La carte nationale d'identité électronique (CNIE)

Bienvenue à Gattaca

Introduction

En 2003, une loi a généralisé le recours aux techniques biométriques pour renforcer les procédures de vérification des identités des ressortissants étrangers lors de la délivrance des visas et lors du contrôle aux frontières. Au plan européen, des initiatives ont été prises pour introduire la biométrie dans les visas, les titres de séjour et les passeports. Annoncé mi-avril 2005 par le ministre de l'Intérieur, Dominique de Villepin (pas encore 1er ministre), la France veut se doter d'une carte d'identité électronique **obligatoire** et **payante**, en 2007.
Le projet INES voit le jour le 1er Mars 2005 (PDF) :
http://www.foruminternet.org/telechargement/forum/pres-prog-ines-20050301.pdf

Terminologie
CNIL : Commission Nationale de l'Informatique et des Libertés.
CNIE : Carte Nationale d'Identité Electronique. Nom de la nouvelle carte.
INES : Identité Nationale Electronique Sécurisée. Nom du projet de sécurisation de l'identité.
FDI : Forum des Droits sur l'Internet
G29 : Groupe de travail européen crée par l'article 29
Convention 108 : Comité consultatif du conseil de l'Europe
VIS : Projet européen de mise en place d'un système commun d'identification sur les visas.

Identification Biométrique : toute reconnaissance d'une personne basée sur des particularités physiques uniques chez un individu. (iris, rétine, empreintes digitales, forme du visage, empreinte dentaire, ADN, forme de la main, etc …).

L'aspect politique

Aujourd'hui, la situation de la carte d'identité

La carte nationale d'identité est une pièce d'identité**.** Même périmée, elle permet de justifier de son identité, tant que la photo est ressemblante. Elle n'est pas obligatoire. Durée de validité: 10 ans.
Au-delà, vous pouvez faire établir une nouvelle carte (renouvellement) par la carte nationale d'identité informatisée, créée par le décret du 19 mars 1987, remplace la carte d'identité en papier. Elle est délivrée sur l'ensemble du territoire national depuis décembre 1995 (métropole et DOM). Plus petite que la carte papier, elle est en plastique rigide. La délivrance d'une carte informatisée permet de limiter les risques de falsification ou de contrefaçon. Comment la faire établir ? Les formalités sont celles de l'établissement d'une première carte d'identité. Vous devez de plus apposer votre empreinte digitale sur le formulaire de demande.

Qui peut contrôler votre identité?
Le contrôle d'identité peut être fait par un policier ou un gendarme. Le contrôle d'identité de police administrative vise toute personne se trouvant en France. Il est fait à titre de prévention d'une atteinte à l'ordre public. Il a lieu dans des lieux publics: rue, gare....

Quand ?
Des contrôles d'identité peuvent être pratiqués à l'égard des personnes dont un indice laisse penser qu'elles:
- ont commis ou tenté de commettre une infraction,
- se préparent à commettre un crime ou un délit,
- sont susceptibles de fournir des renseignements sur un crime ou un délit,
- font l'objet de recherches ordonnées par une autorité judiciaire.

Depuis l'entrée en vigueur de la convention de Schengen, des contrôles peuvent être effectués:
- dans les zones situées à moins de 20 kilomètres des frontières des Etats signataires de la convention (Allemagne, Belgique, Luxembourg, Espagne),

- dans les ports, aéroports, gares routières et ferroviaires ouverts au trafic international.

Le contrôle d'identité de police judiciaire est pratiqué sur instruction du procureur de la République pour la recherche d'infractions précises, dans des lieux et pour une période déterminés. La police ou la gendarmerie peut vous retenir sur place ou dans leurs locaux pour établir votre identité. Vous pouvez être présenté à un officier de police judiciaire. Vous pouvez présenter de nouveaux papiers, faire appel à des témoignages. Délais: 4 heures maximum entre le début du contrôle d'identité et la fin de la vérification d'identité.

Prise d'empreintes digitales
La prise d'empreintes digitales ou de photos ne peut être faite que sur autorisation du procureur de la République ou du juge d'instruction si elles constituent l'unique moyen d'établir votre identité.
La vérification d'identité doit donner lieu à un procès-verbal. Vous pouvez refuser de le signer. Vous pouvez en demander copie.

