

## **DEBAT NATIONAL SUR LA CARTE D'IDENTITE ELECTRONIQUE**

### Avis de spécialistes

Pour compléter les débats, voici l'avis de quelques spécialistes à la fois sur le projet de carte nationale d'identité électronique et sur les discussions en cours, mais aussi, plus généralement, sur ces nouveaux titres d'identité électronique qui apparaissent dans de nombreux pays, sur la biométrie, sur la notion d'identité numérique, les libertés individuelles...

#### **Jean Gonié**

Animateur, Juriste, Le Forum des droits sur l'internet

\*

**I.** Contribution de **Pierre PIAZZA, chargé de recherche à Institut National des Hautes Études de Sécurité (INHES)** - 7 mars 2005

**II.** Contribution de **Thierry PIETTE-COUDOL, Avocat près la cour d'appel de Paris** - 7 mars 2005

**III.** Contribution de **Youval ECHED, Secrétaire Général de l'Académie Internationale des Droits de l'Homme** - 7 mars 2005

**IV.** Contribution d'**Arnaud BELLEIL du groupe « Identité Numérique » de la Fondation Internet Nouvelle Génération** - 7 mars 2005

**V.** Contribution de **Cyril ROJINSKY, Avocat au barreau de Paris** - 7 mars 2005

**VI.** Contribution de **l'Association pour la Promotion et la Recherche en Informatique Libre (APRIL)** - 23 mars 2005

**VII.** Contribution d'**Alain DAMASIO, écrivain** - 23 mars 2005

**VIII.** Contribution de **Gérard WEISZ, Fédération Nationale des Tiers de Confiance** - 23 mars 2005

**IX.** Contribution de **Gérard DUBEY, sociologue à l'Institut National des Télécoms** - 30 mars 2005

**X.** Contribution d'**Amar LAKEL, Chercheur associé, Université de Paris X, Nanterre** - 30 mars 2005

**XI.** Contribution de **Xavier GUCHET, philosophe, Université de Paris 1** - 30 mars 2005

**XII.** Contribution de **l'Observatoire des Usages de l'Internet (OUI)** - 4 avril 2005

**XIII.** Contribution de **Claudine GUERRIER, Enseignant chercheur à l'Institut National des Télécoms** - 4 avril 2005

**XIV.** Contribution du **Club de l'Hyper République** - 4 avril 2005

**XV.** Contribution d'**Olivier ITEANU, Avocat à la Cour d'Appel de Paris** - 8 avril 2005

**XVI.** Contribution de **Patrice FLICHY, Professeur de sociologie à l'Université de Marne-la-Vallée** – 13 avril 2005

**XVII.** Contribution de **Thomas LAMARCHE, enseignant chercheur à l'université Lille 3** – 21 avril 2005

**XVIII.**Contribution de **Pierre TRUDEL, Professeur à l'Université de Montréal, Canada** – 11 mai 2005

**XIX.** Contribution de **Claudine DARDY, Professeur de sociologie à l'Université Paris XII** – 12 mai 2005

**XX.** Contribution de **Philippe RIGAUT, sociologue, enseignant à l'université de Picardie - Jules Verne** – 12 mai 2005

**XXI.** Contribution de **Eric CAPRIOLI, Avocat et membre de la délégation française auprès des Nations Unies sur les questions de commerce électronique** – 1<sup>er</sup> juin 2005

**XXII.** Contribution de **Thierry AUTRET, Expert Sécurité, Groupement des Cartes Bancaires** et **Marie-Laure LAFFAIRE, Avocat à la Cour d'Appel de Paris** – 1<sup>er</sup> juin 2005

## **I. Contribution de Pierre PIAZZA, chargé de recherche à l'INHES - 7 mars 2005**

Par **Pierre PIAZZA**

Chargé de recherche à l'INHES (Institut National des Hautes Études de Sécurité)

Auteur de *Histoire de la carte nationale d'identité* (Paris, Odile Jacob, 2004)

Pierre Piazza a coordonné le n° 56 des Cahiers de la sécurité consacré à la problématique « Police et identification » (à paraître en mars 2005)

Pierre Piazza a aussi co-dirigé, avec Xavier Crettiez, l'ouvrage *L'Encartement des individus. Histoire et sociologie d'une pratique d'État* (à paraître au premier trimestre 2005 à La Documentation française/ INHES)

Un détour par l'histoire s'avère indispensable afin d'éclairer la nature des débats consacrés au projet INES sur le forum des droits sur l'Internet. Les interrogations, les avis et les propositions des internautes s'ancrent dans des enjeux passés dont ils n'ont pas toujours conscience et qu'on se propose ici brièvement d'explicitier.

### **AU COEUR DE LA LOGIQUE DE L'ÉTAT**

#### **Exigences d'État**

L'émergence de la carte nationale d'identité doit être comprise au regard de la logique de l'État-nation qui trace une frontière juridique entre les nationaux et les individus ne relevant pas de cette catégorie. La nécessité de matérialiser cette frontière se fait surtout ressentir dès la fin du XIX<sup>e</sup> siècle<sup>1</sup>. La question de l'instauration d'une carte d'identité pour les nationaux répond également à la volonté des pouvoirs publics de rompre avec des modes traditionnels de reconnaissance considérés comme inefficients. Ainsi, en décidant d'instituer la première « carte d'identité de Français » dans le département de la Seine en septembre 1921, le préfet de police Robert Leullier entend surtout substituer un mode de preuve sûr à la formalité des témoins patentés qui, jusqu'alors réclamée pour toute démarche administrative où l'identité d'un individu doit être attestée, donne lieu à de très nombreux abus<sup>2</sup>. Enfin, en diffusant un modèle unique et uniforme de carte d'identité, les autorités visent à remédier aux problèmes engendrés par l'hétérogénéité des modes de déclinaisons identitaires auxquels les citoyens ont recours (passe-port intérieur, livret ouvrier, livret de famille, acte de naissance ou encore, à partir du début du XX<sup>e</sup> siècle, cartes d'identité délivrées par certaines associations). La pluralité de ces titres, la diversité de leur forme et de leur contenu ainsi que leur faible force probante sont perçues comme autant d'entraves aux pratiques policières et administratives d'identification.

#### **Rationalisme d'État**

Ces impératifs permettent d'appréhender l'enjeu que constitue la création et la généralisation d'une carte d'identité pour les nationaux. Il est indispensable de les prendre en considération afin de comprendre le travail bureaucratique qui a progressivement été déployé pour rendre ce titre sans cesse plus fiable. En effet, en même temps que s'impose progressivement l'idée de munir les Français d'un tel document, se développe une multitude de réflexions cherchant à en améliorer les performances afin de conférer aux autorités la possibilité d'identifier à tout instant chaque citoyen avec certitude. Émanant à l'origine d'auteurs de thèses de doctorat, de fonctionnaires de police ou encore de parlementaires, ces réflexions influencent les méthodes et pratiques administratives des services amenés à délivrer les premières cartes d'identité. Par la suite, le ministère de l'Intérieur va constamment s'évertuer à développer ces méthodes et pratiques pour parfaire son savoir et son savoir-faire en la

---

<sup>1</sup> Cf. Gérard Noiriel, *Le creuset français. Histoire de l'immigration. XIXe-XXe*, Paris, Seuil, 1988 et Gérard Noiriel, *La tyrannie du national. Le droit d'asile en Europe 1793-1993*, Paris, Calmann-Lévy, 1993.

<sup>2</sup> Cf. Pierre Piazza, « Septembre 1921 : la première "carte d'identité de Français" et ses enjeux », *Genèses*, n° 54, mars 2004.

matière. Il est à l'origine de très nombreux projets auxquels sont associés d'autres ministères ou bien des organismes d'État (par exemple les services statistiques durant l'Occupation, puis l'INSEE à la Libération). L'évolution des types d'identifiants mobilisés (photographie, empreintes digitales, numéro d'identification, etc.), des procédés utilisés pour conserver et classer les données individuelles recueillies ou encore des techniques employées en vue de protéger matériellement les cartes pour éviter les fraudes renseigne sur l'essor d'une logique proprement bureaucratique. En retraçant précisément, en longue durée, les différentes étapes de cette évolution, on se donne la possibilité d'éclairer une facette peu connue de l'État et de mieux comprendre comment il a pu se consolider en diffusant toujours plus largement au sein de la société un type de rationalité qui lui est propre<sup>3</sup>.

## Légitimation

Si les autorités se sont évertuées à légitimer les bénéfices qu'est susceptible de procurer à l'État la généralisation d'une carte d'identité autorisant une identification certaine des nationaux, au travers de leur rhétorique transparaît aussi la volonté de susciter l'adhésion des citoyens à leur projet d'encartement. Hormis durant la période de Vichy où le port de la « Carte d'identité de Français » est alors autoritairement imposée comme obligatoire, les pouvoirs publics développent une véritable stratégie discursive destinée à convaincre les citoyens de la nécessité de posséder un document répondant à des besoins étatiques. Leur objectif est de favoriser l'émergence d'un lien d'obéissance nouveau reposant exclusivement sur le consentement des citoyens et de parvenir ainsi à ce qu'ils s'obligent eux-mêmes à réclamer une carte grâce à laquelle l'État pourra accroître sa capacité de contrôle<sup>4</sup>.

Le caractère pratique de la carte est systématiquement vanté par les autorités : loin de constituer un dangereux outil de police, elle ne serait qu'un instrument pratique grâce auquel chaque citoyen peut apporter facilement (c'est-à-dire sans avoir besoin d'exhiber une multitude de titres) la preuve de son identité et de sa qualité de Français dans un monde caractérisé par une complexification croissante des rapports sociaux où la nationalité est devenue le critère prédominant conditionnant leur appartenance à la nation. Alors que la société se transforme sans cesse davantage en une collection d'individus atomisés, les pouvoirs publics insistent aussi sur l'idée selon laquelle cette carte permet de matérialiser incontestablement l'unicité de chaque citoyen et lui confère le sentiment de la voir constamment reconnue tout en lui évitant les désagréments de l'usurpation d'identité. La carte d'identité a même parfois pu être assimilée à un véritable certificat de respectabilité<sup>5</sup>. À d'autres époques, des élus ou fonctionnaires ont encore proposé d'introduire dans la carte d'identité des données précisant les antécédents judiciaires de son porteur<sup>6</sup> ou bien sa position vis-à-vis de ses obligations militaires<sup>7</sup>. Autant d'informations par le biais desquelles il deviendrait possible de s'assurer qu'un citoyen désireux de se munir de ce document n'a rien à dissimuler sur son propre compte et ne mène aucunement un mode de vie répréhensible.

---

<sup>3</sup> Cf. Pierre Piazza, *Histoire de la carte nationale d'identité*, Paris, Odile Jacob, 1994. Sur une période antérieure, cf. Vincent Denis, *Individu, identité et identification en France, 1715-1815*, à paraître chez Champ Vallon en 2005.

<sup>4</sup> Cf. notamment les débats spécifiquement consacrés à cette question par les membres de la Société générale des prisons en décembre 1921, *Revue pénitentiaire et de droit pénal*, n° 1-3, janvier-mars 1922.

<sup>5</sup> Cf. Frédéric Thomas, « La ligue du mal public », *Revue politique et littéraire*, 25 novembre 1882.

<sup>6</sup> Cf. la proposition de loi déposée par le député Pascal Ceccaldi, *J.O.*, Chambre des députés, onzième législature, documents parlementaires, n° 2 895, annexe au procès-verbal de la séance du 19 janvier 1917, p. 33.

<sup>7</sup> Cf. les propos tenus par le colonel Bayle lors de la séance de la Société générale des prisons de décembre 1921, *Revue pénitentiaire et de droit pénal*, *op.cit.*, p. 29.

## Matérialisation d'une appartenance commune/discriminations

Dès les débuts de la Troisième République, l'identification des Français par le papier est pensée comme un moyen de matérialiser une appartenance commune entre des citoyens reconnus comme égaux. L'encartement n'est plus, comme autrefois, alors uniquement perçu comme un dispositif destiné à faciliter la surveillance de certaines catégories de citoyens stigmatisées comme potentiellement dangereuses. Pour être « imaginée comme intrinsèquement limitée et souveraine<sup>8</sup> », la nation doit donc aussi revêtir une dimension concrète que l'État contribue à faire exister effectivement. L'entreprise étatique d'encartement des citoyens participe à mettre en forme la nation et à lui donner une plus grande cohérence. La généralisation progressive au sein du corps social d'une carte d'identité aux caractéristiques sans cesse davantage standardisées accrédite et renforce l'idée qu'elle constitue un « tout unifié ». Par la carte, l'État impose sa présence dans la vie quotidienne de chacun en même temps qu'il « fabrique de l'identique » en éradiquant progressivement les moindres différences dans la façon de matérialiser l'identité des citoyens. En tant que « dénominateur commun » donnant une consistance tant matérielle que symbolique à l'idée de nation comme collectif unifié, la carte d'identité a donc certainement permis aux citoyens de se forger une conscience plus nette de leur appartenance à cette communauté élargie au détriment d'autres types d'attaches en intériorisant « le découpage étatico-national de l'espace et du temps comme une donnée fondamentale de leur propre biographie<sup>9</sup> ».

Instrument d'unification de la collectivité nationale, la carte d'identité a aussi pu être mobilisée à des fins d'épuration de cette dernière. Les pratiques d'encartement du régime de Vichy sont à cet égard particulièrement révélatrices. Pour cimenter une communauté neuve et saine, Vichy entreprend d'en exclure les « métèques » qui l'ont abâtardie. Si un tel processus se dessine dès les années 1930, l'entreprise gouvernementale d'exclusion des Français d'origine étrangère se durcit à partir de 1940. Dans le cadre de la politique ségrégationniste qui se met alors en place, les procédures d'attribution de la « carte d'identité de Français » (créée en octobre 1940 et effectivement délivrée dans certains départements à partir de 1943) revêtent une importance cruciale pour le nouveau régime. Le rigoureux travail de contrôle accompli par les préfetures et les services statistiques leur permet de s'assurer du mode d'acquisition de la nationalité française de chaque demandeur de la carte et de l'inscrire sur ce document. Durant l'Occupation, l'apposition de la mention « Juif » sur les cartes d'identité sert aussi à rendre visible une sous-citoyenneté. Réclamée par l'autorité allemande et par les institutions vichystes spécialisées dans la traque des Juifs, cette mesure fait également l'objet d'une attention particulière de la part de certains fonctionnaires du ministère de l'Intérieur qui, en 1942, décident par exemple de favoriser la diffusion de machines perforatrices spéciales destinées à éviter toute altération de la mention « Juif » apposée sur les cartes d'identité. Dans le même temps, des fonctionnaires de la police française ne semblent nullement s'opposer aux investigations menées par des agents du Commissariat Général aux Questions Juives dans les fichiers départementaux des cartes d'identité en vue de retrouver des Français de confession juive à partir de leur nom patronymique<sup>10</sup>.

Si avec le rétablissement de la légalité républicaine toute forme de distinction entre citoyens est proscrite en matière d'encartement, il convient tout de même de signaler qu'un des objectifs motivant la création de la « carte nationale d'identité » en octobre 1955 est le contrôle des Français musulmans d'Algérie. En 1955, une circulaire « confidentielle » adressée par le ministère de l'Intérieur aux préfets détermine les

---

<sup>8</sup> Pour reprendre une expression formulée par Benedict Anderson dans *L'imaginaire national*, Paris, La Découverte, 1996, p. 19.

<sup>9</sup> Hubert Pérès, « Le village dans la nation française sous la Troisième République. Une configuration cumulative de l'identité » in Denis-Constant Martin (sous la dir.) *Cartes d'identité. Comment dit-on « nous » en politique ?*, Paris, PFNSP, 1994, p. 225.

<sup>10</sup> Cf. sur point Joseph Billig, *Le Commissariat général aux Questions juives (1941-1944)*, vol. II, Paris, éditions du Centre, 1957, p. 221.

dispositions qu'ils doivent systématiquement appliquer pour toute demande de carte d'identité émanant d'individus appartenant à cette catégorie de citoyens (saisine du préfet du lieu de naissance des requérants et envoi à la Direction générale de la Sûreté nationale d'un état récapitulatif des cartes délivrées à des Français nés en Algérie et domiciliés en métropole)<sup>11</sup>. Le contrôle préfectoral particulier dont ces derniers sont les seuls à faire l'objet est alors motivé par la recherche d'éventuels suspects ou d'individus dangereux qui chercheraient à s'affubler d'une fausse identité. De même, au cours des années 1990, le « durcissement » des conditions d'attribution de la carte nationale d'identité sécurisée décidé pour améliorer les performances du dispositif de délivrance de ce document s'effectue parfois au détriment du principe d'égalité entre les citoyens. L'obligation de produire un double justificatif de domicile avec des documents récents aura surtout pour effet de renforcer le processus de marginalisation dont sont victimes les citoyens « sans domicile fixe »<sup>12</sup>. Dans le même temps, la décision prise par le ministère de l'Intérieur de considérer chaque demande de carte nationale d'identité sécurisée comme une première demande aura une incidence directe sur d'autres catégories de citoyens : ceux nés en France de parents étrangers, ceux nés de parents naturalisés, ceux mariés avec un étranger ou encore ceux nés hors de métropole dans un territoire français au moment de leur naissance mais ayant ensuite accédé à l'indépendance. Pour plusieurs milliers d'entre eux, la présentation d'un extrait d'acte de naissance avec filiation sera jugée insuffisante par certains services de l'administration qui, afin de déterminer leur nationalité, exigeront la production d'un certificat de nationalité. De nombreux témoignages publiés dans la presse et une multitude de questions écrites au gouvernement rédigées par les députés sur ce thème montrent à quel point ces pratiques ont été très souvent mal ressenties par ces Français, indignés de faire l'objet de cette « xénophobie d'État au quotidien<sup>13</sup> » et de voir qu'on pouvait ainsi les considérer comme des citoyens de « seconde zone ».

## **RESISTANCES MULTIFORMES**

### **Résistances individuelles et collectives**

On ne comprend que difficilement les dispositifs d'encartement si on les considère comme des instruments de pouvoir imposés unilatéralement par une sorte d'État « Big Brother » à des citoyens complètement obéissants ou amorphes. Ces dispositifs doivent être appréciés au regard des résistances ayant jalonné le cheminement souvent mouvementé qui a conduit à leur progressive institutionnalisation. Historiquement, ces résistances revêtent des formes multiples et émanent d'acteurs très différents. Ce sont, par exemple, des résistances individuelles : la contrefaçon, la falsification ou encore les usurpations d'identité apparaissent comme autant de pratiques manifestant un refus des assignations identitaires de l'État. Bien d'autres stratégies individuelles de contournement ou de contestation des règles imposées par l'État existent encore. Actuellement, on pourrait mentionner le refus de certaines françaises de confession musulmane d'apparaître non voilées sur les photographies apposées sur leurs documents d'identité.

Les résistances revêtent aussi une dimension plus collective. On pense à certaines associations (des droits de l'homme ou de défense du statut des étrangers) ou à des journaux qui, de manière récurrente, s'évertuent à dénoncer les risques que font courir aux individus la mise en place de documents d'identité présentés comme liberticides. Certains syndicats entrent aussi dans cette catégorie : le Syndicat de la magistrature en France ou encore la CFDT ont, par exemple, au cours des années 1980, alerté les

---

<sup>11</sup> Circulaire « confidentielle » n° 481 du 7 décembre 1955, CAC 860 580 art. 7.

<sup>12</sup> Cf. Maryse Bresson, « Sans-adresse-fixe. Sans-domicile-fixe. Réflexion sur une sociologie des assistés », *Revue française des Affaires sociales*, n° 2-3, avril-septembre 1995.

<sup>13</sup> Expression utilisée par Maurice T. Maschino dans son article « Êtes-vous sûr d'être Français ? » publié dans *Le Monde diplomatique*, juin 2002, p. 7.

parlementaires sur les dangers inhérents à l'instauration de la première carte nationale d'identité informatisée. Ces résistances peuvent aussi émaner d'institutions étatiques : la CNIL, mais aussi le Médiateur de la République qui a pu jouer un rôle déterminant lorsque s'est posé le problème de la domiciliation des personnes sans domicile fixe évoqué précédemment. D'autres formes de résistances collectives sont encore à prendre en considération. Il s'agit par exemple des réseaux de résistance spécialisés dans la confection de faux papier durant l'Occupation. Depuis quelques années, dans un but de dénoncer la logique étatico-nationale, certains mouvements autonomistes ou nationalistes créent aussi pour leur adhérents ou sympathisants des papiers d'identité d'un modèle spécifique : Ligue Savoisiennne ou, plus récemment, le mouvement « Indipendenza » en Corse<sup>14</sup>.

Enfin, il convient de ne pas oublier que la question de l'encartement des Français peut encore être érigée en enjeu politique national et donner lieu à un affrontement partisan. Ainsi, en 1981, le gouvernement socialiste a, au motif que cela constituait un péril pour les libertés citoyennes, décidé de stopper la délivrance de la carte nationale d'identité informatisée instituée quelques mois auparavant par le gouvernement précédent.

### **Registres de dénonciation**

Hormis les formes de résistance qui visent à remettre en cause la logique même sur laquelle s'est construite l'État-nation, beaucoup ont pour fondement la nécessité de protéger les individus contre une « colonisation de leur vécu » par des instances étatiques présentées comme toujours plus inquisitoriales dans leurs entreprises d'encartement. C'est ici, en quelque sorte, l'aspect tyrannique de l'État *Big Brother* face à des individus démunis qui est dénoncé.

En France, plusieurs facteurs ont pu donner et donnent toujours du poids à ce type d'argument. Il faut, tout d'abord, évoquer le poids de l'héritage historique. Concernant les citoyens, une idée a, pendant longtemps, été évoquée de manière récurrente : il est intolérable de les soumettre à des formalités (les empreintes digitales notamment) initialement appliquées à des catégories d'individus considérées comme déviantes<sup>15</sup> ou stigmatisées comme dangereuses<sup>16</sup>. Le souvenir de la période de Vichy apparaît aussi déterminant, car les procédures d'identification ont alors joué un rôle majeur dans la répression des Juifs étrangers et nationaux.

Il convient également de faire allusion à l'aspect peu publicisé des enjeux relatifs à la mise en carte. Jusqu'alors en France, aucun débat d'envergure nationale n'avait jamais été spécifiquement consacré à la carte nationale : les décisions des pouvoirs publics empruntaient toujours la voie réglementaire. Parfois même, certains projets gouvernementaux ont pu revêtir un caractère totalement opaque alimentant tous les fantasmes : cela a notamment été le cas de la première carte nationale d'identité informatisée instituée en 1980.

