique

Olivier **CHAVRIER**, Directeur de la division identité et sécurité, Gemplus

Simon **CHIGNARD**, Vice-Président de l'association multimédia BUG

Contribution du **Club de l'Hyper République**

Alain **DAMASIO**, écrivain

Claudine **DARDY**, Professeur de sociologie à l'Université Paris XII

Marcel **DESVERGNES**, Président d'Aquitaine Europe Communication

Bernard **DIDIER**, Directeur développement des affaires, division sécurité Sagem

Gérard **DUBEY**, sociologue à l'Institut National des Télécoms, chercheur au CETCOPRA (Centre d'étude des techniques, des connaissances et des pratiques)

Youval **ECHED**, Secrétaire Général de l'Académie Internationale des Droits de l'Homme, Administrateur et Trésorier de L'Association Française du Net

Bernard **FITOUSSI**, Préfet, Directeur du Programme INES, ministère de l'intérieur

Patrice **FLICHY**, Professeur de sociologie à l'Université de Marne-la-Vallée

François **GIQUEL**, Vice-Président de la Commission Nationale de l'Informatique et des Libertés

Martial **GABILLARD**, Président de l'Association des villes et collectivités pour les communications électroniques et l'audiovisuel (AVICCA)

Sylvain **GOMBAULT**, Enseignant/Chercheur à l'École Nationale Supérieure des Télécoms de Bretagne, Membre du projet SERES (Sécurité des réseaux et des applications réparties)

Xavier **GUCHET**, philosophe, chercheur au CETCOPRA (Centre d'étude des techniques, des connaissances et des pratiques), Université de Paris I

Claudine **GUERRIER**, Enseignant chercheur à l'Institut National des Télécoms

Olivier **ITÉANU**, Avocat à la Cour d'Appel de Paris

Christophe **JOLIVET**, membre du bureau du Club de la Sécurité des Systèmes d'Information Français

Vania **JOLOBOFF**, Silicomp – AQL, société d'ingénierie en informatique

Daniel **KAPLAN**, délégué général, Fondation Internet Nouvelle Génération.

Marie-Laure **LAFFAIRE**, Avocat à la Cour d'Appel de Paris

Frédéric **LAGANDRÉ**, Responsable du Pôle technique, Direction de la Sûreté, Aéroports de Paris

Amar **LAKEL**, Chercheur associé, Université de Paris X, Nanterre

Thomas **LAMARCHE**, enseignant chercheur à l'université Lille III

Jean-Jacques **LAVENUE**, Professeur de droit, Université Lille II

Meryem **MARZOUKI**, Présidente de l'association IRIS (Imaginons un Réseau Internet Solidaire) et chercheuse au CNRS

Patrick **NOUVEL**, Directeur commercial domaine identitaire Thales Security System

Contribution de l'**Observatoire des Usages de l'Internet (OUI)**

Jean **PÉRINGUEY**, Président de la communauté de commune de Villandraut et maire de Noaillan

Pierre **PIAZZA**, chargé de recherche à Institut National des Hautes Études de Sécurité

Thierry **PIETTE-COUDOL**, Avocat près la cour d'appel de Paris

Gilbert **PUECH**, Président de l'Université de Lyon II

Philippe **RIGAUT**, sociologue, enseignant à l'université de Picardie - Jules Verne

Alain **RISSON**, maire de Gluiras et responsable du groupe de travail « Nouvelles technologies » de l'Association des Maires de France

Cyril **ROJINSKY**, Avocat au barreau de Paris

Pierre **TRUDEL**, Professeur à l'Université de Montréal, Canada

Michel **TUBIANA**, Président de la Ligue des Droits de l'Homme

Hubert **VIGNERON**, Président de la section « carte à puce » du Gixel (Groupement des industries électroniques) et Directeur Marketing Stratégique, Axalto

André **VITALIS**, Directeur du Centre d'Étude des médias Université Michel de Montaigne Bordeaux III

Gérard **WEISZ**, Secrétaire général de la Fédération Nationale des Tiers de Confiance

Thierry **WICKERS**, Avocat, Président de la Conférence des Bâtonniers

| |
|---|
| COMPTES RENDUS DES DÉBATS EN RÉGIONS ET EN LIGNE ET LES CONTRIBUTIONS DES EXPERTS EN LIGNE |
|---|

Les débats en ligne ont été animés par :

Jean Gonié, Juriste, le Forum des droits sur l'internet

Fabrice Mattatia, Ingénieur en chef des Télécommunications, Direction de programme INES (Identité Nationale Électronique Sécurisée), ministère de l'intérieur

Sophie Planté, Adjointe au Directeur, Direction de programme INES (Identité Nationale Électronique Sécurisée), ministère de l'intérieur

Yann Tésar, Modérateur, Le Forum des droits sur l'internet

Les débats en régions ont été animés par :

Jean Gonié, Juriste, le Forum des droits sur l'internet.

La Direction de programme INES (Identité Nationale Électronique Sécurisée) du ministère de l'intérieur a été représentée dans les débats par Bernard Fitoussi, Préfet, Directeur du Programme INES et Sophie Planté, adjointe au directeur.