En Europe, tour d'horizon des pratiques
http://www.senat.fr/lc/lc118/lc1180.html

Un essai de carte sécurisée avait été entrepris déjà en France
En 1979, le Ministre de l'Intérieur avait annoncé l'introduction d'une nouvelle carte d'identité plus sécurisée à lecture laser afin de réduire les fraudes. Il y eut peu de résistance de la part du public au départ, mais au fur et à mesure que les détails techniques du projet furent publiés, les oppositions du public grandirent. Le débat public s'intensifia en 1980, avec le Syndicat de la magistrature émettant ses craintes. La CNIL intervint également concernant l'utilisation d'une numérotation qui aurait pu être utilisée pour lier différents fichiers administratifs et notamment ceux de la police. Dans sa délibération de 1980, la CNIL a même recommandé qu'en cas de circonstances exceptionnelles, il puisse être procédé à la destruction du système. En 1981, le **projet fut abandonné** quand François Mitterrand fit également part de ses craintes partagées par Robert Badinter, alors Ministre de la Justice.

Mais alors pourquoi changer ?

Les raisons apparentes

Diminuer le montant de la fraude aux prestations sociales en France

Aucune étude ne permet de quantifier cette prétendue fraude. Mais il est certain que le coût du projet INES va dépasser de très loin l'éventuelle perte financière évoquée. Le gouvernement semble se référer à une étude du gouvernement britannique, comme indiqué dans la note de bas de page n°2 du document de présentation du programme INÉS (voir références). La majorité de la fraude sur les prestations sociales est due à une sous déclaration des revenus ou à une non-déclaration des circonstances particulières financières ou familiales. Les agences nationales offrant des prestations sociales semblent s'accorder sur le fait que le vol d'identité n'est pas un problème majeur. Par exemple la sécurité sociale australienne a estimé que le vol d'identité ne compte que pour 0.6% de ses sur-paiements alors que la non déclaration des variations de revenus représente 61% ! Ironiquement, Chris Pond, membre du parlement britannique, a confirmé que le vol d'identité ne représente qu'une fraction minuscule de la fraude sur les prestations sociales. Sur les deux milliards de livres annuels dus à la fraude (estimation), seulement cinquante millions seraient dus à des personnes n'étant pas celles qu'elles prétendent être. Cela n'empêche pas Monsieur Fitoussi, Préfet, directeur du programme INÉS d'utiliser le chiffre total dans ses présentations pour promouvoir la CNIÉ ! Le coût de mettre en place la CNIÉ sera bien supérieur à ces pertes !

Epouser les exigences internationales en matière de lutte contre le terrorisme.
En Avril 2004, Privacy International, un groupe international pour la défense des droits de l'homme, a publié le seul rapport public (PDF - http://www.privacyinternational.org/issues/idcard/uk/id-terrorism.pdf) dans lequel sont étudiés les liens entre terrorisme et cartes d'identité. Ce rapport indique entre autres :
« La présence d'une carte d'identité n'est pas reconnue par les analystes comme un composant significatif ou important des stratégies anti-terrorisme. »
« L'analyse détaillée des informations disponibles dans le domaine public n'a pas permis de mettre en évidence un lien entre cartes d'identité et mesures anti-terrorisme réussies. Les terroristes ont

habituellement traversé les frontières avec des visas touristiques (tels ceux impliqués dans les attaques aux États-Unis), ou bien ils sont domiciliés et en possession légitime de cartes d'identification (comme ceux impliqués dans les explosions de Madrid). »
« Des 25 pays qui ont été les plus touchés par le terrorisme depuis 1989, quatre-vingts pourcent ont des cartes d'identité, un tiers desquels incluent des données anthropométriques. Cette étude n'a pas pu trouver un seul exemple où la présence d'un système de cartes d'identité dans ces pays avait été considérée comme un élément significatif de la lutte contre l'activité terroriste. »
« Presque deux tiers des terroristes connus opèrent sous leur identité véritable. Le reste utilise des techniques variées pour forger ou voler des identités. Il est possible que l'existence d'une carte à haute sécurité apporte une mesure de légitimité accrue pour ces personnes. »

Insécurité des « procédures actuelles de délivrance des CNI et des passeports
Le fait d'avoir des demandes distinctes ne serait-il pas dû au fait que les passeports sont délivrés par les préfectures et que les cartes d'identité sont produites à Val Maubué ou à Limoges ? Il existe déjà un formulaire unique de toute façon.

Développement de nouvelles applications en ligne
La CNIÉ ne servira pas de carte de paiement (voir le document gouvernemental de présentation de la CNIE) mais pourra être utilisée pour s'identifier avant de pouvoir acheter. En pratique cela veut dire que les sites de commerce électronique demanderont non seulement les détails bancaires du consommateur (carte de crédit) mais également une preuve de son identité. En pratique cela ne fait que compliquer la transaction et donner encore plus de détails personnels au vendeur.