On pourrait ajouter à cela, le caractère souvent évasif des discours de légitimation des dispositifs mis en place par les autorités. À cet égard, l'idée selon laquelle la rationalisation des procédures d'encartement des Français permettrait de lutter plus efficacement contre le terrorisme mériterait d'être rigoureusement démontrée.

---

<sup>14</sup> Cf. Xavier Crettiez, « Les cartes d'identité régionalistes Un instrument de contestation de la logique de l'État ? » in Xavier Crettiez et Pierre Piazza (dir.), *L'encartement des individus. Histoire et sociologie d'une pratique d'État*, à paraître à la Documentation française/ INHES en 2005.

<sup>15</sup> Sur mise en carte et « Bertillonage », cf. Pierre Piazza, « La fabrique "bertillonienne" de l'identité. Entre violence physique et symbolique », *Labyrinthe*, n° 6, printemps-été 2000.

<sup>16</sup> Cf. Pierre Piazza, « Au cœur de la construction de l'État moderne. Socio-genèse du carnet anthropométrique des nomades », *Les cahiers de la sécurité intérieure*, n° 48, deuxième trimestre 2002.

## Nouvelles craintes suscitées par la biométrie ?

En ce qui concerne la biométrie, on constate que les nombreuses formes de résistance qu'elle commence à susciter s'articulent souvent autour des thèmes précédemment évoqués. Toutefois, certaines spécificités peuvent être repérées en la matière, qui semblent exacerber les « crispations » autour de cette question.

La dimension transnationale de l'entreprise de biométrisation des titres d'identité (pourtant régulièrement présentée comme un acte de souveraineté propre à chaque État) paraît influencer fortement sur la nature des inquiétudes suscitées. Tout d'abord, il n'est pas évident de décrypter le processus par lequel s'est imposée la décision de biométriser les documents d'identité : quel est le rôle joué par les États-Unis, l'OACI (organisation de l'aviation civile internationale), le G8 et le G5, l'Union Européenne, les États ? La complexité de ce processus a pour effet de « brouiller » les enjeux auxquels il renvoie et d'alimenter les angoisses d'une partie des citoyens qui, jusqu'ici, pouvaient être amenés à considérer qu'on leur imposait des normes sans les consulter sur la question de leur bien-fondé.

C'est aussi la crainte de voir se constituer des méga-bases de données biométriques centralisées qui est souvent avancée (y compris des bases de données que des pays pourraient constituer sur des ressortissants qui ne sont pas les leurs). Ainsi, l'Association française IRIS (Imaginons un Réseau Internet Solidaire) insiste beaucoup sur ce point. Qui constituera ces bases de données ? Qui y aura accès et comment ? Ces bases seront-elles interconnectées ou croisées avec d'autres fichiers, notamment des fichiers gérés par des opérateurs privés<sup>17</sup> ? Autant d'interrogations qui renvoient, *in fine*, à la question du contrôle de ces énormes bases d'informations à caractère nominatif par des autorités de protection des données disposant d'un véritable pouvoir d'investigation et d'un financement à la hauteur de leurs missions de contrôle.

On dénonce en outre la foi aveugle en la technologie. C'est ici l'idée selon laquelle le processus de biométrisation des titres d'identité renvoie finalement à la volonté de faire prédominer des modes de preuves techniques ou scientifiques régulièrement présentées comme infaillibles. Elle suscite de nombreuses réactions allant de la simple interrogation à la franche hostilité. Tout d'abord, certains se demandent s'il est raisonnable d'aller dans ce sens, alors que certaines techniques biométriques sont encore loin d'être totalement fiables (qui peut affirmer aujourd'hui qu'une base contenant des millions de données le sera véritablement?) et paraissent pouvoir être contournées (fabrication de fausses empreintes digitales, possibilité de modifier le contenu des puces dans lesquelles sont insérées les données biométriques, etc.). Qu'arrivera-t-il, par exemple, aux individus dont les documents biométrisés ne seront pas reconnus lors d'un contrôle ? Pourront-ils porter réclamation ? Si oui, auprès de qui ? L'argument régulièrement développé (qui a d'ailleurs été quelquefois évoqué lorsque l'on a commencé à informatiser certains documents d'identité en France<sup>18</sup>) est le suivant : chaque individu ne risque-t-il pas d'être réduit à un ensemble d'équations qui le déshumaniseront totalement et le placeront dans une situation kafkaïenne en cas d'erreur de la machine devenue toute-puissante. Dès lors, certains (comme récemment 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.

Autre grande interrogation à l'origine de nombreuses réticences : la biométrisation des documents d'identité (visas, titres de séjour, passeports, cartes d'identité) est-elle

---

<sup>17</sup> Sur cette question aux États-Unis, cf. notamment Ayse Ceyhan, « La biométrie : une technologie pour gérer les incertitudes de la modernité contemporaine. Applications américaines », *Les Cahiers de la sécurité*, n° 56, à paraître en mars 2005.

<sup>18</sup> Cf. notamment le dessin humoristique publié dans *L'Express* du 7 février 1981.

justifiée au vu des finalités qu'on lui fixe ? Au regard des risques encourus, est-il bien nécessaire d'imposer à tous autant de contraintes ? Ainsi la CNIL semble considérer que la constitution de fichiers d'identité centralisés constitue un objectif disproportionné par rapport au phénomène marginal que constituent les usurpations d'identité. Ainsi, Tony Bunyam, président de l'ONG britannique Statewatch, estime que la lutte contre le terrorisme n'est qu'un habile prétexte permettant au gouvernement américain d'instaurer sournoisement un contrôle social massif, généralisé à l'ensemble de la planète. Les identifiants biométriques particuliers, dont l'imposition aux autres pays constitue une des priorités actuelles de Washington, seraient susceptibles d'être couplés à d'autres technologies - vidéosurveillance (voire observation satellitaire), bases de données et logiciels divers, etc. - qui constituerait *in fine* un dispositif ubiquitaire de « surveillance totale », tel que celui imaginé par les scénaristes du film « Ennemi d'État » (Tony Scott, 1998)<sup>19</sup>. Ce type d'indice ne fait qu'accroître les peurs qu'engendre la priorité accordée au « tout technologique ». Pour certains, on pourrait alors glisser progressivement d'une logique d'identification vers une logique de traçabilité conduisant à une remise en cause radicale de l'espace public anonyme (atteinte à la liberté d'aller et venir, à la liberté de manifester, etc.). Pour d'autres, le risque serait de voir, dans un contexte général de privatisation et de désengagement de l'État, des attributions relevant jusqu'alors du service public être déléguées à des acteurs privés avant tout guidés par des impératifs économiques de rentabilité.

**Pierre PIAZZA**

\* \* \*

---

<sup>19</sup> Cf. Jean-Paul Brodeur et Stéphane Leman-Langlois, « Surveillance totale ou surveillance fiction ? », *Les Cahiers de la sécurité intérieure*, n° 55, premier trimestre 2004.

## **II. Contribution de Thierry PIETTE-COUDOL, Avocat près la cour d'appel de Paris - 7 mars 2005**

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

La carte d'identité électronique fournit peut-être l'opportunité de mettre à plat la question de l'identité des personnes dans les NTIC. Surtout à un moment où les besoins d'authentification des utilisateurs se multiplient (blanchiment de l'argent sale, terrorisme, pédophilie, etc.) et où la traçabilité exercée à l'encontre des personnes peut constituer une atteinte à la vie privée ou aux libertés fondamentales.

Les relations entre les êtres humains nécessitent souvent la connaissance de l'identité de l'autre. L'identité repose sur plusieurs éléments dont le plus important est sans contexte le nom. Encore faut-il remarquer que le nom peut compter plusieurs niveaux de précision, le niveau le plus précis ou le plus officiel étant (désormais) le "nom de famille". Pourtant les relations sociales peuvent quelquefois se suffirent d'une reconnaissance de l'autre très rudimentaire (ex.: physionomie).

### **De l'anonymat à l'identité officielle**

Cette approximation existe... même dans le droit ! Un seul exemple, qui a dit que la connaissance de l'identité de l'autre était une des conditions essentielles à la formation des contrats ? Ces conditions traitent du consentement, de la capacité, de la cause, de l'objet... mais pas de l'identité (sauf les cas où la loi en dispose, spécifiquement, autrement). D'où l'anonymat dans certaines relations ou bien le pseudonyme ou encore le nom d'emprunt ou le nom usuel...

En dépit des réalités techniques, il faut rappeler que dans les NTIC, l'anonymat est de rigueur ! Les sources textuelles sont nombreuses au niveau français (code civil, Loi Informatique et Libertés modifiée, Loi sur la Sécurité Quotidienne, plan gouvernemental ADELE) et même au niveau européen (COM(97)503, divers directives dont celle sur la protection des données personnelles).

Pour en venir à la carte d'identité électronique (CIE), comment évaluer le niveau de précision nécessaire dans l'identité ? Par nature, la CIE doit être précise dans la connaissance (et la diffusion) de l'identité. C'est pourquoi l'identification sera dite "forte". L'identité de l'état civil constituera même un niveau minimal, puisqu'il est prévu de renforcer l'identification par des mesures biométriques ! Ce système devrait pouvoir être mis en œuvre –l'époque l'exige- à condition que son déploiement soit suivi à la loupe et à la lumière du respect des libertés individuelles.

### **Quel niveau d'identité dans le certificat embarqué ?**

Par contre ce qui nous fait souci (mais ce n'est qu'un risque) ce sont les blocs relatifs à la signature électronique, comme on peut le voir dans le document du ministère de l'intérieur "Le programme INES" :

- Le bloc "identification authentifiée du porteur " ou « identification certifiée » (par un code secret PIN) permettra d'accéder à des téléprocédures publiques ou privées (par exemple accès à son compte en banque...).
- Le bloc " signature électronique" (voir le glossaire) permettra (par un code PIN secret) de signer électroniquement des documents authentiques, soit à l'intention d'une e-administration, soit pour toute transaction électronique privée.

Or en matière de signature électronique, tout est dans le certificat. Il existe une typologie des certificats en classes selon la précision de l'identité demandée. La plus sûre est dite

"classe 3+" (présentation en face à face des papiers d'identité officiels à l'opérateur technique). Dans la classe 1 selon l'exemple américain, l'identité peut être une simple adresse électronique ; ceci peut être rapproché de la loi française qui prévoit qu'un certificat peut être donné sous un pseudonyme (!). [Autour de cette question, voir notre article "*L'identité des personnes, les certificats et la signature électronique*" au Jurisclasseur Communication et Commerce Electronique – janv. 2005, chr. 2).

### **Notre crainte...**

Dans le contexte d'identification forte de la CIE, le certificat embarqué dans la CIE sera certainement de classe élevée (ou de "niveau élevé" selon la typologie de l'ADAE dans la PRIS v2) (question subsidiaire : qui sera le certificateur ?).

La facilité de pouvoir utiliser le certificat embarqué dans la carte pourrait entraîner une utilisation systématique de ce certificat apportant ainsi aux relations électroniques une précision qui n'est pas demandée par le Droit.

### **Quel besoin d'une identification forte pour les téléprocédures ou le commerce électronique ?**

La question est posée : quel besoin, quel intérêt, quel enjeu pour signer électroniquement avec cette classe de certificat une téléprocédure ? 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 – A combiner avec les disposition du projet d'"ordonnance téléservices" qui fait actuellement l'objet d'une consultation publique).

Bien plus, pourquoi une "identification authentifiée" ou "certifiée", pour accéder à son compte bancaire (cela marche très bien depuis le Minitel, merci) ou 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 ?

### **Quel besoin d'une identification forte pour une signature d'entreprise ?**

Enfin encore un détail (?), pas de signature des personnes morales en France. Pour la signature électronique comme pour la signature manuscrite, c'est une personne physique autorisée qui signe pour le compte de la personne morale (on peut déjà le voir dans la politique de certification-type du MINEFI). Dans ce cas, pourquoi donner les meilleurs gages de son état civil lorsqu'il s'agit d'engager l'entreprise. Ce qui importe est naturellement d'en être membre (voir sur ce point le guide "la qualité professionnelle dans la signature électronique" de l'association IALTA France).

**Thierry PIETTE-COUDOL**

\* \* \*

### **III. Contribution de Youval ECHED, Secrétaire Général de l'Académie Internationale des Droits de l'Homme - 7 mars 2005**

Par **Youval ECHED**

Secrétaire Général de l'Académie Internationale des Droits de l'Homme  
Administrateur et Trésorier de L'Association Française du Net (AFNET)

#### **IDENTITE – LIBERTE – TRACABILITE : UN NECESSAIRE MARIAGE DE RAISON ?**

##### **1. Introduction**

L'Identité Numérique prépare son déploiement tant attendu. Elle était promise comme une étape décisive de l'e-administration et un support permettant de diffuser largement la Signature Electronique. D'aucuns considèrent qu'elle lancera enfin énergiquement le marché et l'Industrie de la Confiance dont on parle tant depuis cinq ans, en parallèle de la dématérialisation des échanges.

Et comme le plongeur retient son souffle sur la planche à sauter, voici que nous nous sentons interrogés par un salutaire paradoxe : La « Confiance-Ethique » contre la « Confiance- Surveillance », mon identité « instrument-de-ma-liberté-et-de-ma-sécurité », contre mon identité « instrument-de-ma-traçabilité ».

Et le débat d'évoquer de manière indifférenciée tantôt la traçabilité des objets, tantôt celle des personnes. Certes l'urgence est de fixer un cadre éthique à l'usage des formes électroniques de procédures et média - par ailleurs anciens - d'identification des personnes. Mais est-ce l'Identité Numérique qui est la cause réelle de nos craintes ?

Cet article tente de faire la part des choses entre l'identité et la confiance d'une part, la traçabilité et l'archivage d'autre part. Il analyse enfin le rapport de fond de ces éléments à l'esprit de nos libertés publiques et individuelles.

##### **2. La Confiance Electronique, une industrie fondée dès l'origine sur la traçabilité.**

La confiance est actuellement un enjeu dominant de nos échanges économiques et de la modernisation de notre société. Le parlement n'a-t-il pas adopté en 2004 la loi sur la confiance dans l'économie numérique et ne vient-il pas d'adopter en 2005 un texte de loi « pour redonner confiance au consommateur<sup>20</sup> » ?

Elle est au cœur des évolutions de nos dispositifs de régulation des relations économiques, sociales ou administratives.

Le climat sécuritaire général ne favorisant guère la prise de risques, les nouveaux référents de confiance se forment en marchant avec l'appui de multiples mécanismes de certification et de réassurance de la responsabilité individuelle, complexifiant parfois les cadres juridiques des relations d'échange.

Dans un tel environnement économique, oscillant de fait entre désir de confiance et sentiment irrationnel de défiance, renforcé par un contexte technologique fortement évolutif de mobilité et de multi-modalité des supports d'échange (papier, électronique,...), le besoin d'assurer voire d'améliorer la traçabilité des flux devient l'une des motivations essentielles de la modernisation de nos échanges ; Une autre étant bien évidemment d'apporter un confort et une performance accrue dans les relations et transactions devenues « multi-canales » .

---

<sup>20</sup> Loi Châtel, consultable sur le site de Légifrance. Loi 2005-67 du 28 janvier 2005.

A ce titre, un des enjeux des back offices dématérialisés ne serait-il pas tout simplement de mettre en oeuvre les obligations de traçabilité, dont les contraintes réglementaires sont de plus en plus nombreuses (Aérospatial, Défense, Nucléaire, Pharmaceutique, Alimentaire, Santé, Financier, Transport, Environnement, ... ) ?

Et derrière ces obligations, l'objectif ne serait-il pas d'assurer les moyens de garantir en permanence **l'imputabilité et l'auditabilité des flux** même et surtout électroniques ?

Il apparaît alors que l'identité numérique peut devenir un des facteurs clés dans les exigences d'imputabilité des flux. Il serait dès lors tentant de lui faire porter toutes les appréhensions collectives inconscientes que le grand public éprouve à la découverte progressive du climat de traçabilité dans lequel notre société en perte de repères évolue depuis quelques années déjà.

Les tenants de cette idée invoquent cette interprétation comme découlant directement de la loi du 13 mars 2000, précisant aux articles 1316 et Suiv. du Code Civil, que la preuve électronique est admissible comme preuve littérale à condition que son émetteur soit identifié de manière certaine (**imputabilité**) et que sa conservation intègre en soit garantie. Cette conservation implique que la trace qui en résulte doit être dotée d'une signification restituable et intelligible (**auditabilité**), comme l'explique plus en détail le commentaire de doctrine juridique de Maître Eric A. CAPRIOLI cité en référence plus avant.

Or la tendance à la traçabilité systématique tire probablement ses origines ailleurs. La dématérialisation des flux, fait émerger nombre de nouveaux opérateurs de médiation, publics ou privés. De plus le cadre concurrentiel mondial et les décisions prises en G8<sup>21</sup> contribuent à fragiliser les spécificités nationales de la régulation de nos échanges et de nos dispositifs de droit. La question de savoir quelle forme il leur sera donné demain et quelles garanties éthiques préserveront l'esprit de l'équilibre dynamique des libertés tant individuelles que collectives est dès lors plus que pertinente. Celle de savoir jusqu'où nous pourrions faire valoir les cadres de valeurs auxquels nous sommes historiquement attachés en est une autre.

Côté avantages, une bonne traçabilité représente un espoir évident de surcroît d'efficacité pour « la transitique »<sup>22</sup> de nos chaînes industrielles, financières ou administratives. En terme de « Risk Management » la voie serait ouverte à une meilleure « prédictibilité » de la qualité générale des échanges, un contrôle accru des fraudes potentielles et donc la possibilité de procéder progressivement à une logique de vérification *a posteriori* plutôt que systématiquement *a priori*, accélérant et facilitant du même coup les échanges et les conclusions de transactions commerciales ou administratives, avec en bout de chaîne un meilleur service potentiel.

Côté négatif, la recherche systématique de traçabilité et l'amélioration des capacités à restituer les éléments de preuve conservés cautionneraient la tendance sous-jacente de notre société à devenir de plus en plus judiciaire, et à identifier en toute circonstance **les responsables et les fautes éventuelles**. Cette dernière tendance tue dans l'œuf bien des initiatives entrepreneuriales potentielles tant publiques que privées. Et il est statistiquement reconnu que moins il y a prise de risques, moins il y a d'opportunités de ruptures et d'innovation et moins il y a création de nouveaux gisements de croissance. De manière caricaturale ne serait-on alors pas tenté de dire que la croissance est molle...par ce que nous faisons tout pour qu'elle le soit ?

---

<sup>21</sup> Voir par exemple la [conférence](#) du G8 intitulée "Un dialogue secteur privé - pouvoirs publics sur la sécurité et la confiance dans le cyberspace ou encore les 29 principes directeurs du G8 portant sur la traçabilité des flux financiers", les coopérations du G8 en matière de cybercriminalité, etc...

<sup>22</sup> Terme fréquemment usité pour désigner la science du contrôle et de la régulation des Supply Chain

On comprend de ce qui précède que la traçabilité comme dispositif de confiance, interroge autant l'archivage des éléments de preuve que l'identification de l'émetteur, voire de l'archivageur. Quelles que soient les modalités d'Identification numérique des Objets et des Personnes, des moyens seront en place et le lancement en cours de l'Identité Numérique n'a pas pour objet de modifier fondamentalement cette donnée de base. Sauf à s'exclure du marché mondial, ce qui est proprement impensable.

Il faut donc avant d'imputer quelques craintes que ce soit à l'Identité Numérique, comprendre quels sont les enjeux de la confiance et de la traçabilité.

### **3. De l'éthique de la gestion des traces à la pédagogie du changement**

Les aspects juridiques et organisationnels de la traçabilité, et de l'archivage implicitement sous-tendu sont un domaine à part entière en pleine maturation. Nous ne l'aborderons pas ici sauf pour rappeler que le libre accès aux traces pour chaque citoyen est un enjeu essentiel dont le cadre éthique doit être complété et diffusé largement.

Il convient de considérer à ce titre que les textes sur la protection des données personnelles sont en pleine mutation (loi du 6 août 2004). Les décrets d'application sont en cours de parution et il n'est donc pas encore possible de faire un travail prospectif sur cette question à ce stade.

En particulier une donnée majeure affectera le destin de la conservation et de l'accessibilité d'une information : il s'agit évidemment des conditions de son rattachement au domaine strictement privé ou à un domaine susceptible de ressortir de l'intérêt général voire de l'état. On voit tout de suite que cette question sensible est variable et éminemment politique. Le cabinet noir de 1804 du Ministre Fouché a de toutes manières montré les limites d'une telle dialectique. Ce n'est pas l'instrument qui porte le risque mais le penchant humain à en dévoyer l'usage. Ce débat a plus de 2500 ans. Et la roue existe malgré les chars offensifs.

De fait, elle est loin d'être résolue la quadrature du cercle qui permettrait à la fois de garantir la liberté fondamentale du droit à la sécurité du citoyen, justifiant à ce titre le droit corollaire d'investigation de l'état sur tout ce qui s'échange<sup>23</sup>, et le droit tout aussi fondamental à la protection de son secret par le même citoyen.

**Sauf à ce que dans un sursaut, la collectivité se réveille de son cauchemar sécuritaire et comprenne que la recherche d'un optimum en ce sens, constitue, dans l'esprit, une démarche contraire à toute forme d'apprentissage de la responsabilité et de la maîtrise du risque.** La première, donne priorité à la conservation des acquis. La seconde, fait le pari du progrès et du mouvement...à condition que celui-ci soit compris par le plus grand nombre. C'est là que la pédagogie devient un facteur essentiel du succès.

Justement, à la question de savoir quelles informations stocker sur le support d'Identification Numérique, la tentation de l'intelligence est toujours d'innover, d'améliorer et de profiter de l'opportunité du mouvement. Or **le problème auquel nous sommes en premier lieu confronté, n'est-il pas un changement pur de média, et un souci d'appropriation le plus large possible ?** Il serait dans un premier temps raisonnable de ne faire qu'une translation à la fois, du papier au numérique. On pourrait admettre la biométrie comme une forme moderne de photo « biologique » et la signature électronique comme un moyen d'identification légal aux fins de transactions

<sup>23</sup> Voir notamment les débats relatifs à la «Loi n° 2004-204 du 9 mars 2004, dite Loi Perben 2», et les usages des NTIC aux fins d'investigation judiciaire, en particulier les articles 706-82, 706-96, 74-2 du NCPP, ou encore la **loi Informatique et Libertés (LIL)** article 9 - possibilité à certaines personnes morales de constituer un fichier d'infraction permettant de recenser, via notamment leur adresse IP, les personnes qui se livreraient au téléchargement de fichiers illégaux, dont les usages en P2P.