1. – Liens vers les comptes rendus des débats itinérants

Bordeaux (8 mars 2005) :

<http://www.foruminternet.org/telechargement/forum/cpte-rendu-bordeaux-20050308.pdf>

Lyon (31 mars 2005) :

<http://www.foruminternet.org/telechargement/forum/cpte-rendu-lyon-20050331.pdf>

Paris (11 avril 2005) :

<http://www.foruminternet.org/telechargement/forum/cpte-rendu-paris-20050411.pdf>

Lille (27 avril 2005) :

<http://www.foruminternet.org/telechargement/forum/cpte-rendu-lille-20050427.pdf>

Rennes (11 mai 2005)

<http://www.foruminternet.org/telechargement/forum/cpte-rendu-rennes-20050511.pdf>

Marseille (25 mai 2005) :

<http://www.foruminternet.org/telechargement/forum/cpte-rendu-marseille-20050525.pdf>

Synthèse générale :

<http://www.foruminternet.org/telechargement/forum/cpte-rendu-debats-itinerants.pdf>

2. – Liens vers les comptes rendus des débats en ligne (du 1er février au 7 juin 2005)

Synthèse de la première semaine de débats – 8 février 2005 :

<http://www.foruminternet.org/telechargement/forum/cnie-enligne-synthese1.pdf>

À propos de la lecture « sans contact » de la carte et la création d'une base d'empreintes digitales numérisées – 24 février 2005 :

<http://www.foruminternet.org/telechargement/forum/cnie-enligne-synthese2.pdf>

Deuxième synthèse des contributions des internautes du 8 février au 29 mars 2005 :

<http://www.foruminternet.org/telechargement/forum/cnie-enligne-synthese3.pdf>

Synthèse des contributions des internautes sur le thème « biométrie » du 29 mars 2005

<http://www.foruminternet.org/telechargement/forum/cnie-enligne-synthese4.pdf>

Synthèse des contributions des internautes sur le thème « vie privée » du 22 avril 2005

<http://www.foruminternet.org/telechargement/forum/cnie-enligne-synthese5.pdf>

Synthèse des contributions des internautes sur le thème « sécurité » du 27 mai 2005

<http://www.foruminternet.org/telechargement/forum/cnie-enligne-synthese6.pdf>

Réponses du ministère de l'intérieur sur le thème « biométrie » - 30 mars 2005

http://www.foruminternet.org/telechargement/forum/cnie-enligne-synthese4_rm.pdf

Réponses du ministère de l'intérieur sur le thème « vie privée » - 25 avril 2005

http://www.foruminternet.org/telechargement/forum/cnie-enligne-synthese5_rm.pdf

Réponses du ministère de l'intérieur sur le thème « sécurité » - 1^{er} juin 2005

http://www.foruminternet.org/telechargement/forum/cnie-enligne-synthese6_rm.pdf

Synthèse générale :

http://www.foruminternet.org/telechargement/forum/syntheses_cnie.pdf

3. – Liens vers les contributions des experts en ligne

Les contributions des experts ayant contribué en ligne :

<http://www.foruminternet.org/telechargement/forum/avis-specialistes-cnie.pdf>

LE SONDAGE IPSOS/FORUM DES DROITS SUR L'INTERNET

20 et 21 mai 2005

FICHE TECHNIQUE

SONDAGE EFFECTUE POUR : le Forum des droits sur l'internet.

DATES DU TERRAIN : les 20 et 21 mai 2005.

ECHANTILLON : 950 personnes, constituant un échantillon national représentatif de la population française âgée de 18 ans et plus.

MÉTHODE : échantillon interrogé par téléphone. Méthode des quotas : sexe, âge, profession du chef de famille, catégorie d'agglomération et région.

RÉSULTATS

1/ Opinion à l'égard de la carte d'identité électronique

Question : dans le cadre de la lutte contre la fraude à l'identité, le ministère de l'intérieur envisage de remplacer la carte d'identité actuelle par une carte d'identité électronique comportant des données personnelles numérisées telles que empreintes digitales, photographie, voire iris de l'oeil. Personnellement, êtes vous très favorable, plutôt favorable, plutôt défavorable ou très défavorable à la mise en place de cette nouvelle carte d'identité ?

Base : à tous

| | <i>Pourcentage (%)</i> |
|------------------------|------------------------|
| • Très favorable | 30 |
| • Plutôt favorable | 44 |
| S/T Favorable | 74 |
| • Plutôt défavorable | 14 |
| • Très défavorable | 11 |
| S/T Défavorable | 25 |
| • Ne se prononce pas | 1 |

2/ Opinion à l'égard de la constitution d'un fichier informatique national des empreintes digitales

Question : pour mettre en oeuvre cette mesure, le ministère de l'intérieur prévoit de constituer un fichier informatique national des empreintes digitales. Laquelle de ces deux opinions se rapproche le plus de la vôtre ? Constituer un fichier informatique national des empreintes digitales...

Base : à tous

| | <i>Pourcentage (%)</i> |
|--|------------------------|
| • Est une mauvaise chose car cela constitue une atteinte à la liberté individuelle | 23 |
| • Est une bonne chose car cela permettra de lutter plus efficacement contre les fraudes à l'identité | 75 |
| • Ne se prononce pas | 2 |
| Total | 100 |

3/ Opinion à l'égard du caractère obligatoire de la future carte

Question : laquelle de ces deux opinions se rapproche le plus de la vôtre ? La future carte d'identité électronique devrait être...

Base : à tous

| | <i>Pourcentage (%)</i> |
|--|------------------------|
| • Obligatoire car cela garantit une réelle diminution des fraudes | 69 |
| • Facultative comme c'est le cas actuellement de la carte d'identité | 30 |
| • Ne se prononce pas | 1 |
| Total | 100 |