Les vraies raisons

Après le 11 Septembre, nous sommes tous américains
Mais l'objectif principal est également d'épouser les exigences internationales en matière de la lutte contre le terrorisme, priorité accrue depuis les attentats de septembre 2001. Ce qui nécessite une bonne dose de coordination entre pays. Car l'un des enjeux cruciaux est de déterminer quels identifiants biométriques seront retenus pour être insérés dans ces cartes à puces. S'il semble définitivement acquis que l'image numérique du visage sera l'un d'entre eux, deux "courants" s'affrontent pour le second identifiant:
les adeptes de l'iris de l'œil d'un côté, et les partisans de l'empreinte digitale de l'autre.

La France s'exécute aussitôt
L'Agence pour le développement de l'administration électronique (Adae) : La nouvelle carte d'identité est l'élément central d'un chantier débuté en 2001 sous l'ère du ministre socialiste Daniel Vaillant. Ce projet, appelé «titre fondateur» (comprendre: titre d'identité), porte sur «la mise en place d'un bloc d'informations sécurisées». Son objectif est de simplifier et de sécuriser les procédures de délivrance des papiers d'identité.

Du pognon en jeu …
L'intérêt est avant tout économique, puisque «c'est une société américaine, Iridian, qui détient le brevet du scanner de l'iris de l'œil jusqu'en 2006», explique un cadre de la police aux frontières. Bizarrement, les Etats-Unis et la Grande-Bretagne sont dirigés vers le scanning de l'iris comme élément biométrique obligatoire sur la CNIE ou le passeport.

Le traitement informatique des empreintes digitales est la grande spécialité du groupe français d'électronique de défense Sagem. Bizarrement, les Français poussent pour les empreintes digitales.
Lors d'une réunion du G8 en mai 2003, Nicolas Sarkozy, alors ministre de l'Intérieur, avait résumé ainsi la position de Paris: «La tradition française, c'est l'empreinte digitale». Selon Le Figaro, la France aurait réussi à entraîner dans son sillage l'Italie, l'Autriche, la Suède, la Belgique, la Lettonie, l'Espagne, la Slovaquie, la Hongrie, la Norvège, la Pologne, le Danemark et la Lituanie

Les acteurs

Dans le reste du monde, euh, enfin, disons les Américains

Les recommandations de l'OACI (document 9303 publié en ***2002***) concernent l'introduction de la biométrie

dans les documents de voyage conformément aux travaux menés par le Groupe consultatif technique sur les documents de voyage lisibles à la machine (TAG/MRTD) mandaté en cela par la convention de Chicago. Ce groupe établit et adopte des « spécifications » (c.-à-d. des exigences techniques détaillées) pour la conception de ces documents de voyage. Les spécifications du groupe consultatif technique sont publiées dans le document 9303 de l'OACI (pour plus d'infos (en anglais) : http://www.icao.int/mrtd/overview/overview.cfm).

Après le 11 septembre, tout est possible, surtout de faire des profits …

L'Union Européenne

C'est tranché !

En Europe, toutefois, la question est déjà réglée pour les visas et les titres de séjour: Bruxelles a opté pour la photo numérisée et les empreintes digitales (deux doigts). Paris devrait donc lui emboîter le pas sans scrupules, et entamer les premiers tests à l'aéroport de Roissy avec, comme volontaires, des clients d'Air France.

Mais beaucoup de circonspection …

Sur initiative de la CNIL, le groupe des commissaires européens en charge de la protection des données («groupe de l'article 29») a rendu un avis très circonstancié sur les propositions de règlement, sur les visas et les titres de séjour élaborés en ce domaine et en particulier sur les questions que soulève au regard des principes de protection des données, la création au plan européen d'une base centralisée de données biométriques. Il a également fait part au président du conseil de l'Union européenne de ses réserves sur les propositions de règlement concernant les passeports biométriques.

Le G29 de l'Union européenne
Créé par l'article 29 de la directive européenne de 1995 sur la protection des données personnelles, ce groupe, à caractère consultatif, est composé des représentants des autorités nationales de contrôle. Il a rendu, le ***11 août 2004***, un avis sur l'insertion d'éléments biométriques dans les visas et titres de séjour en tenant compte des projets de création du système européen d'information sur les visas délivrés aux ressortissants des pays tiers (projet VIS). Tout en se déclarant conscient des impératifs liés à la lutte contre le « visa shopping » et à l'usurpation d'identité, ce groupe a souligné la nécessité de respecter tout particulièrement les droits et libertés fondamentaux des personnes dans le cadre des traitements de données biométriques, telles les empreintes digitales qui laissent des traces dans la vie quotidienne.