électroniques. Mais il conviendrait probablement pour le reste de se limiter aux données caractérisant l'identité dans un premier temps. Tout viendra ensuite en son temps.

#### **4. De l'Identité Numérique comme facteur du développement des libertés ?**

Si l'on reprend la brillante démonstration du rapport « La Confiance et l'Etat » publié par Henri Prévôt avec le Conseil Général des Mines<sup>24</sup>, le rapport à la Confiance n'est en somme qu'une perception complexe du rapport au Risque. On en déduit que l'Identité Numérique, dont l'objet est de rassurer celui qui reçoit quant à la véritable identité de celui qui émet, intervient en fait comme facteur minorant du risque.

Et paradoxalement, ce qui augmente la capacité de prise de risque, augmente *de facto* le champs des possibles, donc indirectement celui des Libertés.

François Dubet et Danilo Martuccelli (EHESS - CNRS)<sup>25</sup> rappelaient en 1998 : « *L'identité dans l'architecture de la société française est historiquement porteuse des principes d'égalité et de liberté : L'égalité prévalant sur le domaine public, la liberté garantissant plutôt le droit de séparer le domaine public du domaine privé* ».

Danilo Martuccelli ajoute en substance «...*la modernité a fait exploser le concept d'identité absolue et universelle au profit d'une pluralité d'identités comme autant de facteurs d'attente de reconnaissance des différentes communautés auquel l'individu se rattache culturellement* ».

**On ne peut dès lors nier que l'Identité, fût-elle numérique, est un facteur d'intégration et de rattachement à un corpus commun et à une culture commune de la pratique des libertés publiques.**

C'est donc l'ensemble du dispositif qu'il faudrait maintenant décrire pour replacer le débat en cours dans la ré-affirmation des principes fondateurs de l'architecture de notre collectivité.

**En somme, l'Identité Numérique, cela n'est ni moderne ni technologique et encore moins contraint par quelque système de contrôle que ce soit...ce serait d'abord fondateur de la continuité de l'architecture de nos libertés publiques.**

Les liens à la traçabilité qui fonderaient nos craintes sont indirects, réels mais inéluctables, et, dans tous les cas, indépendant de tout effet de causalité première.

Le problème du respect de la vie privée est un thème fort médiatique certes. Mais la liberté à préserver est-elle différente lorsqu'il s'agit de notre identité ? De nos traces nombreuses dans l'industrie consumériste au travers de la Relation Client et des cartes de fidélité pour le « scoring » de ma qualité de consommateur ? ou encore de mes traces en télécommunications, où la Triangulation GPS est utilisée « seulement » sur commission rogatoire... ?

---

<sup>24</sup> La Confiance et l'Etat, Etude sur la structure cognitive de la confiance : Groupe d'Etude du CGM, première communication à l'EHESS, avril 2004 en collaboration avec Louis Quéré. La confiance et la sécurité n'existent pas en tant que tels mais comme facteurs de la motivation à assumer ou refuser l'action et la prise de risque associée.

<sup>25</sup> « Dans quelle société vivons-nous ? » François Dubet et Danilo Martuccelli - Seuil 1998 pp197 et suiv. L'Identité Publique du citoyen devient donc un domaine d'identification et de reconnaissance sociale au regard de l'Etat comme gestionnaire in fine de la collectivité publique. Ses travaux montrent combien le paradoxe est saisissant de voir des exclus considérer leur identité officielle comme une reconnaissance de fait de leur existence publique, autant que de voir des personnes bien intégrées préférer la liberté de systèmes de reconnaissance privée, et déconsidérer leur besoin de reconnaissance publique.

De fait le respect de la personne serait par exemple de lui dire que la traçabilité est une donnée incontournable de la vie économique occidentale actuelle et que le respect de la vie privée serait

- de lui laisser le choix entre un titre électronique ou non,
- de lui signaler dans les applications que celle-ci produit une trace.

Et d'accompagner ces choix par un cadre éthique simple qui recréerait le ciment social et fonderait clairement l'esprit des usages des moyens d'identification. A ce moment la personne pourrait choisir d'utiliser son titre électronique en connaissance de cause...le pari étant que dès que le bénéfice serait perçu comme grand, le choix sera fait d'en accepter l'usage courant.

Il est instructif de se rappeler que ce débat a eu lieu exactement dans les mêmes termes pour la Carte Bleue à Puces il y a 20 ans. Certains pays avaient alors refusé la puce.

**In fine, la liberté est-ce l'absence de contraintes ou le libre choix des contraintes ? De Socrate à aujourd'hui la réponse à cette question n'a pas vraiment évolué. Dans notre culture universaliste, le libre choix et la responsabilité ont partie liée et constituent ensemble l'un des piliers de ce que l'on appelle la dignité humaine.**

**Youval ECHED**

\* \* \*

#### **IV. Contribution d'Arnaud BELLEIL du groupe « Identité Numérique » de la Fondation Internet Nouvelle Génération - 7 mars 2005**

Par **Arnaud BELLEIL**

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

#### **DEUX REFLEXIONS SUR LA CARTE D'IDENTITE ELECTRONIQUE**

##### **CNIe : trop beau pour être simple ?**

La carte d'identité électronique devrait permettre d'atteindre plusieurs objectifs. C'est ce qui fait l'intérêt du projet mais peut-être aussi sa complexité, donc sa potentielle fragilité. En forçant un peu le trait, il serait possible de soutenir que les objectifs, ou arguments, en faveur du projet carte d'identité électronique sont, de façon non exhaustive, les suivants :

- répondre aux exigences de l'OACI et des autorités américaines en matière de titres d'identité sécurisés de nouvelle génération ;
- sécuriser l'identité (contrôle des flux migratoires, lutte contre l'usurpation d'identité) ;
- offrir une clé d'accès aux téléservices sécurisés du secteur public ;
- offrir une clé d'accès sécurisé à des téléservices sécurisés du secteur privé ;
- faire un saut technologique pour rendre obsolètes les faux papiers en circulation ;
- profiter du changement de génération technologique pour rendre payant ce qui était gratuit ;
- aider l'industrie française (ou européenne) de la carte à puce ;
- aider l'industrie française (ou européenne) de la biométrie et plus spécifiquement l'industrie des solutions à base d'empreintes digitales ;
- aider l'industrie française (ou européenne) de la signature électronique ;
- faire moderne, au moins autant que les belges ou les estoniens ;
- etc.

Il sera difficile de tout faire en même temps. La diversité des objectifs du projet risque d'être à la fois un facteur de complexité (donc de délais et de surcoûts) et de susciter méfiance et confusion au sein d'une partie de l'opinion. Ce serait alors prendre le risque de fragiliser durablement une évolution souhaitable. Sans doute faudrait-il s'en tenir à un projet simplifié avec un objectif prioritaire clairement affiché, par exemple, moderniser les titres d'identité pour réduire le nombre de faux papiers en circulation (ou le nombre de « vrais » papiers en possession de « mauvaises » personnes). Pour l'accès sécurisé aux services privés en ligne, il n'est sans doute pas indispensable de mobiliser toute la puissance de l'Etat. Il a plus à perdre qu'à y gagner.

##### **CNIe : une technologie de protection de la vie privée ?**

Pourtant, si les promoteurs du projet acceptent de prendre en charge la complexité résultant de la diversité des objectifs, il est alors possible d'en rajouter un de plus. La future carte d'identité électronique ne pourrait-elle pas être envisagée comme une technologie de protection des données personnelles au service du citoyen ; une sorte de coffre-fort électronique portatif ?

Ce serait déjà le cas si certaines des données personnelles étaient « enfouies » dans la puce au lieu d'être exposées, comme c'est le cas aujourd'hui, à la vue de tous. Les caissières des hypermarchés, lors des paiements par chèque, ont aujourd'hui accès à la date et au lieu de naissance du porteur et à une adresse. Est-ce véritablement indispensable ? En outre, l'utilisateur de la carte pourrait disposer d'une relative maîtrise

sur ses données personnelles en ayant la possibilité de procéder à des mises à jour, c'est-à-dire d'exercer son droit d'accès et de rectification prévu par la loi informatique et libertés. Cette idée figurait explicitement dans le Livre Blanc *Administration électronique et protection des données personnelles* de février 2002 (rapport Truche). Depuis, force est de constater que les préoccupations sécuritaires ont fait passer ce type de réflexions au second plan.

Enfin, une des options possibles pour concilier sécurité (de l'Etat et des organisation) et confiance (des citoyens) serait de faire en sorte que la carte électronique du citoyen 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 ne nationalité française, qu'il possède des droits (par exemple le droit de conduire, de chasser ou de pêcher) ou qu'il n'est pas déchu de certains droits (ne pas être interdit de casino, physique ou en ligne) sans avoir pour autant à justifier de son identité.

Une carte électronique du citoyen qui ne soit pas obligatoirement une carte d'identité : ce ne serait ni simple, ni économique. Mais la simplicité et la maîtrise des coûts sont-ils véritablement des critères essentiels pour le projet ?

**Arnaud BELLEIL**

\* \* \*

## **V. Contribution de Cyril ROJINSKY, Avocat au barreau de Paris - 7 mars 2005**

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

Je voudrais ici, dans le cadre de ce débat sur la carte d'identité électronique, insister non pas sur la question de l'anonymat ou sur la protection des données personnelles – toutes choses essentielles, bien entendu – mais sur le risque d'un nouveau mélange des genres entre la fonction régalienne qui consiste à attribuer et à garantir l'identité de chacun, et les éventuelles applications privées, commerciales ou non, qui pourraient être associées à ces nouveaux outils d'identification des personnes.

L'exemple belge (voir en annexe, ci-dessous) est particulièrement frappant à cet égard. Qualifiée « *d'étape historique vers un Internet plus sûr* », nous voyons un gouvernement européen accepter l'intégration de services en ligne privés au sein même de la carte d'identité électronique qu'il est d'ailleurs l'un des premiers à rendre progressivement obligatoire.

Une telle évolution interroge l'articulation entre le rôle de l'Etat – gardien des libertés, mais aussi garant de l'intérêt général – et celui des différents producteurs de solutions techniques, dont la société Microsoft n'est qu'un exemple parmi bien d'autres possibles.

Il faut donc insister : un titre national d'identité, électronique ou non, n'est pas un ticket de métro, une carte de téléphone, un relevé bancaire, ou un coupon d'achat de grand magasin. Il matérialise, il 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'Etat à cet égard.

Or l'exemple de la Belgique, précédemment cité, n'est pas un anachronisme lointain. Le ministère français de l'Intérieur, dans sa note du 31 janvier 2005 sur le programme INES (« *identité nationale électronique sécurisée* ») indique en effet qu'il est prévu de doter cette future carte « *de ces fonctionnalités qui seront valables pour toutes les administrations et tous les services financiers ou commerciaux sur Internet* ».

Il y a donc bien une confusion entre *identité* et *identification*. Or l'identité légale n'est pas une simple fonction, mais un principe qui doit demeurer autonome.

**Cyril ROJINSKY**

### **Annexes :**

#### ***Sources et liens :***

<http://fr.news.yahoo.com/050201/1/4915w.html>

[http://www.microsoft.com/belux/fr/press/info/info.asp?contact=no&mar=/belux/fr/press/info/billg\\_eid.html&xmlpath=/Belux/fr/press/inc/billg\\_eid.xml&rang=0](http://www.microsoft.com/belux/fr/press/info/info.asp?contact=no&mar=/belux/fr/press/info/billg_eid.html&xmlpath=/Belux/fr/press/inc/billg_eid.xml&rang=0)

\* \* \*

## **VI. Contribution de l'Association pour la Promotion et la Recherche en Informatique Libre (APRIL) - 23 mars 2005**

Par l'**APRIL**

L'Association pour la Promotion et la Recherche en Informatique Libre (APRIL)<sup>26</sup> est une association à but non lucratif régie par la loi du 1er juillet 1901. Elle a pour objet d'engager toute action susceptible d'assurer la promotion, le développement, la recherche et la démocratisation de l'informatique libre

### **SUR LES OUTILS D'AUTHENTIFICATION ET DE SUIVI DES BIENS ET DES PERSONNES**

La proposition actuelle de création d'une Carte Nationale d'Identité Électronique (CNIE) survient dans un **contexte de généralisation de technologies permettant d'assurer le suivi ou l'authentification de biens ou de personnes**, telles que les *étiquettes RFID*<sup>27</sup> ou le passe *Navigo*<sup>28</sup> de la RATP.

Les **étiquettes RFID** permettent par exemple aujourd'hui de **suivre les mouvements des biens** dans lesquelles elles sont insérées, offrant de nouvelles facilités logistiques **mais** donnant **également** les moyens de suivre les mouvements et comportements des **citoyens-consommateurs**<sup>29</sup>.

La **RATP** a introduit il y a quelques années le **passe *Navigo***, badge électronique destiné à remplacer la carte orange, permettant une **authentification sans contact** aux portiques, mais permettant également, du fait des choix de conception opérés par la RATP, de **tracer les mouvements d'un porteur dans son réseau**<sup>30</sup>.

On le voit, **ces technologies sont porteuses du meilleur**, en offrant de nouvelles facilités à leurs utilisateurs, **et du pire** donnant la possibilité de suivre tous les mouvements de leurs porteurs.

### **A PROPOS DE LA CARTE D'IDENTITE ELECTRONIQUE**

Le débat sur la carte d'identité survient donc dans un contexte où toutes **les implications de ce type de technologies n'ont pas encore été prises en compte par la puissance publique**.

Dans l'éventualité de l'instauration d'une CNIE, sur la pertinence de laquelle elle n'a pas pour objet de se prononcer, **l'APRIL invite le gouvernement à établir de hauts standards en matière d'interopérabilité (fait que plusieurs systèmes, qu'ils soient identiques ou radicalement différents, puissent communiquer sans ambiguïté<sup>31</sup>), de sécurité et de transparence des systèmes d'informations concernés**. Rappelant que sécurité n'est pas obscurantisme, comme l'illustre le crackage

---

<sup>26</sup> Association pour la Promotion et la Recherche en Informatique Libre APRIL – <http://april.org>

<sup>27</sup> Fondation Internet Nouvelle Génération : Rfid : entre mythes et réalités, la nécessité du débat - [http://www.fing.org/index.php?num=4560\\_2](http://www.fing.org/index.php?num=4560_2)

<sup>28</sup> RATP : Navigo - <http://www.ratp.fr/corpo/service/navigo.html>

<sup>29</sup> 01net : Étiquettes radio : la CNIL tire la sonnette d'alarme : <http://www.01net.com/article/224128.html>

<sup>30</sup> 01net : Le billet électronique Navigo prend la Carte Orange : La CNIL notait ainsi que « *la collecte et le traitement des données relatives aux déplacements des personnes, sous la forme de la date, de l'heure et du lieu de la validation du titre de transport via une borne de contrôle en entrée ou sortie du réseau de transport, sont susceptibles de porter atteinte à la liberté d'aller et venir et au droit à la vie privée lorsque ces données sont associées à un élément permettant d'identifier la personne concernée, en l'occurrence le numéro de la carte.* » - <http://www.01net.com/article/269617.html>

<sup>31</sup> Wikipedia : définition de l'interopérabilité - <http://fr.wikipedia.org/wiki/Interop%C3%A9rabilit%C3%A9>

il y a quelques années des codes des cartes bleues<sup>32</sup>, l'APRIL invite donc le gouvernement :

- **à ne recourir qu'à des standards ouverts** tels que définis dans l'article 4 du chapitre 1er du titre 1 de la Loi sur la Confiance dans l'Économie Numérique<sup>33</sup> ;
- **à diffuser les implémentations de référence** des couches logicielles permettant d'accéder aux différents types de données contenues par la CNIE sous des licences de logiciels libres.

Le recours à des **technologies de cryptologie librement implémentables, exemptes de tout brevet**, permettrait par exemple d'**allier un haut niveau de sécurité à la nécessaire transparence du dispositif**.

On appelle logiciel libre des logiciels dont les licences accordent les quatre libertés suivantes à leurs utilisateurs :

- **Utilisation** : la liberté d'utiliser le logiciel, pour quelque usage que ce soit.
- **Étude** : la liberté d'étudier le fonctionnement du programme, et de l'adapter à vos propres besoins. L'accès au code source est une condition pour tout ceci.
- **Redistribution** : la liberté de redistribuer des copies de façon à pouvoir aider votre voisin.
- **Modification** : la liberté d'améliorer le programme, et de diffuser vos améliorations au public, de façon à ce que l'ensemble de la communauté en tire avantage. L'accès au code source est une condition pour tout ceci.

Des logiciels libres tels que le système d'exploitation GNU/Linux<sup>34</sup> ou la suite bureautique OpenOffice.org sont aujourd'hui largement utilisés par les administrations<sup>35</sup>, les entreprises et les particuliers.

En procédant ainsi, le gouvernement :

- ne faussera pas la concurrence en ne donnant pas la primauté à un acteur commercial et en permettant à tous d'accéder sur un pied d'égalité aux implémentations de référence ;
- donnera à tous les citoyens les outils leur permettant de s'assurer de l'innocuité des titres d'identité électroniques, par exemple en termes de stockage de données ou d'accès non désirés.

Il est intéressant de noter que des préoccupations similaires en matière de respect de la vie privée avait conduit il y a quelques années au développement d'un logiciel de lecture d'étiquettes RFID<sup>36</sup>. En adoptant de tels standards, le gouvernement démontrerait de

<sup>32</sup> 01net : La peine de Serge Humpich confirmée en appel -

<http://www.zdnet.fr/actualites/internet/0,39020774,2061907,00.htm>

<sup>33</sup> Legifrance : Loi sur la Confiance dans l'Économie Numérique, Titre 1er, chapitre 1er, article 4 : « *On entend par standard ouvert tout protocole de communication, d'interconnexion ou d'échange et tout format de données interopérable et dont les spécifications techniques sont publiques et sans restriction d'accès ni de mise en oeuvre.* » - <http://www.legifrance.gouv.fr/WAspad/UnTexteDeJorf?numjo=ECOX0200175L>

<sup>34</sup> Exemples de systèmes GNU/Linux :

- la distribution française MandrakeLinux : <http://www.mandrakelinux.com/fr/>

- la distribution communautaire Debian : <http://www.debian.org/index.fr.html>

<sup>35</sup> 01net : Administration centrale : 225 chantiers ouverts - <http://www.01net.com/article/263192.html>

<sup>36</sup> Transfert.net : Les étiquettes "intelligentes" ont désormais leur logiciel libre - <http://www.transfert.net/a9073>

manière claire la prise en compte de certains arguments des organisations soucieuses de la protection des libertés individuelles et contribuerait donc à l'adoption rapide d'une éventuelle CNIE.

**APRIL**

\* \* \*

## VII. Contribution d'Alain DAMASIO, écrivain - 23 mars 2005

Par d'Alain DAMASIO

Ecrivain et scénariste, l'auteur de *La Zone du dehors* et de *La Horde du Contrevent*

### 0. La charpente branlante

Dans la stratégie discursive, plutôt inconsistante, qui accompagne le projet de carte nationale d'identité électronique (CNIE), quatre justifications sont apportées :

- ▶ La première, la plus probante, insiste sur l'insuffisante sécurisation des titres actuels ;
- ▶ La seconde évoque la lutte contre le terrorisme et tente d'inscrire le projet français dans une mouvance européenne, en se gardant bien de stipuler ce qu'il doit à la pression sécuritaire américaine qui entend faire de la biométrie un principe généralisé de fichage ;
- ▶ La troisième, dérisoire et démagogique, annonce une simplification administrative pour une « contrainte » qui exige aujourd'hui du citoyen une heure de son temps tous les dix ans ;
- ▶ La quatrième enfin, dénoncée par de nombreux spécialistes, veut faire de la carte d'identité un outil de certification électronique pour les transactions publiques et privées en ligne.

Qu'il faille démonter, à la main et poutre à poutre, pareille charpente branlante, nous semble une première, nécessaire, étape — avant de s'attaquer à la construction même d'un édifice — l'identité étatico-certifiée — qui nous paraît inapproprié aux enjeux d'une démocratie avancée.

### 1. Les terroristes encartés vous disent merci !

Commençons par la farce, cette fameuse lutte contre le terrorisme, dont Pierre Piazza, dans son excellente contribution, suggère avec doigté que « *l'idée selon laquelle la rationalisation des procédures d'encartement des Français permettrait de lutter plus efficacement contre le terrorisme mériterait d'être rigoureusement démontrée* ». On ne saurait moins dire, et l'on peut même supputer, avec une très forte probabilité, que les terroristes sont précisément ceux qui, face à une carte d'identité électronique *non obligatoire*, seront les derniers à l'adopter. Ou le feront-ils que ce sera sous une fausse identité de départ dûment validée par les procédures nouvelles, avec des empreintes qu'on peut facilement imaginer greffées sous les doigts. Sans verser dans la science-fiction qui m'est chère, ni imaginer de chirurgie plastique, deux limites invalident l'espoir de lutter adéquatement contre le terroriste grâce aux nouveaux titres :

- Le premier est ce caractère *non obligatoire* de la nouvelle carte qui prorogera les fraudes actuelles pour ceux qui le souhaitent ;
- Le second est l'impossibilité concrète, même si la procédure était décrétée obligatoire, d'obtenir d'une cinquantaine de millions de Français le passage à la CNIE, sauf à échafauder des procédures totalitaires et coercitives insupportables au citoyen honnête.

Le projet INES sera donc inopérant et inefficace face aux terroristes. Il le sera tout autant face aux fraudeurs anciens et nouveaux, aux usurpateurs et aux contrefacteurs qui continueront à utiliser les anciens titres. Certains fraudeurs pourront même se payer le luxe d'en obtenir des flambant neuf « sécurisés » sous leur fausse identité actuelle. Avec une greffe simple de peau sur la dernière phalange, ils pourront même doubler ou tripler cette identité pour leurs besoins d'ubiquité.

## 2. L'État, nouveau service privé

Passons à l'argument « utilitaire », à prétention moderniste, de certification électronique de l'identité. Deux contributions très pertinentes (celle de Thierry Piette-Coudol et celle de Cyril Rojinsky) le battent en brèche.

Le premier rappelle que le commerce est depuis l'antiquité une affaire de confiance, un contrat tacite ou explicite, qui ne nécessite en rien une authentification forte des contractants, et qui peut même très bien se faire sous pseudonyme.

Le second met en garde contre la confusion des genres entre un État régalien chargé de certifier l'identité et un État libéral qui serait désormais le fournisseur implicite d'une *identification* destinée à faciliter le développement de services commerciaux en ligne. L'État est un service public qui doit défendre l'intérêt général, pas un ersatz, d'ailleurs monopolistique, de service privé qui devrait venir au secours de la défiance des consommateurs envers le commerce électronique !

À ces arguments me semblent s'ajouter des incohérences sécuritaires concrètes. En quoi l'accès à son compte bancaire ou l'achat d'un disque sur internet nécessitent-ils une authentification aussi forte que la biométrie ? Qui empêchera un malin « d'emprunter » ma carte d'identité pour acheter sur le net ? Il lui faudra taper le code PIN ? Dans ce cas, qui garantit que ces codes, pour le citoyen honnête, ne seront pas piratés ? Et si l'on prend l'hypothèse de transactions sans code PIN, ne revient-on pas, pour les achats en ligne, à la carte bancaire actuelle et à ses risques de fraude. Où est le gain sécuritaire ?

Plus encore, comment seront traités, par les sites commerçants, les citoyens qui auront refusé le passage à la CNIE ? Comme de potentiels mauvais payeurs, moins « sécurisant » que les « authentiquement certifiés » ? Ou encore, quelle liberté, si l'on impose une authentification absolue de chaque internaute, quelle liberté de prêter sa carte pour que sa sœur, son fils, son ami ou sa mère puisse acheter en ligne ?

Quelle que soit l'approche adoptée, soit on sombre dans l'ultra-identification paranoïde, avec ses contraintes peu supportables, soit on en restera au système actuel (et c'est préférable !).

## 3. Le syndrome du trou dans le grillage

Finissons le démontage de la charpente par l'argument sécuritaire : la CNIE doit aboutir, nous dit-on à « un renforcement de la confiance dans les titres ». Soit. On peut aisément l'accorder. Ne serait-ce pour l'effort d'adaptation demandé aux faussaires !

Et le Ministère de notre sécurité intérieure et de nos libertés locales d'égrener ce fabuleux dispositif, compacté dans la puce, en cinq « blocs distincts et étanches ». Et d'y ajouter cette quadruple sécurité — sécurité des procédures, sécurité logique des composants du système, physique des installations et technique des titres — qui prétend en garantir le haut degré d'inviolabilité.

Sans critiquer sur la forme ces dispositifs (bien que la cryptographie qui soit à la base de la sécurité technique n'apporte pas la certitude de n'être pas cassée dans quelques années puisqu'elle repose sur un principe mathématique, la factorisation des très grands nombres, qui fait l'objet de recherches intensives), nous pouvons légitimement en rire et douter.

Car cette logique sécuritaire reste victime d'un oubli qu'on pourrait qualifier de « syndrome du trou dans le grillage ». Un site peut être enceint d'une clôture barbelée de huit mètres de haut, être physiquement infranchissable, filmé et gardé par des vigiles, celui qui voudra y pénétrer n'aura qu'à soudoyer un gardien pour y parvenir. Tout

système a son trou dans le grillage, trou technique ou humain. La CNIE n'y échappe pas, construite qu'elle est **sur l'habilitation d'agents dont rien ne peut garantir l'honnêteté ou l'éthique, s'ils sont soumis à des pressions affectives ou financières fortes.**

Plus grave, la constitution de fichiers centralisés offre, toujours à travers ce Cheval de Troie tellement humain qu'est le policier (et sans même évoquer le piratage), la possibilité de duplication, de croisements dangereux ou de revente desdits fichiers à des intérêts militaires, maffieux ou capitalistes qui pourront, au besoin, s'en servir pour traquer nos déplacements ou tracer nos consommations.

**Il paraît impossible de croire qu'un Ministère dont la vocation même est de veiller aux délinquances puisse avoir conçu un système sans deviner de quelle façon il serait tourné.** On sait pertinemment, depuis Michel Foucault, que les lois et les dispositifs techniques développés par les pouvoirs qui nous gouvernent visent moins à réduire la délinquance qu'à *gérer et à ménager les illégalismes* en anticipant la manière dont cette loi et ces dispositifs seront contournés par ceux qui ont un intérêt certain à le faire, État compris. État au premier chef, ici.

#### **4. INES, une créature complaisante ?**

On ne reviendra pas sur la complaisance écœurante de la peu séduisante INES face aux injonctions à peine voilées de Washington, ni sur ses avances un rien putassières aux maquereaux multinationaux du commerce électronique. On ne rappellera pas que l'histoire de la carte nationale d'identité a surtout servi à consolider le sentiment d'appartenance franchouillard, à surveiller les classes dangereuses, à fichier les Juifs sous Vichy et les Arabes après-guerre. **On n'insistera pas sur la montée en puissance d'un contrôle social tout à fait conscient de son inefficacité face aux délinquants professionnels, mais qui n'entend pas laisser filer, au nom d'un terrorisme alibi, hyperfantasmé, sa chance de réencarter électroniquement les citoyens honnêtes et de doubler cet encartement d'une base de données dont la fructification commerciale ou l'utilisation totalitaire s'inscriront, dès sa constitution, dans la gamme des possibilités étatiques.**

#### **5. Pour des identités désincarcérées et plurielles - « Je suis légion »**

Notre critique entend aller plus loin et s'attaquer au noyau même de l'identité. Nous allons essayer d'être bref. Philosophiquement, et particulièrement en France, le concept d'identité a depuis longtemps été dynamité par les penseurs les plus proches de l'évolution sociale concrète de nos démocraties. Deleuze, Guattari, Foucault ou Lyotard, pour ne citer que les plus évidents, ont montré à quel point l'identité ne pouvait aujourd'hui être conçue et vécue que plurielle, fragmentaire, éclatée ou clivée, de manière schizophrène et ubiquiste.

Prétendre aujourd'hui individuer quelqu'un par son nom, sa date et son lieu de naissance, en y associant une adresse et des empreintes de doigts, lui imposer des papiers censés certifier cette fiction, croire, plus encore, que ce processus d'individuation est un gage de liberté pour le citoyen, relève de la foi. Une foi technocratique, sécuritaire sans être du tout sécurisante, une foi d'État tautologique qui ne voit dans ses actions qu'un motif d'autorenforcement de sa fonction régalienn.

La liberté citoyenne n'a jamais pâti, par exemple en Angleterre, de l'absence de carte d'identité.

Ne serait-il pas temps, à l'aube du XXI<sup>e</sup> siècle, dans une France où la multiplication concrète des pseudos et des identités réellement vécues, à une époque de polyphonies émotives, d'hétéronymie, d'appartenances tribales proliférantes, de personnalités

auxquelles la pluralité même de nos statuts professionnels et sociaux, de nos figures affectives, sexuelles ou familiales, de nos visages artistiques ou militants, apporte le meilleur gage d'épanouissement, le plus souple support de tissage collectif, la meilleure chance d'adaptation à la mobilité partout bruissante des repères — ne serait-il pas temps d'abandonner la carte d'identité en la laissant mourir de sa belle mort ? Et d'en faire tout simplement (au moins pour les citoyens qui y tiendront comme à la preuve rassurante de leur insertion sociale) une option toute personnelle — facultative pour les autres ?

**L'identité, en soi, n'existe pas. Il n'existe que des processus d'individuation et des méthodes d'identification. L'identité est une construction relationnelle, hautement.** Une construction qu'aucun titre ne peut prétendre valider parce qu'elle dépend de l'autre, *des autres*, multiples et changeants, et des liens qui m'y tissent, par lesquels cœur, corps et tête s'étoffent, sans cesse. D'où tire t-on cette évidence, très récente dans l'histoire, qu'une instance, fût-elle républicaine, puisse décider de figer ce tissage et d'en garantir le nœud, toujours déliant ?

**Nous ne souffrons pas d'un doute sur l'identité. Nous souffrons au contraire d'une surassignation individuelle, à une charnière historique qui grince de la perte des liens collectifs. Offrir la possibilité à chaque citoyen de se dédoubler, de multiplier ses approches identitaires au sein des milieux qu'il est amené à côtoyer, ne serait-ce pas lui offrir, enfin, l'opportunité d'une mobilité, d'une vitalité relationnelle que la carte d'identité handicape ?**

Que notre Ministère des Libertés, dites Locales, ait la bienveillance d'y réfléchir. La liberté ne devrait pas se concevoir sur le mode défensif, jamais. Les politiques qu'on nous propose, et les sages dispositifs qui les appuient, ne sont que des politiques de la peur. Une habile « gestion des petites terreurs quotidiennes » comme l'a si bien vu Paul Virilio. Excusez-moi de vouloir y opposer — y apposer peut-être — un peu de confiance dans la nature humaine.

**Alain DAMASIO**

\* \* \*

## **VIII. Contribution de Gérard WEISZ, Fédération Nationale des Tiers de Confiance - 23 mars 2005**

Par **Gérard WEISZ**

Secrétaire Général de la Fédération Nationale des Tiers de Confiance

La France à l'instar d'autres pays d'Europe va devoir se doter d'un titre électronique d'identité pour ses citoyens.

Les enjeux technologiques et industriels sous-jacents à ce projet n'ont échappé à aucun des acteurs présents aujourd'hui sur le marché de la sécurité des systèmes d'information, de la conception et la gestion de moyens électronique d'identification, d'authentification, de signature ou de chiffrement.

En d'autres termes, les professionnels, dont une part importante est présente au sein des instances de la F.N.T.C., se sont préparés de longue date pour ce projet majeur et fondateur de la dématérialisation des échanges entre les organisations de toute nature, les individus, les entreprises, etc.

Ma contribution ne sera pas seulement d'ordre technique ou organisationnel car manifestement, ce qui agite les esprits, les thèmes du débat public lancés par le Forum en sont la preuve, est plus d'ordre politique voire éthique.

Le progrès au travers des nouvelles technologies va-t-il une nouvelle fois porter atteinte à la liberté des individus, à l'égalité des citoyens devant les institutions, à la préservation de la vie privée ?

En d'autres termes, faut-il mettre en œuvre le projet d'identification électronique des individus face aux multiples risques réels ou supposés qu'il inspire ?

Au risque de prendre des positions hétérodoxes, je pense que les libertés individuelles, l'égalité de traitement des citoyens dans leurs rapports avec l'administration, les sécurités au sens large seront d'autant mieux assurées que les institutions chargées des différentes tâches d'intérêt public dont elles ont la charge disposent de moyens fiables, performants et ciblés de traitement parmi lesquels l'identification certaine des individus occupe une place importante.

### **Les identifiants biométriques**

La CNIE se doit d'être le titre électronique de référence permettant l'authentification des citoyens dans tous ses rapports avec les organisations qu'elles soient publiques ou privées et dans toutes les circonstances.

Cette authentification est par nature indissociable de la personne, elle doit donc disposer de moyens biométriques utilisables même dans des conditions extrêmes. En effet, dans certaines circonstances, les empreintes digitales ne sont plus accessibles, l'empreinte génétique reste le moyen ultime d'identification. Bien qu'il ne soit pas cité, ce mode d'identification devra être également envisagé dans le projet.

### **Protection de la vie privée**

Cette question comporte un aspect concernant les informations contenues dans la CNIE d'une part et l'exploitation des informations de traçabilité potentielle à partir des événements que la CNIE, dans ses usages, peut générer.

Cet aspect rejoint plus largement celui des sécurités et sur ce plan, je ne verrai aucun inconvénient à ce que, notamment, des informations personnelles de nature médicale figurent dans la CNIE et soient accessibles librement par les services d'urgence.

Au-delà, se place également la question de la consolidation des informations, de la détection des déplacements et des actions des personnes et par conséquent de leur surveillance.

D'ores et déjà le téléphone mobile rend possible certaines de ces opérations mais la CNIE, de part sa connotation administrative, y ajoutera une suspicion liberticide. Le sujet est d'importance mais, si nos libertés démocratiques et notre modèle de société sont mis à profit pour des actions subversives, nous devons nous donner les moyens d'y répondre en faisant confiance à l'arsenal juridique existant dans ce domaine pour pallier les dérives.

### **Les applications**

La CNIE ne peut conceptuellement et juridiquement se substituer directement à des moyens d'authentification à vocation marchande.

En effet les services marchands s'accompagnant nécessairement de garanties assurées par leurs promoteurs, il serait difficile pour l'Etat, dans le cadre de ses responsabilités en tant qu'émetteur de la CNIE, d'assumer un engagement quelconque dans les transactions de toute nature, dont il n'aura pas nécessairement connaissance et qui pourraient être réalisées grâce notamment à l'authentification des parties.

En revanche, certains services marchands pourront être conçus en adoptant la CNIE comme un moyen possible d'authentification, à charge pour leur promoteur d'assumer les différentes responsabilités attachées aux transactions.

Par ailleurs, la CNIE peut s'avérer un support multi usages de nature administrative et il serait donc opportun d'envisager qu'elle supporte l'ensemble des autorisations délivrées par l'Etat : permis de conduire, de chasse, de navigation, de port d'arme, etc...

### **Modalités pratiques**

Dans la présentation du projet il est fait explicitement mention d'une carte à puce comme support de la CNIE.

Ce choix a été fait en Belgique mais les hollandais expérimentent pour leurs passeports un support à lecture sans contact qui permet de fluidifier les passages lors des contrôles de frontières notamment.

Ce point ne devrait pas être négligé à l'heure où les très gros porteurs amplifieront le flot des voyageurs déversés simultanément dans les aéroports.

Par ailleurs, la CNIE doit être l'occasion de mettre en place une procédure dématérialisée pour le dépôt du dossier accompagnant la demande de carte et d'une délocalisation pour la remise de celle-ci.

En tenant compte du fait que l'Etat tiendrait le rôle de l'autorité de certification dans ce projet, les agents de l'Administration peuvent être considérés comme des mandataires de certification habilités à faire les « face-à-face » exigés lors de la remise de la CNIE ayant un niveau un certificat qualifié.

A ce titre et moyennant l'équipement et les formations adéquates le lieu de remise peut devenir indifférent.

### **Conditions financières**

Les documents administratifs sont rarement gratuits, même si la CNI n'était plus payante, la CNIE peut le redevenir compte tenu des services et avantages qu'elle procurera au même titre que chacun accepte de payer les services que procure une carte bancaire.

**Gérard WEISZ**

\* \* \*

## **IX. Contribution de Gérard DUBEY, sociologue à l'Institut National des Télécoms - 30 mars 2005**

Par **Gérard DUBEY**,

Sociologue à l'INT (Institut National des Télécoms)

Chercheur au CETCOPRA (Centre d'étude des techniques, des connaissances et des pratiques),

Auteur de "Le lien social à l'ère du virtuel", Paris, PUF, 2001.

### **IDENTITE NUMERIQUE ET NOUVEAUX RISQUES : LE CAS DE LA BIOMETRIE**

L'enquête sociologique que nous avons réalisée autour de quelques applications de la biométrie (sécuritaire, pour l'accès aux zones réservées à ADP ou non sécuritaires comme l'accès aux cantines scolaires dans les collèges) a révélé une forme d'atonie sociale, une quasi-absence de réaction de la part des usagers vis à vis la mise en place de ces dispositifs.

C'est ce qui nous a étonné dans un premier temps et constitue pour l'essentiel l'objet de nos recherches actuelles.

Que signifient cette quasi acceptation, ce désintérêt ou cette apparente indifférence ?

Il est par exemple 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.

On pourrait s'en tenir à ce constat et parler d'acceptabilité élevée de ces techniques. Ou bien à l'inverse associer a priori les techniques biométriques aux notions de totalitarisme, d'atteintes aux libertés individuelles, comme on l'entend dans la presse, Mais ce serait d'une part refuser d'entendre ce que disent les premiers usagers de ces techniques ; d'autre part, ce serait s'interdire de commencer l'analyse précise du type de pouvoir, de la nature de la surveillance que ces techniques matérialisent.

L'apparente acceptation sociale ne doit pas pour autant dissimuler les contradictions et les tensions qu'elle engendre. Ce qui rend ces techniques acceptables, et presque désirables, est aussi ce qui nourrit la défiance à leur égard. La spécificité de ces techniques qui procèdent à une numérisation du vivant, de parties du corps, appellent des réactions spécifiques, nouvelles, et difficilement pour cette raison à identifier. En creusant un peu on s'aperçoit en fait que l'attitude des usagers est caractérisée par une certaine ambivalence.

D'un certain côté les techniques d'identification biométriques entrent en résonance avec certaines attentes de la société contemporaine. Dans la mesure où ces dispositifs physiques contribuent en effet à stabiliser et assurer une identité individuelle (en la réifiant) qui s'éprouve, par ailleurs, comme continuellement menacée et vulnérable, ils apparaissent comme des solutions non seulement acceptables, mais souhaitables. Si l'identité individuelle n'est plus attestée socialement, en références à des cadres communautaires et à des appartenances sociales, mais physiquement, elle ne peut être validée et garantie que techniquement, par des dispositifs matériels.

Il faut donc toujours replacer ces techniques dans le contexte d'une société de masse, mondialisée, en proie au brouillage et au télescopage des repères culturels et identitaires traditionnels. C'est ici qu'il y a convergence de forme entre le souci

gestionnaire d'un contrôle renforcé des flux de population et le besoin de repères des individus.

En dernière analyse, la perte de confiance envers les médiations sociales et l'autonomie de la société semblent constituer un puissant moteur en faveur des techniques biométriques d'identification, le terreau sur lequel celles-ci pourraient être amenées à se développer.

D'un autre côté, le manque de résistance affichée, et donc l'apparente bonne acceptabilité sociale de ces techniques, ne signifie pas qu'elles ne suscitent pas d'inquiétudes et n'induisent pas de profonds bouleversements (souvent latents) dans la manière de se représenter et de définir l'identité, ainsi qu'au niveau du nécessaire rapport de confiance entre les administrés et les institutions.

C'est aussi ce que révèle notre enquête et qui mérite d'être approfondi et confirmé par d'autres études. C'est par l'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.

*« Je ne sais pas pourquoi on accepte de pouvoir être suivi avec son portable, de laisser une trace lorsqu'on retire de l'argent » alors qu'on redoute d'être fiché en laissant son empreinte digitale »* s'étonnait, par exemple, l'une des responsables des expérimentations conduites à Air France auprès des agents du passage et des passagers du vol Tel Aviv.

Un élément de réponse est donné sur le mode de la dérision un peu plus loin lors de l'entretien. *«C'est une part de moi que je laisse –semblaient vouloir dire certains- donc je ne veux pas que mon intimité soit comme ça perdue sans que je sache ce qui va en être fait ».*

Ce complément d'information 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 ?

Cela ressort encore clairement des remarques sur l'intolérance des dispositifs biométrique aux variations historiques, à la diversité humaine et aux petites irrégularités caractéristiques de la vie.

Ce que pointent en fait nos interlocuteurs, c'est le passage de systèmes d'identification des personnes, jusqu'à présent principalement centrés sur la recherche d'informations administratives (témoignages et traces écrites sur l'histoire de la personne), à des systèmes automatiques de saisie (on parle ici de capture), de stockage et de traitement d'informations relatives à l'identité physique des personnes. Cette distinction est loin d'être indifférente. Ce qui est ainsi saisi ne relève plus d'un mode de validation sociale de l'identité, ni d'un agencement de signes qui sollicite toujours l'interprétation, mais est de l'ordre de la matérialisation et de l'automatisation.

C'est pourquoi 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, fluidifier les passages, 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. On assiste donc à un déplacement des risques, mais peut être pas à leur réduction. Ce qui est fragilisé, plus profondément, ce sont les rapports de confiance sans lesquels il n'existe pas de société. Or ces rapports de confiance se construisent aussi au sein de l'espace public, au gré des expériences

et des interactions sociales (mêmes conflictuelles) avec les institutions et leurs représentants. La réduction des médiations humaines pose donc ici une grave question, celle du lieu de l'apprentissage de la vie en commun et de la construction de la confiance.

Nous soulignons comme essentiel ce risque de déshumanisation induit par l'automatisation, au sens où l'automate peut dégrader, voire annuler la médiation humaine. Cela ne signifie pas, encore une fois, que nous sommes plus attentifs au risque de déshumanisation qu'à celui de la constitution de bases de données centralisées, puisque les deux mouvements sont généralement associés, l'automatisation impliquant en effet un transfert de pouvoir aux dispositifs techniques, c'est-à-dire une perte de contrôle et d'autonomie du côté des acteurs sociaux.

Donc, le problème n'est peut-être pas tant de savoir si la confidentialité des données personnelles sera assurée par des moyens de sécurisation adaptés. A ce type de question existe toujours une réponse technique, c'est-à-dire une solution à portée de main. La question est plutôt de savoir ce que signifie et ce que change, dans le rapport à soi et aux autres, le fait de déléguer à des automatismes le soin de définir l'identité, à commencer par sa traduction en langage numérique. Quel nouveau rapport au sens et la Loi est impliqué dans cette affaire ?

L'intolérance contemporaine à la fraude, à l'erreur, au risque de falsification, qui fait écho aux problèmes engendrés par la société de masse et la mondialisation des échanges, ne doit pas faire oublier qu'il n'y a d'identité réelle que sociale, sujette au changement, en prise avec l'histoire, 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. A 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.

Le danger consisterait ici, par souci d'authenticité, la recherche d'indices immuables, à perdre de vue l'identité réelle des sujets, celle dont les institutions sociales ont justement la charge, et qui est alors susceptible de leur échapper encore plus radicalement.