Le groupe de l'article 29 a ainsi considéré comme légitime l'insertion de la photo et des empreintes digitales dans une puce sans contact, dès lors qu'elle a pour finalité d'établir un lien plus fiable entre le visa ou le titre de séjour et son titulaire (vérification de l'identité), étant entendu que cette finalité devrait être clairement précisée dans l'acte créant le traitement. En outre, sa mise en œuvre suppose que soient tranchées les questions liées à la fiabilité et à la sécurité des systèmes qui seront retenus (sécurité de tout le processus de collecte et d'insertion, garanties lorsque la personne ne dispose pas des éléments biométriques en cause, haute fiabilité des systèmes et garanties contre les faux rejets, mesures contre l'accès à l'insu de la personne ou par des personnes non autorisées). En revanche, le groupe a exprimé de sérieuses réserves sur la conservation des données biométriques, telles que les empreintes digitales, dans des bases de données (au-delà de la période nécessaire aux contrôles légaux pour la délivrance des documents, à leur production et à leur remise aux demandeurs) à des fins de contrôle ultérieur des immigrants illégaux. Le groupe de l'article 29 a par ailleurs fait part au président de l'union européenne, le 30 novembre 2004, de ses réserves sur les propositions de règlement concernant les passeports biométriques.

Le comité consultatif du Conseil de l'Europe
Le Comité consultatif créé par la Convention 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel a récemment rendu public un rapport d'étape relatif à l'application des principes de la Convention 108 à la collecte et au traitement des données biométriques. La CNIL, comme les autres autorités de protection des données à été consultée.

La France

C'est tranché !

Conformément à ce que recommande l'Union européenne et à ce que réclament les ***États-Unis*** depuis le ***11 septembre 2001***, la France va se doter de papiers d'identité dans lesquels seront intégrés des identifiants biométriques. Lancement prévu pour 2006.

En ce qui concerne le projet INES et la CNIE en France, beaucoup de critiques de la part des opposants, sur la méthode d'abord. **Dominique de Villepin** a dévoilé ses ambitions alors que, deux mois auparavant, il avait lui-même confié au Forum des droits sur l'Internet (FDI) la mission d'animer une réflexion sur le sujet, dans l'optique d'un débat législatif à venir. Bref, le ministre aurait pris ses décisions avant même d'obtenir les avis qu'il avait sollicités.

Le débat ne fut qu'une mascarade. Celui-ci devait se terminer en mai, pourtant le 11 Avril 2005, M. Raffarin donna son feu vert, sans même avoir attendu les conclusions du débat et sans même avoir saisi la CNIL ou le Conseil d'État ! Vu le manque de budget de la CNIL et le peut de temps qui lui a été concédé pour se pencher sur ce dossier, il ne fait aucun doute que sa voix sera très limitée.

Mais beaucoup de circonspection …

Le Sénat
La mission d'information de la commission des Lois du Sénat sur la nouvelle génération de documents d'identité et la fraude documentaire a tenu sa réunion constitutive le ***mercredi 9 février 2005***. Ses travaux porteront sur l'évaluation de la fraude à l'identité et les réponses apportées par les pouvoirs publics; ils traiteront notamment de la "nouvelle génération de titres d'identité électroniques intégrant des données biométriques et offrant des services nouveaux".
Pour plus d'informations : http://www.senat.fr/presse/cp20050211.html

FDI
Le Forum est investi de trois grandes missions : la concertation entre les acteurs, l'information et la sensibilisation du public et la coopération internationale. Les membres sont :
http://www.foruminternet.org/quisommesnous/membres.phtml?PHPSESSID=fbfe107e35636bd658ddfc4d1edf00a4

Les opposants
La Ligue des Droits de l'Homme, le Syndicat de la magistrature, le Syndicat des avocats de France, les organisations CFDT, CFTC, CGT et Sud de l'Insee, les associations Iris et Delis, l'Association française des juristes démocrates dénoncent de graves dérives dans ce projet Ines (Identité nationale électronique sécurisée). Et demandent son retrait.