**Gérard DUBEY**

\* \* \*

**X. Contribution de Amar LAKEL, Chercheur associé, Université de Paris X, Nanterre - 30 mars 2005**

Par **Amar LAKEL**

Doctorant en Sciences de l'Information et de la Communication  
Chercheur associé au CRIS – Université de Paris X, Nanterre

**LA CNIE ET LE POUVOIR D'ENQUETE EN FRANCE**

***L'interconnexion au défi des technologies de l'information et de la communication.***

Si Pierre Piazza a su rappeler la pertinence d'une approche généalogique de la question de la carte d'identité dans le débat sur la CNIE, il nous faut ajouter à ce recul sur le temps long la spécificité d'un contexte particulier lié au double phénomène de la mondialisation et de la démocratisation des échanges publics. Les pouvoirs publics et de nombreux essayistes n'ont cessé de problématiser la mondialisation comme une remise en cause de l'Etat-Nation. En deux décennies, cette assertion semble accumuler les preuves, du moins au niveau médiatique, de l'émergence de nouvelles formes de délinquances. Le crime organisé et la corruption, le terrorisme international, les migrations organisées n'ont cessé de défrayer les chroniques pour constituer la nouvelle forme de menace dans les sociétés modernes. Face à cela, l'Etat-Nation apparaît, aux yeux des citoyens, comme impuissant. En portant les infrastructures de communication humaine à un niveau de développement autorisant la communication commutative de tous vers tous, Internet a fait entrer, après les biens, les actes et les hommes, la production du sens dans la tourmente d'un écosystème qui apparaît au citoyen comme incontrôlé. Deux affaires sont concomitantes de l'arrivée de l'Internet en France : l'affaire du docteur Gubler et l'affaire Yahoo ! Ces deux paradigmes exemplifiés (LAKEL, 2005) ont fait, en leur temps, la réputation d'Internet comme espace virtuel de non droit donnant lieu à un véritable chaos où anarchie et débauche se côtoient en toute impunité. La thèse des nouvelles formes de délinquances mondialisées est alors réactivée. Dès son discours de Hourtin, Lionel Jospin fait place aux inquiétudes qui n'ont cessé de s'exprimer en France sur la question d'une communication sans régulation. « *La généralisation de l'usage des technologies et des réseaux d'information (...) la mondialisation des flux d'information...Qu'il s'agisse du satellite ou d'Internet, les nouveaux réseaux multimédias ne connaissent plus de frontière. C'est pour les Etats, habitués à intervenir dans le cadre national, un défi considérable.* » (JOSPIN, 1997) L'idée d'une crise de l'Etat-Nation face à la démocratisation de la communication publique dans un espace globalisé sans frontière appelle à une réflexion sur l'avenir de la gouvernance en France. Lionel Jospin réagit aux injonctions issues de plusieurs horizons, médiatisées par les « affaires Internet ». « *Le développement d'un réseau ouvert et mondial comme Internet suscite des craintes souvent légitimes.* » (JOSPIN, 1997) Entreprises privées, associations de citoyens, acteurs du droit, police...de nombreux éléments de la société s'engagent dans une course stratégique pour contrôler la mise en agenda des thématiques. De 1997 à 2004, l'insécurité électronique sera une donnée majeure des débats permettant ainsi aux hauts fonctionnaires en charge d'établir une politique de régulation de l'Internet, dans le cadre de la souveraineté nationale, de problématiser la relation entre le pouvoir d'Etat et le réseau des réseaux, en termes de pouvoir inquisitorial afin de permettre de repenser le rôle de l'Etat dans un système complexe et décentralisé.

Le pouvoir inquisitorial est le fondement essentiel du pouvoir régalién de justice. Consubstantielle au développement de l'Etat-Nation, l'autorité judiciaire se fonde sur le passage d'une justice tribale, basée sur le flagrant délit, à une justice instituée, capable de réinvoquer l'acte par l'enquête. Une technologie informationnelle, du recueil de la trace à la réification de l'acte, en passant par la

profilisation du délinquant, assiste le pouvoir de véridicité de l'instance judiciaire chargée de condamner les infractions. Cette *technologie d'attribution* de l'acte au sujet, désormais « responsable » devant le souverain (que ce soit le Roi ou la Loi), est le premier pilier fondateur de l'Etat de droit. Avec le développement de la police et du dispositif de normalisation des sujets de la nation, le dispositif d'enquête s'étendra de l'infraction à l'évaluation de la quotidienneté. Garant de la santé publique et des bonnes mœurs, l'Etat se dote des moyens d'appréhender les comportements des individus pour mieux mesurer les écarts par rapport aux comportements idéaux inscrits dans une économie globale de la puissance de la nation. Cette *technologie de traçabilité* du quotidien est le second pilier d'un Etat-Providence responsable de la bonne santé de chacun et de l'efficacité globale de l'économie nationale. Sa politique d'éducation et de conduite du changement social l'amène à développer la profilisation des individus qui se voient désormais refléter en de nombreux dossiers administratifs plus ou moins publics. C'est l'ère du développement bureaucratique des fichiers. Dans une logique nosographique, une *technologie de stigmatisation* assurera le marquage des individus selon des paramètres qui varieront au gré des évolutions des politiques de gestion. Selon la logique d'un pouvoir pastoral, l'individu fait partie d'un groupe qualifié selon son espèce et sa position sur le territoire (âge, sexe, origine, adresse territoriale, numéro d'immatriculation, « ethnie »<sup>37</sup>...).

La carte nationale d'identité *électronique* apparaît alors comme le point nodal de rencontre entre la longue évolution d'un dispositif de gouvernementalité de la population (et des individus), le pouvoir inquisitorial et l'émergence d'une nouvelle forme d'espace public médiatisé : Internet. Dans le cadre d'une recherche en science de l'information et de la communication<sup>38</sup>, nous avons tenté de suivre la construction des politiques publiques des NTIC en France sur ces dix dernières années au regard d'une rationalité de l'Etat moderne en butte aux nouvelles opportunités d'une mise en réseau des groupes sociaux. Plus de deux décennies après la loi Safari, enterrée par la loi informatique et libertés de 1978, après la première tentative de la carte d'identité électronique abandonnée à l'arrivée des socialistes au pouvoir en 1981, la CNIE semble réactiver les projets de perfectionnement du ministère de l'intérieur de sa capacité d'enquête sur le territoire national. Pour autant, l'histoire ne se répète jamais. S'il nous faut saisir la spécificité du débat actuel et des enjeux qu'il soulève, nous ne pouvons que revenir sur les modes de problématisation qui ont présidé à la question de la régulation de l'Internet par le contrôle de l'identité. Face à ce qui s'est élaboré comme une nouvelle modalité de la délinquance moderne, l'Etat souhaite y opposer un renforcement de ses dispositifs de pouvoir actualisés par les nouvelles technologies. Pour autant, ce renforcement n'est pas un simple accroissement de moyens ou de degrés mais une remise en cause radicale du « compromis de 78 ».

### **Les NTIC au service du pouvoir inquisitorial : répondre aux nouvelles délinquances**

Dans un premier temps, l'Internet fut présenté comme une immense zone d'ombre, un immense chaos, un nuage bouillonnant. Les menaces prenaient appui sur les caractères intrinsèques de l'Internet qui en faisaient une zone d'incertitude maximale. L'architecture des nouvelles technologies de communication fut

---

<sup>37</sup> Même si en France, cette référence est devenue indirecte en raison du passé de l'administration française sous Vichy. En effet, contrairement à de nombreux pays (les ex-pays du bloc soviétique en sont l'exemple le plus notable), en France l'ethnie ne se déclare pas mais peut se déduire par recoupement du nom et du prénom, du lieu de naissance et de la photo. En cas de recherche, les ascendants peuvent permettre de retrouver avec certitude « l'appartenance ethnique » d'un individu.

<sup>38</sup> Cette réflexion repose sur mon travail de thèse en science de l'information et de la communication, « Analyse des fondements des politiques publiques des NTIC en France (1995 – 2004) » (2005), et se poursuit dans le cadre d'une étude, menée avec David Alcaud (CIR), basée plus spécifiquement sur les catégories d'élaboration de la modernisation de l'Etat par les NTIC (Alcaud, Lakel, 2003 ; Alcaud, Lakel, 2004).

directement mise en cause. Ces propriétés, qui en font pour certains une révolution technologique, apparaissent comme une somme de contraintes s'opposant à toute forme de régulation. « *La régulation publique, par la loi, par le règlement ou par le juge a toute sa place sur l'internet. Pourtant, les caractéristiques du réseau rendent délicates son application et son édicition.* » (PAUL, 2000) Par la modification des conditions spatiales et temporelles de l'échange numérique, le rapport entre actes, populations et territoires, sur lequel reposait la construction de l'autorité judiciaire, semble aux yeux des régulateurs profondément remis en cause. L'angoisse de la trace, comme élément fondamental du rapport inquisitorial (à la fois rapport de pouvoir et relation d'information), sera la clef d'entrée de la problématisation de la société de l'information. Entre trop de traçabilité et trop d'anonymat, le pouvoir régulateur s'interroge sur ses conditions de possibilité.

L'interconnexion généralisée apparaît aux acteurs publics comme la condition même du développement des infractions. Ces dernières seraient internationales dans leur essence même. En un mot, la nature du réseau mondial interconnecté fait de l'Internet un espace de communication qui ne respecte ni les frontières de l'Etat-Nation, ni les lois, ni les règles qui régissent l'ordre de l'échange. Le « zonage », qui permettait de qualifier un sujet et ses actes, par son identité nationale, semble avoir volé en éclats sur Internet. En effet, bien plus qu'une facilitation des échanges transfrontaliers, c'est l'émergence d'un champ d'action sans territoire, véritablement globalisé, qui rend préoccupant l'avenir des régimes politiques. La globalisation enfin réalisée par la technique est la première épreuve que les organisations de l'Etat doivent affronter pour assurer l'effectivité de leur pouvoir. Vient ensuite la fugacité des actes qui pose problème aux pouvoirs inquisitoriaux de la police. Le régime de la preuve repose sur les techniques de traçabilité que mettent en branle les agents de la force publique. Sans trace, on ne peut que constater les dégâts sans pouvoir établir les infractions. Or, Internet semble avoir instauré une course poursuite avec le temps. L'enquête serait le fruit d'une course entre deux régimes de temporalité : celui de la technologie d'enquête, qui tente de reconstituer la scène du crime et celui de l'empreinte, qui a enregistré pour un temps les conséquences de l'acte. Temps de l'enquête et temps de l'acte entreraient en compétition avec le risque d'obsolescence qui pèserait sur le premier. Ainsi s'ajoute à la dispersion et à l'internationalisation de l'acte, son extrême rapidité, sa volatilité, voire son instantanéité. « *Ce qui est nouveau, c'est d'une part, la plus grande facilité avec laquelle ces infractions peuvent être commises et diffusées dans le monde, du fait de la structure du réseau et de son mode de fonctionnement et, d'autre part, les difficultés rencontrées dans l'application des textes du fait de la fugacité extrême des contenus et de la dimension internationale d'Internet.* » (FALQUE-PIERROTIN, 1998) En effet, les contraintes infrastructurelles jouent également contre le pouvoir inquisitorial. Si l'espace a connu une extension dans la globalisation des échanges, le temps s'est quant à lui contracté. « *Avec la croissance exponentielle du trafic, la limite de notre capacité à garder le traçage IP passe de six à quatre mois. D'où une inadéquation entre le temps de stockage et le temps de la justice.* » (CSA, 1999). Accélérer les dispositifs d'investigation et rallonger la conservation des traces apparaît très logiquement comme les fondements d'une restauration du pouvoir de l'enquêteur. La question de l'archivage est donc politique, la mémoire des actions est la base de la responsabilité.

Derrière la question du temps et de l'espace de l'acte, émerge un troisième enjeu primordial pour le pouvoir inquisitorial : la possibilité de l'identification des auteurs de l'acte. « *Le vrai problème actuel est la lutte contre l'anonymat, qui est la base de tous les dérapages, car sans auteur du délit, pas d'application de la loi.* » (CSA, 1999) La dimension virtuelle du réseau permettant la dichotomie des sujets virtuels et des sujets réels (et en particulier du sujet légal, le citoyen), les techniques d'anonymisation défient le droit, qui repose son pouvoir sur la

responsabilité. « *L'utilisation d'un pseudonyme concernait, autrefois, un nombre limité de personnes : artistes et auteurs, principalement. Avec le développement du courrier électronique, des forums et des chats sur internet, des jeux en réseau, un grand nombre d'internautes utilisent des pseudonymes, se construisent des identités artificielles, virtuelles, parfois multiples. La question de l'anonymat sur les réseaux est complexe.* » (TRUCHE, 2002) Ainsi, le pouvoir justicier disparaît dans une société de l'information où il deviendrait difficile de traduire l'identité virtuelle en identité réelle.

### **Le contrôle d'identité comme fondement du pouvoir d'Etat**

Entre remise en cause radicale et extension infinie, les défenseurs du droit ont pris appui sur la notion d'identité numérique – qui a le grand avantage d'être à la fois une propriété en tant que réification informationnelle de la personne et la base de la liberté comme connaissance du sujet. Dans un premier temps, la puissance publique a la charge d'assurer sa présence dans la société de l'information. Elle s'appuiera pour cela sur une triple extension de sa capacité inquisitoriale, censée résoudre les défis du réseau des réseaux. Construire un système d'instances électroniques tierces, capables d'assurer le contrôle d'identité dans les transactions contre l'anonymat et la fugacité ; développer le pouvoir d'enquête absolu dans les systèmes d'information informatisés afin de poursuivre la cybercriminalité dans un monde en réseau ; mettre en place un système global d'information informatisé qui adapterait les forces de police aux nouveaux modes de criminalité.

La question du pouvoir de connaître le sujet en acte est devenue un enjeu de pouvoir et un objet primordial du sujet de légitimation. Outre le spam ou la sécurité des transactions, l'identité numérique fait partie de ce type de problématisation paradigmatique qui permet de légitimer la mise en place d'un dispositif de régulation étatique. On peut affirmer que très vite l'ensemble des problématiques politiques repose sur la question de l'identité comme objet même du pouvoir inquisitorial. L'identité est cet ensemble de données rassemblées, puis unifiées et attribuées à un sujet. L'identité est en quelque sorte le fruit d'un processus de réification du sujet de la loi que les agents de l'Etat, de l'inspecteur des finances au sociologue de l'INSEE, tentent depuis plus de trois siècles de constituer<sup>39</sup>. Sans entrer dans le détail d'une réflexion épistémologique, l'identité est ce modèle qui permet de faire exister un sujet dans la connaissance. La possession de ce modèle est de la plus haute importance dans la relation de pouvoir qu'un Etat peut établir avec ce sujet modélisé dans la mesure où elle réduit l'incertitude sur ses possibilités de décision. Cette possibilité de modélisation d'une identité est donc bien consubstantielle à la notion de mise en réseau des données. La défense de la protection de la vie privée vise à empêcher et à limiter l'enquête comme connaissance illégitime du sujet. La « profilisation » est donc la technique qui permet de reconstituer une identité à partir de fragments de données de transactions éparées. Plusieurs catégories de données sont à la source de ce type de traitements. Les données relatives au trafic permettent d'enregistrer les comportements des individus bien souvent à leur insu. Les actions du sujet sont captées et enregistrées comme des variables pertinentes en fonction de profils élaborés. Les données de transaction sont du même ordre mais sont plus souvent échangées avec le consentement de l'interlocuteur (même si les traitements postérieurs en vue d'une profilisation ne sont pas toujours clairement perçus, l'archive est à ce titre un enjeu essentiel.)

---

<sup>39</sup> Michel Foucault a même tenté de montrer, dans « Il faut défendre la société », la liaison consubstantielle entre l'Etat moderne, le pouvoir inquisitorial et le sujet statistique. Erik Neveu (NEVEU, 2001) a réintroduit cette réflexion dans la problématisation de la société de l'information.

Dans la question de cette identité, une information particulière, si menue soit-elle<sup>40</sup>, joue un rôle stratégique, voire systémique : l'identifiant. L'identifiant est une méta-information qui s'ajoute à une grappe de données reliées entre elles de façon définitive. Cet identifiant permet de rassembler toutes ces grappes en un tout unique et ce indépendamment de leurs éparpillements temporel ou spatial. Sans identifiant, la grappe de données est fermée sur elle-même et donc très limitée dans son usage. Sans identifiant, pas d'identité digne de ce nom, capable de constituer un sujet. Par contre, plus le même identifiant sera utilisé, plus l'interconnexion permettra une pertinente d'analyse, plus elle sera capable d'individualiser le sujet. Au premier rang des identifiants numériques viennent ces numéros que les institutions attribuent à leurs assujettis, usagers, clients, membres. Ces « *identifiants de gestion* » permettent aux organisations de regrouper, sans ambiguïté, toute une série d'informations sur une même personne. Certains identifiants sont stables » (TRUCHE, 2002)<sup>41</sup>. La signature manuscrite a joué ce rôle de signe métonymique arbitraire individualisant. Elle joue encore de nos jours un rôle d'authentification de la personne et du consentement en acte. Son équivalent numérique est le couple login/mot de passe qui assure une reconnaissance du sujet au fur et à mesure des transactions. (Les cartes de crédit et leur couple numéro/code appartiennent à cette catégorie)

Parmi ces identités (accompagnées de leur identifiant), une identité particulière possède une valeur sans égal dans la relation de pouvoir que l'on peut établir avec un individu : l'identité personnelle. Une identité qui relie une somme d'informations à une vie biologique unique, et ce de façon indiscutable. Cette identité personnelle fonde la relation de pouvoir entre le souverain et ses sujets par la connaissance des corps. Cette identité se fonde sur la présence d'une trace valide du corps du sujet comme identifiant infalsifiable (présence réifiée par une donnée biométrique : empreinte, photo et tout autre procédé comme l'ADN). L'identité personnelle révèle clairement la base du pouvoir de l'Etat : la vie de l'espèce territorialisée. Chaque ministère a en réalité développé son identifiant personnel unique (NUMEN pour l'éducation nationale ; SPI pour l'administration fiscale). Or, ces identifiants ne peuvent devenir certains que par recoupement via le NIR. Dans nos sociétés, l'Etat civil et ses différents supports (dont la carte d'identité est la base) jouent ce rôle. Ils sont la base du pouvoir régalien. Dans le cadre d'une procédure formalisée, le sujet habitant en France devient citoyen ou résident étranger (ou réfugié politique, etc.) par la reconnaissance de son identité manifestée par la possession d'un titre d'identité. Pour que ce titre d'identité soit valable, la procédure doit avoir mis en relation un ou plusieurs agents accrédités

---

<sup>40</sup> Souvent une simple combinaison alphanumérique.

<sup>41</sup> En France, la loi sous le contrôle de la CNIL, surveille l'usage des identifiants pour qu'il ne soit pas signifiant. « *C'est-à-dire qu'il soit impossible, à la simple lecture d'un identifiant, d'apprendre quelque chose sur la personne concernée, par exemple un numéro tiré au hasard.* » (TRUCHE, 2002) La plupart des identifiants furent décriés dans le cadre de la distribution de la prestation de services publics. L'adresse postale, par exemple, sous couvert de neutralité territoriale, permet une discrimination sociale et ethnique grâce à une procédure d'attribution de logements (privés ou publics) largement ségrégative. Mais la bataille la plus importante autour d'un identifiant fut sans nul doute celle du NIR. Sous le régime de Vichy, l'INSEE a créé le NIR, numéro d'inscription au RNIPP, afin de renforcer l'identification des sujets vivant sur le territoire d'une façon permanente, fiable et stable. Cet identifiant est totalement signifiant au point d'être une véritable carte d'identité numérique qui renseigne le lecteur de ce numéro sur le sexe, l'âge, et le lieu de naissance (et particulièrement, par le 99, si ce lieu est étranger au territoire français). Son utilisation est strictement encadrée par la CNIL et les acteurs de la société civile qui luttent contre les discriminations de toutes sortes. Herbert MAISL nous rappelle l'origine de cet identifiant : « *il ne faut pas oublier que l'utilisation de ce numéro, pendant la dernière guerre, a été envisagée comme instrument de tri des juifs.* » (MAISL, 1997) Toutefois, son utilisation est possible. Les administrations sociales l'ont amplement utilisé sans réel contrôle de la CNIL. Pierre Truche nous rappelle que, mise devant le fait accompli, la CNIL fut bien obligée d'accepter sa diffusion : la délibération de la CNIL du 29 novembre 1983 constate que le NIR est devenu « *l'instrument de référence fondamental de l'état civil en France, destiné en particulier à lever le doute sur les homonymies* » et qu'il a été utilisé d'emblée par la sécurité sociale. Admettant donc par force cette utilisation du NIR, la CNIL souligne le risque, en raison du caractère signifiant des chiffres le composant, de voir le NIR se généraliser et devenir l'identifiant national.

par l'Etat en présence corporelle de la personne à identifier. L'agent assermenté relèvera une série d'informations pertinentes pour l'identification physique de la personne (taille, sexe, âge, lieu de naissance, signature et surtout photo). A cette présence physique, il associera les informations propres à l'Etat civil (prénom, nom, adresse et ID). Il ajoutera, à des fins de contrôle, l'identification de l'autorité de certification (la préfecture et signature de l'autorité). Afin de s'assurer de l'unicité du titre, il rendra cette carte infalsifiable et renouvelable périodiquement. Mais la procédure d'authentification, si elle est déjà bien assurée par la possession de ce titre matériel, n'est absolue que dans la relation triangulaire qui relie un agent identificateur et un sujet identifié par le recours à la base de données de l'autorité d'authentification.

### **Les technologies de l'information et de la communication comme mode absolu d'identification.**

L'identité a une double nature, à la fois un objet informationnel et une réification d'un sujet, qui peut être par extension un être humain. Le pouvoir inquisitorial n'est donc pas un outil de savoir neutre. L'appropriation d'objets informationnels, quand elle autorise la connaissance de sujets actants, est le préalable à une connaissance des conditions de la liberté humaine. La base d'une technologie permet donc de déterminer une stratégie dans le cadre d'une relation de pouvoir. Si Internet semble permettre une extension quasi-infinie du pouvoir inquisitorial, l'enregistrement généralisé, la mémorisation infinie et la puissance des outils de recherche formeraient un formidable dispositif de contrôle. Mais au service de qui ? Ainsi, que ce soit par la description d'un Internet comme barrage au pouvoir inquisitorial ou celle d'un Internet comme extension infinie de ce pouvoir, la problématisation juridique de l'Internet s'attache à souligner une question essentielle : l'émergence de la technique et des opérateurs privés dans cette relation de pouvoir et leur légitimité. « Code is law », nous avait prévenu Lawrence Lessig, dès 1999, dans son ouvrage *Code and other laws of cyberspace* (LESSIG, 1999). La technologie apparaît en effet comme une première solution aux problèmes de virtualisation de l'acte. Par un retournement propre aux relations de pouvoir, les Etats nationaux, en lutte avec les « contraintes » imposées par le nouveau système d'action de la Global Information Infrastructure, affirmeront en effet, au vu des tentatives des acteurs privés de protéger leurs droits sur la propriété informationnelle, que ce n'est pas seulement par une gouvernance sur les usages mais aussi par une gouvernance sur la technique que réapparaîtra la possibilité d'une régulation du Net. En effet, dans un premier temps, la focalisation sur les infrastructures de communication permet d'ancrer l'objet de la loi dans le territoire. En agissant directement sur les conditions de possibilité techniques de la communication, le pouvoir judiciaire récupère un acteur à portée de main. Ensuite, l'implémentation de la loi en code informatique permet d'établir des règles d'usage qui conditionnent radicalement les pratiques. On voit ainsi le mariage entre le code juridique et le code informatique se conjuguer de plus en plus pour déterminer l'infrastructure web à devenir « gouvernable ». L'émergence de ce nouveau mode de régulation, technique et programmatique, révèle une nouvelle configuration de la société de la communication médiatisée<sup>42</sup>.