CNIL
La CNIL n'a pas encore été réellement chargée du projet INES mais le ministère de l'Intérieur ayant lancé, en 2001, une mission d'étude sur ce projet de carte d'identité électronique, la CNIL a été tenue informée du déroulement des réflexions et travaux menés par le ministère ainsi que par le Secrétariat d'Etat à la réforme de l'Etat dans le cadre, en particulier, du plan de développement de l'administration électronique, la nouvelle carte électronique étant susceptible d'être utilisée pour accéder à des télé services.
La CNIL a pu ainsi faire part au ministère de l'intérieur de ses premières observations et interrogations sur ce projet. Elle lui a ainsi demandé un argumentaire précis sur, d'une part, la situation actuellement constatée en matière d'usurpation d'identité et d'autre part, les finalités et les modalités selon lesquelles seraient utilisées les données biométriques, qu'il s'agisse de leur consultation par lecture directe de la carte d'identité ou de la conservation, dans une base de données centrale, des empreintes digitales. La CNIL suit très attentivement les travaux conduits au plan européen et visant à généraliser l'introduction de données biométriques (photographies et empreintes digitales) dans les passeports, les visas et les titres de séjour et à mettre en place un système commun d'information sur les visas (VIS) qui permettrait de recenser dans une base unique les demandes et les refus de visas.

Vive la politique

Bon, alors voilà un problème réglé. La CNIE va devenir obligatoire et payante (30 à 40 euros ?) en France. Tout cela a été décidé unilatéralement. Le coût global estimé de la mise en place de la CNIÉ par l'Agence pour le développement de l'Administration électronique est de 60 millions d'euros (presque 400 millions de francs). En fait « les coûts de fonctionnement supplémentaires à ceux de la CNI actuelle sont estimés à 36,7 M€ » (coûts supplémentaires sans estimation de retour sur investissement). Comme on peut aisément l'imaginer, « la diversité des objectifs du projet risque d'être à la fois un facteur de complexité (donc de délais et de surcoûts). » Ces estimations ont changé et le 12 avril 2005, M. Villepin a annoncé un surcoût de 25 M€ par an qui devrait être « compensé par les économies dues à la baisse des fraudes ». M. Villepin a également annoncé que la carte serait obligatoire et payante. On peut donc se demander si le surcoût ne sera pas simplement compensé par cette nouvelle taxe étatique, l'expérience d'autres pays montrant que les économies faîtes ne seront que très faibles et certainement en dessous du surcoût. Le coût annuel quant à lui est estimé à 205 M€ (soit plus de 1,3 milliards de francs) ! Ne serait-il pas mieux utilisé pour sauver la Recherche française ?Il faut noter que ces estimations n'incluent pas les autres aspects du projet INÉS comme l'interconnexion des bases de données nationales. En fait, le plan d'administration en ligne présenté par le Gouvernement en Février 2004, se décline en 140 initiatives, représentant un investissement initial de 1,8 milliards d'euros. À titre de comparaison, en 2002, le gouvernement britannique avait estimé l'introduction d'un système similaire à 4,5 milliards d'euros. Il a corrigé son estimation en 2004 pour atteindre 8 milliards d'euros sur dix ans. Enfin l'expérience montre que la politique informatique de l'État a été révélatrice d'immenses gâchis, gâchis industriel avec Bull, mais aussi gâchis financier, avec, par exemple le plan informatique pour tous en 1985 dont l'utilisation sera plus que limitée.

L'aspect technique et les dangers éventuels

Teneur annoncée du projet

Si vous jetez un œil sur la description du projet INES (en référence) :

Données présentes sur la carte
- nom
- prénom
- date de naissance
- lieu de naissance
- sexe
- adresse
- signature manuscrite
- préfecture ayant délivré la carte
- numéro de carte
- photographie
- deux empreintes digitales numérisées
- D'autres informations pourront être stockées si le porteur de la carte le souhaite

Utilisation
- signature électronique
- identification sur Internet
- applications de la vie courante (« commerce, poste, etc. »)
- nombreux usages « imaginés par nos concitoyens » ;
- remplissage de formulaires (e.g., administratifs) en ligne
- substitution à d'autres papiers (e.g., permis de conduire)

Les problèmes possibles et relevés

Dans la définition de ce projet et sa mise en application, un certain nombre de zones d'ombre a été identifié par les différents syndicats (magistrature, etc…) et les parlementaires.

Regroupement de données : un fichier de la population

Ensuite, regrouper des éléments d'identification qui, aujourd'hui, existent de manière éparse. Le projet INES nécessitera alors la *« constitution d'un **fichier central** de toute la population, dans la mesure où la carte va être obligatoire »,* explique Côme Jacquemin. Fichier qui permettra alors de recouper une adresse avec une empreinte digitale, un nom avec une transaction sur Internet, etc.
« Il existe bien un fichier d'empreintes digitales, mais, aujourd'hui, il est limité aux personnes déjà connues de la justice. On donne aussi déjà son empreinte digitale pour faire faire sa carte d'identité, mais elle n'est pas fichée. » La constitution d'un tel fichier irait ainsi à l'encontre du principe de « proportionnalité » entre les traitements de données à caractère personnel et le but de ce traitement, tel qu'édicté par la loi Informatique et libertés.