---

<sup>42</sup> Sous le gouvernement de Lionel Jospin, le projet de loi sur la société de l'information aurait constitué une étape fondatrice dans ce processus juridico-technique. Il transposait à la base la directive européenne du 8 juin 2000 sur le commerce électronique. La nouvelle majorité rejettera ce projet de loi pour disséminer le programme de cyber-police dans trois ensembles législatifs : la Loi sur la Confiance et l'Economie Numérique (LCEN), la Loi dite « Paquet Télécom », et les lois dites Perben I et II. Ce « droit de l'Internet » sera renforcé par les chapitres technologiques d'une nouvelle définition de la répression des « nouvelles délinquances » à la fois locales et internationales. La loi sur la Sécurité Intérieure, proposée par Nicolas Sarkozy, alors ministre de l'intérieur, fut adoptée le 19 mars 2003. Elle s'inscrit dans un programme qui la relie aux lois Perben I et Perben II, ainsi qu'à la loi Economie Numérique toujours sous son ministère, aux finances et à l'économie, comme un ensemble de dispositifs visant à renforcer le pouvoir inquisitorial en France. La loi d'orientation et de programmation pour la justice, dite loi Perben I du 9 septembre 2003 est la première étape du programme du gouvernement

On peut dire que sur Internet, il ne peut y avoir de communication sans signature électronique, c'est-à-dire comme processus d'authentification. La première des signatures est inscrite au cœur même du protocole TCP/IP et vise à identifier les machines. D'une part, l'adresse IP fait office d'identité temporaire de la machine car elle est fournie par le fournisseur d'accès durant un délai limité et d'autre part l'adresse MAC du module de connexion permet de connaître son identité définitive (l'adresse IP permet toutefois de connaître l'identité fixe du fournisseur d'accès)<sup>43</sup>. Mais l'identité d'une machine n'est pas celle d'un sujet de droit. Même si aujourd'hui l'ensemble des fournisseurs d'accès sont tenus de garder leurs journaux de connexion associant leurs clients à des adresses IP utilisées, la responsabilité individuelle est toujours sujette à caution. Cette adresse peut toujours être usurpée ou « spoofée » (particulièrement avec l'explosion du Wi-Fi), la connexion Internet peut être collective (cas d'un cybercafé ou d'une entreprise avec un serveur proxy ou un routeur NAT, d'un réseau familial, etc.), la responsabilisation d'un acteur identifié est précaire (même si elle n'est pas impossible). Dans le système Internet, la signature électronique, basée notamment sur une infrastructure à clé publique (type PKI), est la seule capable d'assurer l'authentification des interlocuteurs d'une transaction spécifique par l'intervention d'un tiers. Ce tiers permet non seulement l'intégrité de l'échange, en assurant le traçage et l'enregistrement des informations, mais aussi l'identification réelle des auteurs en fonction des règles en vigueur. En imposant, comme condition a priori, la signature électronique à l'ensemble des échanges, on s'assure en amont de la réintégration de la communication à un espace traçable au niveau du sujet de la loi. La question de la signature électronique assure, à condition que le tiers de confiance obtienne une légitimité de l'Etat, la non révocabilité des actes. Comme l'acte notarié, l'enregistrement de l'acte par le tiers de confiance assure de la preuve de l'acte. La signature électronique apparaît alors comme l'antidote de l'anonymat dans la communication électronique sur Internet. Contre la fugacité des échanges, un espace de séquestre des actes légaux rend possible la constitution d'actes authentiques. Mais l'émergence d'un tiers comme condition de possibilité d'une communication électronique authentifiable fait apparaître un dispositif qui se constituera comme le modèle d'un droit assuré par une technique administré par un opérateur. La question de la signature électronique est manifestement apparue comme un laboratoire testant, dans un champ restreint, les possibilités de régulation de la communication.

Pourtant, le tiers n'a que très peu de moyens pour s'assurer de la véracité des déclarations préalables des auteurs. Numéro de carte de crédit et photocopies de documents identifiants sont encore sujets à falsification. Seul un pouvoir de contrôle avancé permettrait de résoudre définitivement cette incertitude. Seul l'Etat, dans sa volonté de récupérer la gouvernance de l'information sur Internet, peut réaffirmer son droit au contrôle absolu de l'identité. Parallèlement aux modes de régulation traditionnels, la régulation par le code pourrait voir émerger de nouveaux types d'instances de régulation. Importer directement des transactions

---

Raffarin pour réformer la justice et la police en France. Après le passage de la LSI, la loi Perben II bouleversera, en 224 articles, le code de procédure pénale en opérant, au grand damne de toute la magistrature, une révolution de la tradition juridique et policière française. Sous le modèle des réformes menées par John Aschcroft aux Etats-Unis, le gouvernement français introduit un nouveau modèle de pouvoir inquisitorial copiant les procédures américaines. La Loi du 9 mars 2003 se veut une adaptation de la justice aux évolutions de la criminalité.

<sup>43</sup> Il faut se rappeler que depuis son origine jusqu'à la création de l'ICANN, le réseau des réseaux, qui partout promeut le mode organisationnel complexe d'unités autonomes interconnectées (sur le paradigme du P2P), a fait preuve d'un conservatisme anachronique en ce qui concerne les questions d'identité. Si de nombreux experts ont fait preuve de leur étonnement devant cette « anomalie » technique, l'infrastructure hiérarchique et centralisée des adressages (IP et Nom de domaine), nous voudrions soutenir l'hypothèse qu'à l'origine du projet la question de l'identification et de son architecture technique était inscrite dans le code.

privées entre entreprises privées et clients, les transactions entre l'Etat et la société civile serait assurées par un dispositif électronique de gestion d'identité électronique : la Carte nationale d'identité électronique. Fruit d'une série de projets en technologies de l'information et de la communication autour d'une infrastructure de gestion de clés pour ses propres services administratifs en ligne le ministère des finances, en tant que ministère le plus avancé en matière de NTIC, et le ministère de l'intérieur, seul légitime à contrôler l'identité des citoyens, souhaitent désormais mettre en place une véritable « citoyenneté numérique » chargée de restaurer la base de l'Etat de droit sur Internet par l'authentification et la responsabilité du citoyen. « *En sécurisant cette procédure, l'État se donnerait les moyens de mieux garantir l'identité des citoyens français (la situation actuelle n'étant de ce point de vue pas entièrement satisfaisante : on en prend la mesure dans les cas d'usurpation partielle ou totale de l'identité).* » (TRUCHE, 2002) Tout d'abord, les acteurs publics de l'Internet souhaitent constituer une identité numérique publique pour chaque résident français. Cette identité serait conservée par l'Etat dans un coffre fort et permettrait d'interconnecter toutes les informations de tous les services publics. Ainsi, la problématique de l'interconnexion des bases de données des administrations serait dépassée par l'émergence d'un espace tiers, ayant seul le pouvoir de recevoir ou d'émettre les données. Cet espace conserverait en son sein l'ensemble des données pertinentes pour les transactions administratives ou privées. Ces dernières seraient ainsi mises en relation sans que les bases de données des administrations aient à l'être. De plus, cet espace pourrait archiver les transactions administratives et conserver les documents produits dans la période de leur validité. Il s'agit directement d'une récupération de projets de compte universel de consommateur tel le projet « passeport » de Microsoft. « *Un certain nombre de solutions technologiques permettent de placer les données personnelles sous le contrôle effectif des personnes. Elles constituent, en un sens, la traduction technique du principe de maîtrise des données personnelles. Ces solutions ont reçu le nom de « coffre-fort électronique.* » (TRUCHE, 2002). La métaphore du coffre-fort suggère que les données personnelles sont « enfermées » (sous clef) et que seule la personne concernée (son détenteur ou son « propriétaire ») est habilitée à y accéder ou à les transmettre. Pour aller puiser ces données dans le coffre-fort, les interlocuteurs (entreprises ou administrations) doivent obtenir son autorisation et, éventuellement, la clef. Cette notion de coffre-fort renvoie à une grande diversité de dispositifs et d'architectures. Le coffre-fort peut ainsi être installé sur l'ordinateur de la personne, sous son contrôle direct ou chez un intermédiaire public ou privé (un « notaire » ou « tiers de confiance » ou « infomédiaire »). Ce coffre-fort peut être lui-même compartimenté en zones : une clef spécifique donne alors accès à chacune de ces zones. En lieu et place d'une clef unique, l'utilisateur est doté d'un trousseau de clefs électroniques. On fait valoir que ce type de système transmet le pouvoir d'interconnexion à l'utilisateur, qui par la détention exclusive des clefs d'entrée, accède non seulement à une maîtrise complète des données mais manifeste son consentement aux transferts d'une base à l'autre de ses données personnelles. Indépendamment de sa forme, cet espace ne serait accessible que par des clefs en la possession de chaque citoyen. Cette clef est le pilier du dispositif car elle assure le principe de liberté et de consentement de l'individu qui serait le seul à pouvoir accéder à cet espace d'informations. De plus, il porterait la responsabilité envers l'Etat de la régulation de ses données personnelles. Plusieurs solutions techniques ont été discutées. Pourtant, l'idée d'une nouvelle génération de carte d'identité apparaissait à tous comme le meilleur compromis entre fiabilité et facilité. Cette carte deviendrait, outre une carte comportant une série d'informations sur l'utilisateur, un trousseau de clefs d'entrée au compte personnel public. Le rapport Truche, après consultation des intéressés, nous a annoncé très officiellement que le ministère de l'Intérieur, sous la direction de son ministre de l'époque, Nicolas Sarkozy, conduisait très sérieusement un projet en ce sens. Le ministère de l'Intérieur a réaffirmé son angoisse permanente de rendre plus sûre la procédure de délivrance des titres d'identité. Le projet

unifierait l'identité du sujet sous un « titre fondateur » dans la mesure où elle permettrait la délivrance dans un premier temps de la carte nationale d'identité, du passeport et autoriserait ensuite, l'ajout d'autres titres publics ou privés : la carte nationale d'identité électronique (CNIE+passeport) ; la carte du citoyen (CNIE +carte électorale) ; la carte du conducteur (CNIE +permis de conduire)

### **L'actualité de la question de l'interconnexion comme limite aux pouvoirs d'Etat.**

Aujourd'hui, Internet comme système d'information constitué de l'interconnexion a priori des réseaux (le réseau des réseaux), rend possible l'interconnexion globale des systèmes de fichiers. Dans cette Société de l'Information, le droit distingue un système de cercles concentriques qui, de la périphérie au centre, autorise toujours plus de pouvoir sur la gestion des données personnelles. La zone du secteur privé, la zone des services publics délégués aux organismes annexes, la zone des institutions étatiques et enfin la zone des institutions de police et de justice sont quatre lieux où les données personnelles peuvent être enregistrées de manières plus ou moins absolue. Données relatives au trafic, données de transaction, données personnelles, données personnelles sensibles (Article 8 de la loi informatique et liberté rénovée), données d'identification sont éparpillées en une multitude de fichiers qui forment une mosaïque complexe qui réifie l'identité du sujet et l'histoire de ses transactions avec son environnement. Mais pour que cette mosaïque forme une unité liée à un individu, il faudrait un identifiant unique à tous ces fichiers (fusse-t-il une simple combinaison alphanumérique) enregistré selon une procédure d'authentification biométrique certaine archivant chaque transaction. Un fichier central de l'identité numérique ne serait autre qu'une méta-base de données relationnelle dont l'une des tables principales fonderait la carte nationale d'identité électronique (les autres servant principalement à l'archivage des transactions certifiées<sup>44</sup>). Chaque individu sur le territoire (est interconnecté à ce fichier sur l'ensemble des territoires) obtiendrait donc une occurrence de ce fichier à travers l'obtention de sa CNIE. Dans une infrastructure interconnectée a priori, la société de l'information deviendrait un unique fichier contenant une base de données relationnelle répartie, dont la cohérence reposerait sur l'utilisation de l'identifiant numérique unique (un simple numéro unique et infalsifiable)<sup>45</sup>. Aujourd'hui le ministère de l'intérieur souhaite voir cet identifiant unique (matérialisé par la CNIE) servir à l'ensemble des transactions des individus (qu'elles soient publiques ou privées) que ce soit sur le territoire national ou en dehors (d'où l'intérêt d'unifier cartes d'identité et passeports). Ainsi l'ensemble des données d'un individu, qu'elles soient contenues dans des fichiers privés ou publics, serait mis en cohérence par cet identifiant. A chaque usage d'une identification certifiée par l'utilisation de la CNIE, les données

---

<sup>44</sup> La conservation des données personnelles mutualisées dans cette base de données est une option qui n'a que très peu d'importance dans le système, car peu importe le lieu où sont conservées ces données (sur la carte, dans un fichier central, dans des fichiers non interconnectés, etc.), c'est avant tout les modalités d'accès qui sont véritablement un enjeu politique.

<sup>45</sup> Le ministère de l'intérieur a écarté ces préoccupations citoyennes avec une grande légèreté. « Le ministère de l'intérieur a rappelé qu'avec le GSM, un opérateur de téléphonie sait déjà où l'abonné se trouve « à 100m près, 24h/24 » et qu'avec la carte Visa, « votre banquier sait tout de vos dépenses ». Il en est de même avec les cartes de fidélité, les compagnies aériennes ou encore les grandes surfaces qui savent « tout » des habitudes de vie de leurs clients. En outre, avec Internet, il est techniquement possible de savoir qui est l'internaute en ligne, malgré un pseudonyme, et d'obtenir l'historique de toutes les navigations sur le web. En conclusion le ministère a souhaité préciser qu'un Etat qui voudrait « cliquer » quelqu'un n'aurait pas besoin d'investir dans une carte d'identité électronique ; il lui suffirait de recourir à ces moyens (GSM, CB, Internet, cartes privatives) déjà existants. » (FDI, « *A propos de la lecture « sans contact » de la carte et la création d'une base d'empreintes digitales numérisées* » <http://www.foruminternet.org/forums/read.php?f=16&i=1733&t=1733>).

Il est surprenant que le ministère nous annonce ce fichage généralisé par les opérateurs privés, qui soit dit en passant servent aussi d'auxiliaires de police, et qu'il ne nous explique pas le rôle de la CNIE dans ce système.

recueillies nourriront le fichier unique virtuel du sujet actant<sup>46</sup>. Pour apporter une certitude à l'authentification de l'interlocuteur, la carte a enrichi sa batterie d'identifications personnelles en y ajoutant de nouvelles données biométriques (photo et empreinte digitale numérique, et pourquoi pas Iris ou code ADN) et en les numérisant. Le législateur a modifié la loi informatique et libertés pour autoriser l'ensemble du service public à procéder à des identifications biométriques<sup>47</sup>. Les services privés étant autorisés à relever les identifiants généraux et à les vérifier par une authentification moins sûre (type carte de crédit, qui combine le numéro de la carte, son code PIN et une validation interne ou externe).

Ce fichier unique, qui recouperait l'ensemble des données d'un individu, réside cependant dans une base de données virtuelle qui nécessite son actualisation par une procédure d'interconnexion, car en effet, dans un système de données relationnelles réparties et basées sur une infrastructure de communication interconnectée a priori, il n'est nul besoin que les fichiers soient interconnectés en permanence. C'est le traitement des données à partir de la mise en relation par l'identification unique qui actualise l'occurrence d'un fichier unique. Il suffit donc à un agent d'obtenir un ensemble de grappes de données réparties mais possédant toutes le même identifiant pour actualiser l'occurrence d'un fichier global pertinent. Ce ne sont pas les fichiers qui sont interconnectés, mais la requête de l'agent qui interconnecte des tables réparties. Or, les réformes récentes ont donné au pouvoir inquisitorial d'Etat, dans l'océan numérique, une extension de ses prérogatives à partir de l'année 2004. La volonté de rendre transparente à l'œil de l'autorité une société de l'information qui recoupe toute la communication sociale est très claire. D'une part, nulle barrière ne doit exister entre l'autorité judiciaire et le cyber-citoyen. Le droit de la police à accéder à toutes les communications est réaffirmé avec force. Inversement, son droit à garder secret ses démarches d'enquête lui assure une invisibilité dont la logique fut largement explicitée par Michel Foucault. Pourtant, l'une des nouveautés de ce pouvoir inquisitorial est la reconnaissance d'un droit de poursuite de l'enquête qui tranche avec la tradition juridique. Un véritable pouvoir auto-légitimant est instauré afin de permettre à l'officier judiciaire de profiter des connexions du réseau pour remonter les filières. Les forces de police et de justice obtiennent un pouvoir absolu d'accès aux données informationnelles. La société de l'information doit être absolument transparente au regard du pouvoir d'Etat. Ce droit d'accès est renforcé par un droit de poursuite en cas de perquisition. La LSI introduit le droit de perquisition informatique locale dans le

---

<sup>46</sup> Insistons sur un point : le système de fichage n'a aucun rapport avec ce que l'on met sur la carte. Le contenu de la carte est un débat secondaire. Il suffirait que la carte porte un identifiant alphanumérique certain, validé par une empreinte biométrique, pour donner une cohérence à toutes les grappes rattachées à cet identifiant. Ce dernier est donc le seul devant être centralisé, l'identité numérique étant très largement répartie dans l'ensemble des fichiers privés ou publics. Cette dernière sera une réalité d'autant plus complète que le sujet aura laissé des traces « identifiées ».

<sup>47</sup> L'article 27, partie II, alinéa 4, permet donc à toute personne morale, publique ou privée, de mettre en place un téléservice d'administration électronique s'appuyant sur un système d'identification biométrique relié au répertoire national d'identification des personnes physiques. De plus, le Conseil d'Etat peut soustraire à cette autorisation toute personne morale, publique ou privée, gérant un service public, lorsqu'il constitue un fichier « qui porte sur des données parmi lesquelles figure le numéro d'inscription des personnes au répertoire nationale d'identification des personnes physiques » (Art.27) Dans la même logique, l'article 27 ajoute que les traitements de l'Etat « qui portent sur des données biométriques nécessaires à l'authentification ou au contrôle de l'identité des personnes » sont, elles aussi, soustraites à l'autorisation de la CNIL. Enfin, sont exclus du pouvoir de l'autorisation de la CNIL, par simple décision de l'organe délibérant d'un établissement public ou d'une personne morale de droit privé, gérant un service public, les enregistrements du numéro d'inscription au répertoire national d'identification des personnes physiques. Les données biométriques d'identification, sont autorisées dans les mêmes conditions si le fichier ne comporte pas les données « interdites » de l'article 8 ou les données judiciaires de l'article 9 et si elles sont « mises en œuvre par des services ayant pour mission, soit de déterminer les conditions d'ouverture ou l'étendue d'un droit des administrés, soit d'établir l'assiette, de contrôler ou de recouvrer des impositions ou taxes de toute nature, soit d'établir des statistiques », à condition qu'elles « ne donnent pas lieu à une interconnexion entre des traitements ou fichiers correspondant à des intérêts publics différents. »

code de procédure pénale. L'article 56 de la section du code de procédure pénale sur le crime et les flagrants délits a profondément étendu le pouvoir de perquisition et de saisie de la police judiciaire en matière de système d'information. Avec l'article 57-1, un officier de justice est autorisé à « accéder par un système informatique implanté sur les lieux où se déroule la perquisition à des données intéressant l'enquête en cours et stockées dans ledit système ou dans un autre système informatique, dès lors que ces données sont accessibles à partir du système initial ou disponibles pour le système initial. » Cet article institue dans le droit français, ce droit de poursuite sur les ordinateurs interconnectés à distance. Ainsi, la notion de réseau est ici appréhendée pour permettre à l'officier d'entrer dans une toile par n'importe quel noeud. L'article 76-3 étend ce pouvoir au cadre de l'enquête préliminaire et le 97-1 à la commission rogatoire. Ce qui fait de ce droit de perquisition un usage facile à mettre en place, banalisant la procédure d'intrusion dans les données personnelles. La Loi sur la Confiance dans l'Economie Numérique, appuyée par la loi Perben II, a radicalement renforcé ce droit de poursuite. « Si la nature du crime est telle que la preuve puisse en être acquise par la saisie des papiers, documents, données informatiques ou autres objets en la possession des personnes qui paraissent avoir participé au crime ou détenir des pièces, informations ou objets relatifs aux faits incriminés, l'officier de police judiciaire se transporte sans désemparer au domicile de ces derniers pour y procéder à une perquisition dont il dresse procès-verbal. » Ce pouvoir d'introduction libre dans le domicile privé, très vaguement encadré, permet de saisir, par une fouille étendue, l'ensemble des documents électroniques qui pourront servir à constituer des plaintes contre la personne soupçonnée. « Il est procédé à la saisie des données informatiques nécessaires à la manifestation de la vérité en plaçant sous main de justice soit le support physique de ces données, soit une copie réalisée en présence des personnes qui assistent à la perquisition. » La possibilité d'une authentification sans contact (c'est-à-dire à distance et par champ magnétique) de la carte d'identité s'inscrit dans la logique de généralisation de cette possibilité d'assurer une enquête sans être perçu par le sujet enquêté.

Entre l'émergence des nouvelles modalités d'une interconnexion généralisée et le renforcement du pouvoir inquisitorial d'Etat, la CNIE semble parachever un dispositif de pouvoir qui rend indiscutablement possible une connaissance fine du quotidien des citoyens. Ce pouvoir potentiel, en assurant un véritable bouleversement des équilibres de 78, refonde entièrement le débat de la relation entre informatique, société et pouvoir d'Etat. D'une part, le pouvoir inquisitorial (l'ensemble des forces de police et de justice) tend à répondre à sa propre rationalité administrative de recherche permanente de perfectibilité par l'exhaustivité et l'expansion de ses techniques. D'autre part, la société défend un principe fondamental de l'Etat de droit républicain, à savoir, la préservation de la vie privée face à l'intrusion injustifiée de la puissance publique : ce que Pierre Piazza appelle la défense légitime contre la « colonisation de leur vécu ». Or la CNIE peut être perçue, à ce jour, comme l'aboutissement d'un renversement paradigmatique au service d'une logique managériale et pastorale, qui tend à totaliser la gestion des ressources et des flux (lire pour cela la contribution de Yoval Eched). Partant du modèle où l'enquête a priori aboutissait au fichage d'un suspect sous contrôle judiciaire, le système généralisé de la trace, qui se met en place aujourd'hui, entraîne un fichage généralisé des innocents, dans le secret le plus total, pour en extraire a posteriori des suspects, dans le cadre d'une enquête de plus en plus policière (Perben I et II). On ne peut qu'être saisi par l'analogie entre ce nouveau dispositif d'enquête et le projet du panoptique de Jeremy Bentham tel que Michel Foucault nous l'a révélé dans *surveiller et punir*.

## En guise de conclusion

A l'aune de ce galop d'essai, initié timidement par le ministère de l'intérieur comme entraîné au débat devant l'assemblée nationale, de nombreux indices interrogent l'évolution de la réflexion en France sur le projet INES. En premier lieu, sur le mode de communication initié par un ministère qui n'est visiblement pas habitué au fait que l'on discute ses actions<sup>48</sup>, on peut constater que le jeu des critiques/explications adopte davantage une posture pédagogique que celle d'une ouverture de débat sur un projet dont nul ne connaît véritablement l'avancée<sup>49</sup>. Le débat du Forum des Droits sur l'Internet met bien en tension un espace délibératif ouvert et démocratique où la parole experte et citoyenne, issue de tous les horizons, questionne un discours qui se contente, à ce jour, de se limiter à un argumentaire orthodoxe de la pensée managériale des hauts fonctionnaires. Pourtant, que ce soit dans les interventions des experts ou celles du forum, ces arguments ont tôt fait de disparaître devant un jugement raisonnable. D'un côté, le ministère se plaint de la falsification des cartes d'identité alors que de l'autre, les participants rappellent à juste titre que l'informatique a montré qu'elle était le seul secteur économique et technique incapable de résister au piratage, à la falsification et au détournement. Le ministère nous annonce qu'il faut lutter contre le terrorisme, alors que de nombreux commentateurs pointent la disproportion des dommages collatéraux en matière de libertés civiles, sans avoir l'assurance de l'efficacité de la lutte contre le crime organisé international. Le ministère prône la simplification de la vie quotidienne alors que, jusqu'à preuve du contraire, l'usage d'un dispositif portable de signature électronique nécessite incroyablement plus de ressources cognitives que celui d'un stylo et d'une carte papier. Dans la même veine consumériste, il argue de la nécessité d'investir massivement des dizaines de millions d'euros (combien exactement ?) pour dépenser moins (quelles économies ?). De plus, la CNIE serait la clef de voûte des téléprocédures à venir. Sauf que cela fait désormais près d'une décennie que l'on attend l'arrivée des téléprocédures et que les téléprocédures commerciales (comme la gestion de son compte bancaire sur Internet) fonctionnent très bien sans la CNIE. Il suffit de retirer au guichet ou de recevoir par courrier recommandé son login et son mot de passe. Enfin, la conformité à la contrainte internationale (américaine) et européenne est un argument tellement usité qu'un participant au débat a soulevé la nécessité de délibérer sur la scène nationale.

Tout laisse à penser que, sauf réactions et émotions très vives de la société civile (mais les exemples européens montrent l'atonie de celle-ci), la carte nationale d'identité électronique verra le jour. Pourtant, si l'on prend au sérieux l'invitation du ministère de l'intérieur, et de tous ceux qui travaillent depuis quelques années dans les différents ministères régaliens intervenant sur la question, à délibérer démocratiquement sur l'aboutissement du projet, les points suivants devront être résolus en toute transparence et selon le principe de « bonne foi ». Quels sont véritablement l'utilité et l'apport d'un fichier central d'Etat civil numérique, couplé à un fichier de traces biométriques ? Mesure-t-on réellement les dangers que ce dispositif de pouvoir pourrait faire encourir à la population en cas de nouveau dérapage de nos sociétés modernes ? L'ajout d'un contrôle « sans contact » de l'identité a-t-il une autre fonction que la surveillance policière des

---

<sup>48</sup> Que le représentant du ministère rappelle, durant le débat de Bordeaux du 8 mars 2005, qu'il aurait pu lancer la CNIE par voie réglementaire sans débat, met en évidence l'hésitation avec laquelle il entame la démarche de mise à l'épreuve d'une délibération démocratique. En effet, si l'assertion est vraie en droit, elle s'avère fautive au vu des enjeux politiques du sujet et au regard du précédent de 78.

<sup>49</sup> Même si les années d'élaboration consacrées à ce projet, les marchés publics et les premiers rendus effectués par Thales, nous montrent que, sur la courbe d'un projet TIC, nous en sommes à la phase du premier déploiement du test grandeur nature. Alors, l'hypothèse de restituer ce débat dans la phase marketing de diffusion et d'intégration du produit élaboré à son marché potentiel d'utilisateurs, avec verrouillage final et adaptation réactive, donnerait un sens particulier au mélange discursif entre écoute et explication.

populations<sup>50</sup> ? Y a-t-il aujourd'hui des garanties suffisantes et des contrôles réguliers prévenant d'éventuels abus du pouvoir inquisitorial ? Sommes-nous exempts de tout détournement des fonctions policières au service d'intérêts particuliers ou partisans ? Quelles seront les procédures exactes de l'usage de ces nouvelles capacités de surveillance ? Qui contrôlera et sanctionnera, en toute impartialité et avec les moyens nécessaires, le pouvoir inquisitorial ? A ce jour, le ministère a éludé toutes les réponses en se voulant aussi rassurant qu'évasif.

Nous avons tenté de démontrer que si la problématisation de la CNIE (en termes de fichiers) recoupe largement une réflexion mûre, initiée par le projet Safari en 1974 et la loi informatique et libertés de 1978, la question du traitement des données, comme actualisation d'un fichier virtuel central de la société, pose la véritable question d'un nouveau pouvoir inquisitorial sous un régime démocratique. La véritable généralisation de nos traces numériques indélébiles a redoublé notre quotidien d'une représentation extrêmement fine et totalisatrice de notre vie privée. La nécessité d'une prise de conscience citoyenne sur les bases d'une information exhaustive et claire, l'élaboration de règles respectueuses de la vie privée et des libertés fondamentales et le contrôle effectif des enquêteurs sont autant de caractéristiques qui révèlent la nécessité d'une autorité de régulation indépendante du pouvoir effectif et base d'un forum public. Or le gouvernement, en modifiant la loi informatique et libertés en juillet 2004, a souhaité le contraire pour tout ce qui concerne les forces de police et de justice. S'il a renforcé la CNIL dans ses prérogatives envers les acteurs économiques et la société civile, il a, par les articles 26, 27, 32 (section V) et 44 (section IV), profondément réduit et obscurcit la gestion des fichiers de police et de justice les rendant indiscutables sur la place publique. Il est donc difficile de saisir la stratégie du gouvernement qui d'une part, invite au débat démocratique et d'autre part, réduit la transparence de ses actions en matière de pouvoir inquisitorial.

**Amar LAKEL**

\* \* \*

---

<sup>50</sup> La réponse du ministère de l'intérieur est à ce titre singulière. Il compare les étiquettes RFID de la grande distribution, qui assureront la traçabilité de tous les produits de consommation, à la CNIE. La seule différence étant que, avec la CNIE, seules les forces de police seront habilitées à effectuer ce traçage. Voilà donc un privilège rassurant !

**XI. Contribution de Xavier GUCHET, philosophe, Université de Paris 1 - 30**  
mars 2005

Par **Xavier GUCHET**

Philosophe

Chercheur au CETCOPRA (Centre d'étude des techniques, des connaissances et des pratiques), Université de Paris 1.

Auteur de *Le sens de l'évolution technique*, Editions Léo Scheer, mars 2005

**LA BIOMETRIE ET LA QUESTION DE L'IDENTITE**

Les thèmes de l'identité numérique et de l'identité biométrique ne sont pas équivalents et ne doivent donc pas être confondus. Des données relatives à l'identité d'une personne peuvent être numérisées sans recours à la biométrie. Il est bien sûr impossible de dissocier la biométrie du contexte plus général de la numérisation des documents d'identité ; néanmoins, il convient de souligner les enjeux spécifiques liés à la biométrisation de l'identité.

La notion d'identité biométrique implique deux choses : d'abord, que l'identité d'une personne est quelque chose qui peut être attesté par des *data* biologiques, morphologiques ou comportementaux (*bios*) ; ensuite, que ces *data* identifient une personne dès lors qu'ils sont accessibles à la mesure (*metron*).

La notion d'identité biométrique ne signifie pas que l'identité est considérée en soi comme de nature biométrique, et que l'individu est en soi réduit à des *data* mesurables. Cela signifie que l'identité est requalifiée de façon à donner prise à la mesure. Et si l'identité peut être requalifiée, c'est qu'elle est toujours déjà qualifiée dans un processus qui la construit. L'identité n'est pas une donnée en soi, elle est toujours le produit d'un acte constructif.

La requalification biométrique de l'identité est en l'occurrence indissociable d'un processus technique d'identification, et ce qu'il faut comprendre c'est précisément la nature très spéciale de cet acte constructif de l'identité biométrique.

Dès lors, l'utilisation de la biométrie à des fins d'identification signifie autre chose et plus qu'une simple numérisation de l'identité, au sens où l'identité elle-même ne changerait pas quant à sa nature et quant à la manière dont elle se construit.

Bien au contraire, la biométrisation de l'identité contribue à modifier en profondeur l'identité elle-même, c'est-à-dire la manière dont on la définit et la manière dont elle se construit.

En substance, la biométrie nous fait passer de l'identité à l'identifié, plus précisément elle signifie que l'identité est indissociable d'un processus d'identification, qui est en même temps un processus technique de contrôle.

C'est cela qui est nouveau.

Traditionnellement, l'identité se détermine à partir d'un processus de connaissance ou de reconnaissance sociale. La nouveauté, c'est que nous sommes passés de la reconnaissance à l'identification, de l'être reconnu à l'être identifié techniquement. La différence est dans la mesure et dans la mise en œuvre de techniques de mesure. L'identité sociale, construite dans un processus de connaissance ou de reconnaissance, n'est pas une identité techniquement mesurable ; l'identité biométrique, c'est l'identité construite *via* des techniques de mesure. Dans les deux cas, l'identité n'est pas une réalité déterminée en soi, elle est indissociable d'un processus qui lui donne ses déterminations. Mais ce processus diffère à chaque fois. Ce qui est intéressant dans la biométrie, ce n'est pas de réfléchir à l'identité en soi (qui n'existe pas donc), mais au processus à partir duquel cette identité se détermine.

C'est donc la notion que nous avons de l'identité qui se trouve bouleversée en profondeur. Réfléchir au thème « identité numérique et biométrie », ce n'est donc pas seulement étudier la faisabilité technique de la biométrie, et ce n'est pas non plus seulement évaluer « l'acceptabilité sociale » de la biométrie.

La notion « d'acceptabilité sociale » suggère en effet que les éventuelles implications problématiques de la biométrie, si elles existent (en matière de protection des données personnelles notamment), se traduiront nécessairement par un rejet de la part des usagers. En d'autres termes, pas de rejet, pas de problème. Ou alors, on prétendra que les usagers ne rejettent pas les techniques, parce qu'ils sont contraints, asservis, non libres.

Or, il apparaît que la relativement bonne « acceptabilité sociale » de ces techniques dans les processus de contrôle ne signifie pas que la requalification biométrique de l'identité est sans problème, et ne signifie pas non plus que les gens ne sont pas libres. La question est plutôt la suivante : la biométrie est-elle compatible avec les modalités traditionnelles de la construction de l'identité ? Ne faut-il pas plutôt reconnaître qu'elle introduit une notion inédite de l'identité (construite dans le processus même de l'identification, processus technique de la mesure) dans laquelle les usagers, tout en se conformant aux prescriptions techniques, risquent de ne pas se reconnaître ? Les contextes culturels doivent évidemment être considérés comme déterminants de la façon dont l'éventuelle contradiction, ou incompatibilité entre identité biométrique et identité sociale, va être perçue.

Le problème ne se limite donc pas à la sécurisation des documents d'identité. D'ailleurs, la biométrie est utilisée aussi dans des contextes qui ne sont pas directement liés à la sécurité et au contrôle des flux migratoires. En milieu scolaire par exemple, l'usage de la biométrie pour contrôler l'accès au réfectoire semble se répandre très rapidement, en France et en Europe. Le problème touche plus généralement la construction de l'identité et plus précisément, la confrontation entre plusieurs constructions de l'identité.

En définitive, la biométrie n'est pas un outil au service de problématiques purement techniques. Elle est un instrument de pouvoir. Cela veut dire qu'il faut étudier la biométrie en la resituant dans les relations de pouvoir qu'elle contribue à modifier ou à créer. La biométrie n'est pas au service d'un pouvoir existant qui demeurerait inchangé, dans sa nature et ses modalités d'exercice ; elle fait bien plus que cela : elle modifie la nature même du pouvoir qui s'exerce sur les gens.

Ce thème est apparu fortement dans le contexte scolaire. La biométrie inaugure un type de pouvoir assez nouveau, qui en substance ne passe plus forcément par les surveillants traditionnels et s'appuie sur d'autres relais. Prendre acte de la nature politique de la biométrie, ce n'est pas pour autant reprendre l'idée qu'un nouveau *Big Brother* menace de nous asservir. Les recherches montrent que ce thème n'est pas nécessairement le plus pertinent. Néanmoins, si la biométrie n'est pas l'instrument d'un nouveau Léviathan totalitaire, il faut malgré tout reconnaître sa nature de technologie politique et décrire les mécanismes de pouvoir qu'elle rend possible, et dont elle constitue un point d'appui.

**Xavier GUCHET**

\* \* \*

## **XII. Contribution de l'Observatoire des Usages de l'Internet (OUI) - 4** avril 2005

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

Association dédiée à l'observation et à l'analyse d'usages de l'internet à forte plus value sociale.

L'association Observatoire des Usages de l'Internet (OUI) a été sollicitée par le Forum des Droits sur l'Internet dont elle est membre pour donner son avis dans le débat en cours concernant la carte nationale d'identité électronique (cnie).

Nous prenons ce débat en cours de route : beaucoup d'arguments ont déjà été échangés. A la lumière de notre expérience d'observation et d'analyse d'usages de l'internet reflétée sur le site de l'association <http://oui.net> , nous avons davantage cherché à réagir sur le concept et les usages de la cnie qu'à entrer dans la discussion d'une solution technique.

### **1. L'objet du débat et la responsabilité de son commanditaire**

Une fois mise en place, la cnie deviendra pour chacun un élément fondamental pour accéder et faire valoir ses droits. En consulter les futurs usagers constitue une initiative très positive même si elle ne touche qu'un nombre limité de personnes, sous réserve bien sûr qu'il s'agisse d'une véritable consultation et qu'il soit tenu compte de ses résultats.

Toutefois, la participation au débat a pu introduire chez certains un doute sur son véritable objet : s'agit-il de s'entendre sur les objectifs d'un dispositif à concevoir, ou de faire avaliser un dispositif déjà conçu et d'en suggérer de nouveaux usages ? Le dossier ne propose-t-il pas une réponse avant que ne soient clairement posées les questions ? Le débat ne serait alors qu'un artifice pour médiatiser un service et un produit déjà « ficelé » ? S'il en était ainsi, ce serait une tromperie entachant la crédibilité du commanditaire.

Les archives du forum resteront disponibles. Un forum n'est pas un débat oral où les paroles s'envolent. Chacun pourra revenir à ce qui y a été écrit ; la responsabilité du commanditaire serait lourdement engagée s'il ne tient compte de mises en garde contre des dérives qui se produisent effectivement.

### **2. Légitimité de la cnie**

Il apparaît légitime dans un régime démocratique que le citoyen dispose d'un moyen de prouver son identité de façon à faire valoir ses droits.

Il semble aussi légitime que l'Etat cherche à mettre en place un dispositif sûr pour reconnaître et garantir cette identité et qu'à cette fin il mette en œuvre les techniques les plus avancées à sa disposition.

Par contre la démarche inverse qui serait de partir d'innovations technologiques et de se demander comment en forcer l'utilisation pour le contrôle d'identité serait dangereuse : en effet, l'innovation technologique peut représenter un piège pour les libertés individuelles ; il faut toujours se préoccuper des usages inattendus voire pervers qu'elle peut autoriser.

Tout ce qui est technologiquement possible n'est pas nécessairement éthiquement souhaitable ;

### **3. Un document garant de l'identité de son porteur**

Garantir l'identité des personnes et faciliter l'accès sécurisé aux services par internet, c'est l'objectif assigné à la cnie, et à notre sens il doit rester le seul.

Lui assigner d'autres objectifs « secondaires », impliquant l'enregistrement d'autres informations, serait à notre sens prendre le risque de dangereuses dérives dans son usage.

La cnie ne devrait donc comporter que des informations concernant l'état civil du porteur : nom, âge, nationalité et le moyen de les authentifier : photo, empreintes digitales . Le codage de l'information et double enregistrement des informations sous forme imprimée et électronique dans une puce difficilement falsifiable permet de considérablement réduire les possibilités de fraude.

#### **4. L'éthique de la cnie**

La cnie ne doit pas pouvoir être lue sans le consentement explicite de son porteur (c'est la question sous jacente au débat entre partisans d'une carte « avec contact » ou « sans contact »). Seul le porteur peut affirmer qu'il reconnaît pouvoir être identifié au moyen de cette carte.

La cnie devrait seulement constituer la clé du système de protection et d'accès aux informations personnelles et non leur réceptacle ; elle ne serait en quelle que sorte que la partie émergée d'un système de protection et d'accès aux informations personnelles. Elle autoriserait le porteur ou une personne habilitée à consulter et/ou modifier les données personnelles le concernant selon son niveau d'habilitation.

#### **5. Quelles informations pour quels usages**

L'objectif est donc de fournir une réponse sous forme d'une clé que nous pensons devoir être valable seulement pendant un laps de temps suffisant pour permettre à l'interlocuteur d'ouvrir les tiroirs qu'il est habilité à consulter : ainsi cette clé permettra au policier mandaté d'accéder à certains fichiers de police, au banquier accrédité d'accéder aux comptes personnels de la personne...

#### **6. La tentation d'une carte universelle**

Nous pensons que cette clé ne doit pas en faire plus que la CNI actuelle, mais le faire mieux. Elle ne devrait pas contenir d'autres informations que celles qui lui permettent de garantir son authenticité et d'identifier avec le plus haut degré de certitude son détenteur.

Toute autre information risque d'affaiblir cette fonction principale, d'encourager des compromis concernant ses usages, d'introduire des usages parasites, voire déviants par rapport à son objectif.

En effet, il y a un risque que des intérêts mercantiles ne cherche à s'assurer une influence sur la définition et l'évolution de la carte de façon à permettre des usages dont ils assureraient le développement. Le « marché » de la carte elle-même est déjà considérable par lui-même ; le marché de ses produits dérivés pourrait l'être encore plus et d'autant plus qu'on accepte la prolifération des usages. Si l'on veut rester maître des usages de la cnie, l'Etat doit rester son seul et unique prescripteur.

#### **7. Décrire et valider les scénarios d'usage**

Le projet indique bien les deux objectifs du projet : garantir l'identité des personnes et faciliter l'accès sécurisé aux services par internet. Mais il ne décrit pas clairement les scénarios d'usage envisagés et laisse quelque doute sur leur niveau effectif de sécurité. En effet, si le scénario (présentiel) avec présence simultanée de la personne à identifier et d'une personne habilitée à vérifier son identité et à accéder à un certain niveau d'information à son sujet, semble crédible, il n'en est pas de même du scénario (non présentiel), qui permet l'identification en ligne.

## **8. Un document d'identité unifié**

Aujourd'hui la carte d'identité ne concerne que les personnes de nationalité française. Les étrangers sont porteurs d'autres documents : passeport, carte de séjour, carte de circulation... Ne serait-il pas à la fois plus commode et plus équitable que tout résident en France, voir dans l'Union Européenne soit porteur du même document d'identité.

## **9. Délivrance du document**

La cnie devrait être délivrée à tous « gratuitement », c'est à dire comme un document « existentiel », de la même façon que chaque famille reçoit gratuitement son livret de famille, chaque citoyen devrait recevoir gratuitement sa carte d'identité.

Dans le même esprit, la mise à jour périodique de la cnie, « contrôle technique » nécessaire pour actualiser les données qu'elle contient, devrait être gratuite.

Par contre on peut admettre de facturer un coût lorsqu'il s'agit de la remplacer suite à une perte ou à un vol (ce coût pouvant éventuellement être supporté par une assurance).

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

\* \* \*

### **XIII. Contribution de Claudine GUERRIER, Enseignant chercheur à l'Institut National des Télécoms - 4 avril 2005**

Par **Claudine GUERRIER**

Enseignant chercheur à l'Institut National des Télécoms

Auteur de Droit et sécurité des télécoms, Editions Springer, 2000 et Les écoutes téléphoniques, Editions du CNRS, 2001.

#### **LES CARTES D'IDENTITE ET LA BIOMETRIE**

Depuis le début du vingt-et-unième siècle, la sécurité concerne tous les acteurs économiques et politiques. Il convient de réaliser un équilibre entre la préservation des libertés individuelles, prônées par le Conseil de l'Europe et la Convention européenne de sauvegarde des droits de l'homme, l'Union européenne et la charte des droits fondamentaux et l'exigence de sécurité, indispensable aux personnes publiques comme aux personnes privées.

Les éléments d'identification jouent un rôle privilégié dans cet objectif sécuritaire.

La carte nationale d'identité biométrique est un vecteur de cette politique. Elle permet de justifier de sa nationalité et de son identité. Elle est de plus en plus utilisée dans les pays développés comme dans les pays en voie de développement. Officiellement, la carte d'identité a été introduite en Chine depuis le 1 janvier 2004. Au sein de l'Union européenne, la majorité des Etats, y compris le groupe des cinq<sup>51</sup>, ont adopté une carte d'identité, soit facultative, soit obligatoire.

En matière de biométrie, les techniques les plus utilisées sont la photographie numérique et l'empreinte digitale.

La recherche difficile d'un équilibre entre sécurité et liberté pour les cartes nationales d'identité concerne les flux migratoires et la preuve de l'identité.

#### **I. Carte nationale d'identité et contrôle des flux migratoires**

La carte nationale d'identité intervient dans le contrôle des flux migratoires : cela caractérise le système de Schengen et les documents de voyage.

##### **A) L'Accord de Schengen**

L'Accord de Schengen supprime toute justification de nationalité au sein de certains Etats de l'Union européenne et de l'Espace économique européen tout en permettant la mise en place du Système d'information Schengen.