Lecture sans contact

INES prévoit une carte à puce RFID (Radio Fréquence), pour une ***lecture sans contact***. Les données qu'elle contient vont donc voyager par les ondes. «Cela pose un certain nombre de problèmes, estime Meryem Marzouki, présidente d'Iris. Le contrôle peut se faire à l'insu du porteur, il y a des risques d'interception des données, puisqu'il y a émission d'ondes radio, et des risques de lectures indues, par une personne ou par un matériel qui ne serait pas censé lire la carte. »

Croisement d'informations

Les dérives en matière de croisement d'informations qui sera techniquement possible avec cette carte multi usage. A terme, cette carte pourrait être utilisée pour stocker ***le dossier médical du porteur***, son casier judiciaire, pour obtenir un document administratif, payer ses achats, voter, signer un contrat à distance, etc.

D'accord, mais si …

Questionnement à propos de INES

Les dérives possibles identifiées par les opposants sont déjà assez parlantes mais si nous les reprenons en détail et que nous tentons de les mettre en relief, alors il y a de quoi avoir peur. Je précise que ces questions et/ou prédiction n'ont rien d'irréalistes. Elles sont ABSOLUMENT possibles dés aujourd'hui !!

Général

. Si un escroc vole vos données, alors il sera très difficile pour vous de prouver votre innocence.

. Il est fort probable que les données ADN soient ajoutées à ces infos pour les besoins de la police (interpol, etc…). Toute la population sera alors soumise à une prise de sang.

. Si des lecteurs de cette carte vont apparaître un peu partout, comment contrôler que ces lecteurs vont lire uniquement les données concernant la personne qui initie la lecture (un policier saura, en interrogeant e fichier central, si vous avez payé vos impôts – un commerçant connaîtra votre salaire – un employeur saura si vous avez eu des amendes – un employeur verra votre dossier médical,…)

Lecture sans contact

Voilà un point absolument incroyable. Cette carte est prévue pour être lue à distance !!

. Vous entrez chez un commerçant, il connaît alors votre nom, votre adresse, votre signature !

. Comme tout signal radio- fréquence, il est tout à fait possible soit de le brouiller, soit de le pirater, soit de le scanner. Ainsi vous pouvez imaginer que :

- n'importe qui puisse savoir à quel endroit vous êtes (pensez aux téléphones portables)
- n'importe qui puisse savoir avec qui vous êtes

- un pirate peut se faire passer pour vous
- on puisse vous suivre à la trace avec un nombre suffisant d'antennes

Fichier central

. Le fichier central sera d'une taille énorme (pour 65 Millions de personnes avec un scan des empreintes, la photo et les données annexes). Qui va le gérer ?

. Comme tout système informatique, il est tout à fait possible de trouver des failles. Imaginez que l'on arrive à récupérer les informations de ce fichier. Alors, grâce à votre signature, votre nom et adresse, il sera beaucoup plus facile de se faire passer pour vous.

. Si le système informatique sombre en panne ? Comme il s'agit du socle des transactions administratives, tout sera bloqué. Qui peut nous dire si, en cas de contrôle simple d'identité, nous ne devrons pas rester à disposition le temps de la remise en marche du système ?

. Qui va pouvoir nous assurer qu'aucune autre donnée sera présente dans ce fichier ? En effet, si la carte elle-même comporte des données (à priori) précises, lorsque vous la donnez à un agent quelconque (police, douane, impôts, commerçant,…) qu'est-ce qui vous prouve que dans le fichier central, aux cotés des données de la carte, ne vont pas se trouver des informations additionnelles ? (infractions, barème d'imposition, salaire, lieu de la vérification, etc…) .

Imaginons le pire pour INES

Et puis pourquoi s'arrêter là ? Vous allez me dire que je ne joue pas le jeu de l'objectivité en brandissant le spectre du « Big Brother », en agitant des épouvantails pour aiguillonner vos peurs. J'accepte la remarque, mais j'objecte que :

- *Il y a vingt ans, bon nombre de faits sécuritaires aujourd'hui établis, auraient été taxés de fiction (caméras dans les rues. écoutes téléphoniques, espionnage des ordinateurs, satellites de surveillance,…)*
- *Lorsqu'un tel système veut se mettre en place, cela implique que la confiance du citoyen dans l'éthique de son système politique et policier doit être intact. Ce n'est pas le cas en ce qui me concerne, mais quand bien même, si c'est le cas aujourd'hui, comment préjuger de demain ?*

D'autre part, les faits exposés ci-dessous sont techniquement réels. Ethiquement, tout devrait être évalué (ce qui semble être fait correctement par les instances impliquées), mais lorsque l'on voit comment ce projet INES est devenu effectif, nous sommes en droit d'avoir des doutes.

. Je suis à l'entrée d'une discothèque. Le molosse de l'entrée me balaie avec son scanner portable. Il me dit que je ne peux pas rentrer. Par contre il laisse entrer le type derrière moi : scanning du casier judiciaire.

. Je passe la porte de l'assurance. Un employé s'approche et me précise que les cas d'hépatite ne sont pas pris en charge : scanning du dossier médical.

. Je passe mon badge dans le lecteur du restaurant. Un garçon s'avance et me dit que les seules places disponibles sont dans la partie bar. Un maître d'hôtel prend délicatement le manteau de la personne derrière moi et l'accompagne dans la partie gastronomique : scanning du métier ou de la tranche d'imposition.

. Je passe le lecteur de badge de la librairie. Une dame s'avance vers moi, agacée, et m'annonce que les revues érotiques sont au fond du magasin. Lecture des cookies pour les sites internet de prédilection.

. Une personne me bouscule et me fait tomber. Il m'aide gentiment à me relever. Le lendemain, la police débarque chez moi. Je suis suspecté d'avoir commis un vol avec violence. Je clame mon innocence, mais les inspecteurs ont retrouvé un cheveu m'appartenant sur les lieux et le positionnement électronique de mon badge leur permet d'affirmer que j'étais dans le secteur au moment du vol. Je suis cuit !!

. Je me présente chez un employeur potentiel. Au bout de cinq minutes dans une salle d'attente, on me dit que je ne corresponds pas au profil et on me prie de sortir avec 4 autres personnes : lecture du dossier médical, du casier judiciaire, etc…

….

Mais la CNIE n'est pas la seule voie par laquelle notre vie privée peut être bafouée

Oui je sais, passer en revue les gadgets techniques ex-futuristes n'est pas digne d'une enquête factuelle. Pourtant, en prenant du recul, nous pouvons nous apercevoir que ces dernières années ont été particulièrement riches pour le recul des libertés individuelles.

Badges sous-cutanés

Ah le 11 septembre, que de commerce cet événement tragique aura pu générer : http://www.indexel.net/1_20_3875___/Les_premiers_badges_sous-cutanes_autorises_aux_Etats-Unis.htm

On constate déjà l'aval de la Food and Drug Administration pour l'emploi de puces sous cutanées dans les hôpitaux aux États-Unis pour les patients (http://www.msnbc.msn.com/id/6237364/).

Certains recommandent la même chose pour les cadavres (http://www.newstarget.com/005138.html).

Au Royaume-Uni les délinquants récidivistes sont pistés par satellite grâce à un bracelet émetteur (http://news.bbc.co.uk/1/hi/uk_politics/1841304.stm).

Des bars et pubs comme le « Baja Beach Club » de Barcelone ou le « Bar Soba » de Glasgow offrent déjà une puce électronique sous-cutanée à leurs clients (http://www.prisonplanet.com/articles/april2004/040704bajabeachclub.htm et http://observer.guardian.co.uk/uk_news/story/0,6903,1391545,00.html).

Au Mexique, une société privée offre un service appelé « VeryKid » pour réduire le nombre d'enlèvements d'enfants en implantant une puce émettrice dans le corps de ceux-ci (http://www.wired.com/news/technology/0,1282,60771,00.html)

L'Europe envisage de réglementer l'emploi d'implants sous-cutanés et mais la propagande mercantile est déjà en marche.

Téléphones portables

Une récente déclaration de Pierre Martinet, qui avouait avoir été chargé de surveiller Bruno Gaccio des guignols de Canal+, expliquait qu'il était possible à qui en a les moyens de faire décrocher votre portable, silencieusement, pour l'utiliser comme un micro. Si cela est vérifié sur tous les appareils, avouez que c'est génial. Il est possible de nous situer géographiquement, à quelques mètres près, mais en plus d'écouter nos conversations. Tout cela par un appareil que vous payez vous-même !!
Dans le même esprit, lisez : Espionnage par portable : http://www.netespion.com/produits/phone.htm

Récepteur GPS canettes de Coca : http://www.01net.com/article/247730.html

Satellites et réseaux de surveillance

Parlement européen – techniques de contrôle politique
http://www.europarl.eu.int/stoa/publi/166499/execsum_fr.htm

Téléphones portables espion pour employeurs (PDF) : http://www.geogeny.ch/pdf/matin2_140104.pdf

Echelon et frenchelon : http://www.guajara.com/wiki/fr/wikipedia/e/ec/echelon.html

Conclusion

Beaucoup d'éléments laissent raisonnablement penser que la carte à puce pourrait n'être qu'une étape vers un système de fichage corporel par puce sous-cutanée. Certes l'État insiste sur le fait qu'il veillera aux dérives qui pourraient mettre en danger la vie privée. Mais les États changent et les lois d'exceptions permanentes qui ont fleuri depuis le 11 septembre 2001, en Europe comme aux États-unis, indiquent une évolution négative. De toutes façons il existe trop de flou sur le contenu et le contenant de la CNIE.

Ce qui change, c'est nous, car la technique a toujours été capable du meilleur comme du pire. Nous, nous nous habituons, nous acceptons, nous tolérons et parfois nous acquiessons et jubilons à l'idée des possibilités incroyables. Le plus effrayant est que de plus en plus, ces dispositifs sont mis en place avec notre assentiment, devant nos yeux qui ne voient rien et sous nos applaudissements. Bien sûr le tour de force de M. de Villepin qui a prétexté un débat, pour finalement passer en force n'est pas digne de la démocratie qu'il clame vouloir protéger. Mais pourtant, rien n'a été fait de manière secrète. Toutes ces mécaniques anti-liberté avancent à peine masquées mais sans arrêt. Ainsi certains diront « mais à quoi bon râler pour la lecture sans contact quand les portables nous positionnent et les caméras nous filment ».

Comme l'explique l'excellent article de la montée du flicage (indolore) : http://www.monde-diplomatique.fr/2004/08/DUCLOS/11493 : « …Il ne faut pas croire que le contrôle des individus concerne seulement la surveillance ou la sanction. Au contraire, c'est en opposition à ces dernières que le public est de plus en plus conquis par des propositions techniciennes permettant d'éliminer tout problème à la base... Par exemple, pour justifier de dépenses vouées à automatiser la conduite automobile (et brider la capacité de décision individuelle, considérée comme une source majeure d'erreurs et d'accidents), les autorités s'appuient sur l'appel aux sentiments : « 41 000 morts par an sur les routes européennes » semble l'argument sans réplique pour développer des systèmes de transport intelligents (STI) qui prévoient le téléguidage des véhicules »

Si vous sentez que vous perdez le contrôle alors que d'autres l'assoient, alors signez la pétition.
La pétition en ligne est accessible par : http://www.ldh-france.org/actu_dernieregheure.cfm?page=1&idactu=1059

Et, je vous en prie, allez voir : ***« Bienvenue à Gattaca »*** …

L'Aiguillon

Références

Film : Bienvenue à Gattaca (Excellentissime) : http://www.devildead.com/gattaca/gattaca.htm

CNIL : débat sur la CNIE : http://www.cnil.fr/index.php?id=1772

Rapport du groupe de l'article 29 (PDF) sur le passport biométrique :
http://www.cnil.fr/fileadmin/documents/approfondir/dossier/CNI-biometrie/2004-11-30G29-eupassports_fr.pdf

Avis du groupe de l'article 29 (PDF) sur le projet VIS :
http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2004/wp96_fr.pdf

Forum Internet du FDI pour la CNIE : http://www.foruminternet.org/carte_identite/

Aujourd'hui, la carte nationale d'identité : http://www.reunion.pref.gouv.fr/intpref/demarche/identite/identite.htm

Description du projet INES : http://www.foruminternet.org/telechargement/forum/pres-prog-ines-20050301.pdf

Articles de dénonciation du projet INES :

01net : http://www.01net.com/article/279214.html
zdnet : http://www.zdnet.fr/actualites/informatique/0,39040745,39227151,00.htm
pcinpact : http://www.pcinpact.com/actu/news/Petition_contre_INES_la_carte_didentite_electroniq.htm
indexel : http://www.indexel.net/1_20_3993___/Carte_d_identite_electronique___demain_tous_fiches__.htm
http://www.indexel.net/1_20_4122___/Carte_d_identite_numerique___non_au_flicage__.htm
Evolution des techniques – bethel : http://www.bethel-fr.com/afficher_info.php?id=12767.90