La Communauté, puis l'Union européenne accordent beaucoup d'importance au principe de liberté. Cette liberté concerne l'économie, mais aussi la libre circulation des personnes au sein de la Communauté européenne. Le 14 juin 1985, un premier accord dit de « Schengen » est signé entre la France, l'Allemagne, la Belgique, le Luxembourg, les Pays-Bas et permet une véritable liberté de circulation pour les personnes physiques qui circulent dans ces entités. Le justificatif de nationalité qu'est la carte d'identité, biométrique ou non, n'est plus demandé. L'Espace de Schengen se développe progressivement. Une Convention<sup>52</sup> est élaborée puis signée le 19 janvier 1990. Elle entre en vigueur en 1995. Des règles communes sont instituées aux frontières extérieures en matière de visas, de droit d'asile.

---

<sup>51</sup> Le G5, qui développe une collaboration en matière judiciaire et dans le secteur de la biométrie, comprend la France, l'Allemagne, l'Italie, l'Espagne, le Portugal

<sup>52</sup> Sur la base de l'accord du 14 juin 1985

L'Espace Schengen s'étend aux Etats membres de l'Union européenne et à certains Etats de l'Espace économique européen<sup>53</sup>. Pour pallier la non-justification de la nationalité, s'est mis en place le système d'information de Schengen. Le SIS est une base de données communes, une interconnexion de fichiers nationaux qui regroupent des données nationales<sup>54</sup>. La protection des données personnelles n'est pas oubliée. Les données afférentes à l'origine raciale, aux opinions politiques et aux convictions religieuses, à la santé, à la vie sexuelle sont interdites<sup>55</sup>.

Le SIS II est en cours de développement. Il vise à prendre en compte l'accroissement du flux d'informations, à contrôler les personnes entrant dans la zone de Schengen, à intégrer dans le fichier central des empreintes digitales, les techniques de reconnaissance faciale et d'iris de l'œil. Les défenseurs des libertés individuelles perçoivent un danger<sup>56</sup> : le SIS II élargit sa fonction policière

## B) Les documents de voyage

La carte nationale d'identité, biométrique ou non, fait aussi partie des documents de voyage. Elle participe, comme le passeport et le visa, au contrôle des flux migratoires.

L'Union européenne et des pays industrialisés rendent obligatoire la biométrie pour les autres documents de voyage que la carte d'identité, les passeports, les visas.

Dès mai 2003, le G8, sous l'impulsion des USA, décidait de choisir pour les passeports un procédé biométrique approprié. Aux USA, le Computer Assisted Passenger Prescreening System contrôle de façon automatisée les passeports dans certains aéroports. Au Royaume-Uni, les autorités ont initié un programme de contrôle des passeports dans certains aéroports. Le programme permet, non seulement de vérifier l'authenticité du passeport, mais aussi d'interroger les bases de données policières britanniques.

Au sein de l'Union européenne, un modèle uniforme de titre de séjour<sup>57</sup> est mis en place pour lutter contre l'immigration clandestine et les séjours irréguliers. Le Conseil de Salonique<sup>58</sup> a décidé l'introduction, pour 2005, de données biométriques pour les documents des ressortissants des pays tiers. La Commission européenne est déjà en charge d'un travail afférent au développement d'un système d'information sur les visas<sup>59</sup>. Elle préconise de retenir deux éléments biométriques pour identifier les personnes et pour mieux sécuriser les titres de séjour et les visas. Les éléments biométriques, dont l'empreinte digitale, sont numérisés et stockés sur une carte à puce. Les Exécutifs sont fermement décidés à sécuriser les passeports et les visas. Le Règlement du Conseil du 13 décembre 2004<sup>60</sup> intègre des indicateurs biométriques dans les passeports<sup>61</sup> et les documents de voyage.

Les cartes d'identité, en tant que documents de voyage, participent à la maîtrise des flux migratoires. En Europe, les cartes nationales d'identité sont des documents de voyage, sauf au Danemark et au Royaume-Uni. Elles sont reconnues comme justificatifs de nationalité, au sein de l'Union européenne, de l'EEE.

---

<sup>53</sup> L'Italie signe les accords le 27 novembre 1990, l'Espagne et le Portugal le 25 juin 1991, la Grèce le 6 novembre 1992, l'Autriche le 28 avril 1995, le Danemark, la Finlande, la Suède le 19 décembre 1996. La Norvège et l'Islande, membres de l'EEE, ont signé un accord avec l'Union européenne le 18 mai 1999. Le Royaume-Uni et l'Irlande s'associent à l'acquis de Schengen avec un certain retard.

<sup>54</sup> Les Etats seuls peuvent décider de l'opportunité de l'inscription dans la base.

<sup>55</sup> En cohérence avec les directives européennes d'octobre 1995 et de juillet 2002

<sup>56</sup> « Le SIS sera passé d'un instrument de contrôle des frontières intérieures de l'Union à un outil plus « proactif » d'investigation et de police » Joëlle Van Buuren « Les tentacules du système Schengen » Le monde diplomatique, mars 2003, p10

<sup>57</sup> Règlement du 13 juin 2002

<sup>58</sup> Il s'est tenu les 19 et 20 juin 2003

<sup>59</sup> VIS

<sup>60</sup> Règlement CE n° 2252/2004 établissant des normes pour les éléments de sécurité et les éléments biométriques intégrés dans les passeports et les documents de voyage délivrés par les Etats membres

<sup>61</sup> Décision de la Commission du 28 février 2005

Elles peuvent participer à la lutte contre l'immigration clandestine.

A Hong Kong, depuis juin 2003, les nouvelles cartes d'identité tendent à lutter contre l'entrée illégale de personnes tentées par la prospérité et les éventuelles perspectives d'emploi. Au Canada, le projet de carte d'identité biométrique a pour but de rétablir un flux continu de circulation des personnes physiques entre le Canada et les USA ; les Canadiens n'auraient pas à solliciter de passeport.

La carte d'identité, preuve de la nationalité, participe à l'effort sécuritaire.

## **II. Carte d'identité et protection des données personnelles**

A) La carte justifie l'identité par une carte normalisée, parfois biométrique

La carte d'identité permet l'accomplissement des actes de la vie courante. C'est le cas pour l'inscription aux examens et aux concours, dans l'utilisation des cartes bancaires.

La carte d'identité fait preuve de la possession d'état. En France, la possession d'état détermine l'exercice des droits réservés aux nationaux français.

Les contrôles d'identité sont considérés dans la plupart des Etats comme licites et légitimes.

Les cartes d'identité sont de plus en plus souvent biométriques. Les techniques biométriques en matière de cartes nationales d'identité sont utilisées notamment dans les pays méditerranéens, l'Espagne, le Portugal, l'Italie. Dans ce dernier pays, la prise des empreintes digitales est obligatoire depuis octobre 2002.

En France, la carte d'identité n'est pas actuellement biométrique, mais sécurisée. Lors de la constitution de dossier d'une demande a lieu un relevé des empreintes digitales de la personne concernée. Les enfants de moins de treize ans sont exemptés de cette procédure. Un projet de carte biométrique est à l'étude ; il comprendrait des empreintes digitales. La CNIL est opposée à un fichier centralisant les empreintes digitales et souhaite que les informations soient stockées sur la carte elle-même.

La carte d'identité n'est pas toujours considérée comme légitime au regard des libertés individuelles. Cette conception trouve sa place dans les pays anglo-saxons, Royaume-Uni, Canada, USA.

Un débat est institué sur cette problématique puisque le Royaume-Uni et le Canada envisagent d'instaurer des cartes d'identité et des cartes d'identité biométriques. La police ne procède pas à des contrôles systématiques ; le citoyen n'est pas tenu de prouver à tout moment qui il est. A la carte d'identité peuvent se substituer le passeport et d'autres documents spécifiques, comme le permis de conduire ou, en Afrique du Sud, la Smartcard<sup>62</sup>.

Dans ces pays où l'accent était mis sur la liberté individuelle, l'introduction d'une carte d'identité biométrique se justifie par la protection des personnes physiques. Le vol d'identité est répandu dans tous les Etats développés mais particulièrement dans ces Etats à tradition libérale. Le vol d'identité consiste dans l'usurpation de l'identité d'une tierce personne, est facilité par les technologies de l'information et de la communication. La création d'une carte nationale d'identité peut apporter une aide à la vie des citoyens. Il s'agit d'une pièce plus fiable que le permis de conduire une automobile ou de voyager.

---

<sup>62</sup> Moyen de paiement

## B) Les cartes d'identité au regard de la protection des données personnelles.

La protection des données personnelles intervient chaque fois qu'une carte biométrique est créée. Les autorités de régulation font connaître leurs réticences quand cela leur semble nécessaire.

Au Royaume-Uni, le 3 juillet 2002, le ministre de l'intérieur a proposé l'introduction d'une carte d'identité qui aurait pour mission la suppression de la fraude aux documents d'identité. Les techniques biométriques étudiées sont l'empreinte digitale et l'iris. Le 26 novembre 2003, le Home Office propose un projet de loi instaurant une carte d'identité qui entrerait en vigueur d'ici 2010, et, qui, dans un premier temps, ne serait pas obligatoire. Une base de données nationale stockerait l'élément biométrique, soit l'empreinte digitale, soit l'iris. Néanmoins, il est possible qu'à terme, la base de données génétiques soit utilisée par la carte d'identité<sup>63</sup>.

Au Canada, le ministère fédéral de la citoyenneté et de l'immigration envisage de rendre obligatoire une carte d'identité avec indications biométriques. Les dérives sont possibles en matière de libertés publiques. Julius Grey, spécialiste de la charte canadienne des droits considère que la carte d'identité fédérale n'est pas dangereuse en soi, mais que la centralisation des données personnelles peut induire des dysfonctionnements.

Des débats sont par ailleurs organisés au Royaume-Uni et au Canada. Les critiques se sont surtout centrées sur les menaces éventuelles à l'encontre des libertés individuelles. Quant à la sécurité, elle n'est pas garantie par une carte biométrique ; un étranger, un résident est en mesure de commettre un acte délictueux ou criminel, malgré la carte d'identité biométrique.

L'équilibre entre sécurité et liberté semble bien difficile à réaliser dans le secteur des cartes d'identité biométriques.

Même si l'acceptabilité apparente des procédés biométriques par la société civile est un argument pour les Exécutifs, les autorités de régulation dans le domaine de la protection des données continuent à mettre l'accent sur le danger que font courir à la vie privée certaines techniques biométriques et la centralisation dans les bases de données. Les autorités de régulation jouent un rôle indispensable dans cette période de transition où la biométrie tend à se généraliser dans une société de l'information avec une marge de liberté sensiblement réduite.

Ce contexte, nuancé et sensible, rend particulièrement opportun un débat riche et varié, où la société civile peut faire entendre ses voix par l'intermédiaire de représentants régionaux ou locaux, où le politique prend en compte les remarques contrastées induites par la perspective de la nouvelle carte d'identité française.

**Claudine GUERRIER**

\* \* \*

---

<sup>63</sup> Au Royaume-Uni, le processus a été interrompu en mars 2005

#### **XIV. Contribution du Club de l'Hyper République - 4 avril 2005**

Par le **Club de l'Hyper République**

Le débat sur la future carte nationale d'identité électronique, lancé par le Forum des Droits sur l'Internet, a été relayé sur le weblog du club de l'Hyper République tout au long du mois de mars.

Le Club de l'Hyper République, qui réunit ceux qui souhaitent participer à l'émergence d'une démocratie électronique associant le plus grand nombre de citoyens, se réjouit de l'existence de ce débat essentiel. C'est le signe d'une volonté de dialogue qui s'inscrit parfaitement dans la logique de la société de l'information. La question d'une carte nationale d'identité électronique ne se pose pas vraiment. A l'instar de nombreux pays, la France s'engage sur la voie d'une plus grande efficacité en se dotant des outils modernes qui lui permettront de mieux lutter contre toutes les formes de délits. Ce sont les modalités qui accompagneront cette nouvelle carte qui suscitent de nombreuses questions, notamment sur l'utilisation des informations personnelles qu'elle contiendra et sur son utilisation dans la vie quotidienne par chacun d'entre nous.

##### **Le syndrome « Big Brother »**

La crainte suscitée par l'utilisation de données personnelles stockées sur des systèmes centralisés est réelle et ne disparaîtra que s'il est clairement établi que les informations seront stockées sur la carte elle-même, plutôt que sur un serveur informatique central, ou qu'elles ne feront pas l'objet de traitements croisés sans l'accord préalable de leur propriétaire. Notre héritage historique nous impose, plus qu'ailleurs, de faire preuve d'une grande vigilance quant à l'utilisation d'informations personnelles par les administrations, tout en rappelant que la carte d'identité n'est pas obligatoire en France.

Un autre aspect fréquemment mis en avant est la « privatisation » de l'identité numérique. Les administrations qui utilisent déjà un dispositif d'identité électronique, par le biais de certificats, déploient des services délivrés par des sociétés privées, parfois étrangères. Les fournisseurs de certificats suivent une logique commerciale qui les conduit à proposer la technologie de l'environnement dominant, et les administrations s'adaptent à l'état du marché en n'utilisant que cette technologie. Ainsi s'installe un monopole. Il faut donc clarifier le rôle de l'Etat dans la délivrance de l'identité électronique, fonction régaliennne par excellence.

##### **Une e-carte, pourquoi faire ?**

A quoi servira cette carte d'identité électronique ? Servira-t-elle uniquement à nous identifier lors d'un contrôle de police ? Pourra-t-elle servir d'outil de transactions de la vie quotidienne, pour effectuer des démarches administratives, pour acheter en ligne, pour voter ? Intégrera-t-elle le permis de conduire et la carte santé ? Comment gérer des « identités multiples » qui ne nécessitent pas les mêmes contraintes d'identification ?

Si l'idée de rassembler sur une seule carte les fonctions d'identité et de ses droits associés, comme le permis de conduire ou la carte d'électeur, peut séduire par la simplification qu'elle apporte, elle ne suscitera l'adhésion qu'accompagnée d'explications claires et d'engagements précis quant aux conditions d'accès à ces informations. Après tout, un policier effectuant un contrôle d'identité n'a pas à savoir si la personne contrôlée est inscrite sur les listes électorales.

Comment justifier les coûts de production de cartes à puce à une large échelle ? Si le passage à la carte électronique entraîne la suppression de la gratuité de la carte d'identité, quels bénéfices en tireront les citoyens ? S'il s'agit d'une carte à puce supplémentaire, qui devra trouver sa place aux côtés de la carte santé, des cartes

bancaires, des cartes de grande distribution ou de fidélité, l'intérêt n'en sera que faible.

Le débat actuellement mené vise à informer les responsables du projet de carte d'identité électronique de l'état de l'opinion sur différentes options. Il devra être poursuivi après l'adoption du dispositif retenu par une large campagne de sensibilisation et d'explications en direction du grand public.

Il conviendra aussi de ne pas séparer, une fois de plus, les notions d'e-administration et d'e-démocratie. La Carte nationale d'identité électronique ne doit pas être un simple vecteur de l'e-administration, mais aussi un symbole de citoyenneté !

**Club de l'Hyper République**

\* \* \*

## **XV. Contribution d'Olivier ITEANU, Avocat à la Cour d'Appel de Paris - 8 avril 2005**

Par **Olivier ITEANU**

Avocat à la Cour d'Appel de Paris et Chargé d'Enseignement à l'Université de Paris XI.

Auteur de "Tous cybercriminels", Editions Jacques Marie Laffont, 2004.

### **BIOMETRIE, UNE TECHNOLOGIE A SURVEILLER**

Les travaux sur la carte nationale d'identité électronique revêtent pour la société de l'information une importance toute particulière.

En effet, du point de vue de la systémique et de l'une de ses applications, la cybernétique, cette nouvelle société est un système en soi, c'est-à-dire qu'elle présente les trois caractéristiques habituelles du système. La première caractéristique d'un système est qu'il réunit un certain nombre d'éléments en interaction dynamique. D'un certain point de vue, la place de l'homme parmi ses éléments pose questions mais là n'est pas notre actuel débat. Seconde caractéristique, ces éléments sont structurés selon une organisation complexe et mouvante. La place respective de la loi et des structures techniques, pour savoir qui domine l'autre dans la hiérarchie des normes (la gouvernance), pose là aussi question. Enfin, un système est dit global en ce sens qu'il dispose d'une personnalité, d'une « identité », qui dépasse la simple addition des éléments qui le composent. Dans le cas de la société de l'information, le réseau est un des éléments du système, c'est surtout la représentation de ce système. Dans ce contexte, la plupart des paradigmes de la société réelle se retrouvent dans le nouveau système mais à des places différentes et selon une structuration bouleversée. Dès lors, il paraît tout à fait légitime que la question de l'identité se trouve bouleversée pour toutes les raisons exposées dans le présent débat.

Pour autant, il nous semble ici que le débat tel que posé en Europe et surtout aux Etats-Unis est bien plus ambigu que l'objectif parfois annoncé. Au-delà de trouver de nouvelles représentations à l'identité de l'homme numérique, il s'agit aussi souvent de renforcer les éléments de contrôle sur les individus dans le nouvel espace numérique et même ailleurs. A ce titre, les travaux menés par L'OACI sur le déploiement des technologies biométriques dans les documents de voyage ont de quoi inquiéter. De son côté et de manière moins massive, le projet INES s'inscrit dans cette recrudescence de l'utilisation de la biométrie.

Pour le grand public, cette recrudescence a sonné comme une intrusion dans la vie quotidienne et s'est matérialisée sous la forme d'une annonce : les futurs passeports de nombreux Etats comporteront dans un futur proche des données biométriques, de type copie des empreintes, reproduction des traits du visage ou image de la rétine. Dans les suites des attentats du 11 Septembre 2001, ce sont les officiels états-uniens, et en particulier le Congrès Américains qui, le premier, a décidé la mise en place effective de ces nouveaux passeports au 26 Octobre 2005.

Pour les entreprises, les technologies biométriques sont désormais largement évoquées comme technique d'authentification à l'entrée de leur système d'information, c'est-à-dire comme usage d'un moyen technique, logiciel et / ou matériel, permettant d'identifier et d'authentifier une personne cherchant à accéder à un système d'information.

Parallèlement, la Loi a évolué au cours de l'été 2004, donnant à la Commission Nationale de l'Informatique et des Libertés (CNIL) le pouvoir de fixer les règles

dans ce domaine, ce qu'elle devrait faire prochainement. Des règles qui devraient suivre la Doctrine élaborée par cette même CNIL pour divers traitements comportant des données biométriques qui ont déjà été soumis à son appréciation.

### **La biométrie comme technique d'authentification**

Par les techniques d'authentification, il s'agit de sélectionner à l'entrée d'un système les candidats qui se présentent à l'effet de ne laisser pénétrer que ceux disposant de droits d'accès. Bien évidemment, la finalité d'une telle authentification consiste à interdire l'accès au système à un intrus sans droits quel que soit son mobile, pénétration dans un but de vol d'informations, de sabotage ou même de simple visite. L'authentification d'un utilisateur à l'entrée du système se fait habituellement selon au moins l'un des trois critères suivants :

Critère 1 : ce que sait l'utilisateur,

Critère 2 : ce que possède l'utilisateur,

Critère 3 : ce qu'est l'utilisateur.

Ce que sait le candidat à l'accès, c'est le plus souvent un identifiant (login) et un mot de passe (Pin Code) géré par un système autonome. Ce code lui a été confié par le maître du système. Si on se trouve dans une relation de travail, la notion de garde du code d'accès et de responsabilité à son égard, se trouve souvent incluse dans les chartes d'usage Internet des entreprises. Le code d'accès et le mot de passe peuvent se trouver à distance, c'est-à-dire résider sur le système lui-même, comme un code d'accès à un immeuble. Selon le second critère, ce que possède un candidat, c'est la clef, la carte l'autorisant à pénétrer dans le système. Enfin, selon le critère n°3, ce qu'est l'utilisateur, c'est le recours à la technologie biométrique qui se définit habituellement comme la science des variations biologiques. Elle comporte deux grandes applications : l'identification d'une personne au sein d'un groupe de personnes et l'authentification d'une personne se présentant à l'entrée d'un système d'information, voire d'un local physique. Seule cette seconde application nous intéresse ici, s'agissant des systèmes d'information. Cette technologie fait appel aux caractéristiques physiques de ceux qui détiennent un droit d'accès, on parle alors de reconnaissance biométrique. Le principe est simple : chacun est son propre authentificateur. De l'empreinte digitale, au contour de la main, à l'empreinte vocale en passant par l'empreinte rétinienne, toutes les reconnaissances physiques sont en théorie légalement admissibles. On dit que la biométrie est la forme la plus ancienne d'authentification. Les animaux eux mêmes l'utiliseraient à leur façon. On parle d'authentification forte lorsque deux des trois critères précités se combinent pour authentifier. Par exemple, les code et mot de passe se trouvent détenus par le porteur lui même, comme le code confidentiel d'une carte bancaire enregistré sur la puce de la carte elle-même et gérant l'accès aux terminaux de paiement. Pour revenir à la biométrie, les experts techniques voient au passif de cette technologie, d'une part, son coût, d'autre part, la question de sa révocation. En effet, face à une personne qui a subtilisé un mot de passe ou une signature électronique, le titulaire du mot de passe ou de la signature peut le remplacer ou le révoquer. En revanche, comment faire s'il y a « vol » de l'empreinte digitale ou rétinienne ? Si un tiers s'approprie une telle identité biométrique, il peut passer tout type d'actes au nom du titulaire de l'identité usurpée. Si les experts en sécurité prétendent disposer de solutions à ce problème, ils y reconnaissent cependant là une difficulté au passif de cette protection technique. Or, pour le juriste, une telle difficulté ne peut être envisagée que sous l'angle technique, elle doit également être vue sous l'aspect sociétal. C'est la raison principale du traitement d'exception réservé à la biométrie dans l'arsenal législatif

français et européen. Bien qu'autorisée, la biométrie n'en est pas moins sous surveillance, car jugée dangereuse pour le citoyen.

### **La biométrie sous la surveillance de la Loi**

La biométrie étant une technologie associée à un individu personne physique constitue une donnée à caractère personnel c'est-à-dire, selon la définition posée par la Loi, une « *information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres.* » En cela, tout traitement portant sur la reconnaissance biométrique entre dans le cadre de la loi relative à l'informatique aux fichiers et aux libertés et dans le champ d'investigation de CNIL. Or, la Loi n°2004-801 du 6 Août 2004 venue réformer la Loi informatique et libertés de 1978, a introduit une réforme importante dans le régime des formalités préalables devant être effectuées par les propriétaires de traitement (les ficheurs selon une terminologie ancienne). Sous l'empire de la Loi nouvelle, huit catégories de traitements sont désormais soumis à un régime d'autorisation préalable alors que sous la Loi ancienne, ces mêmes traitements mis en oeuvre par une personne de droit privé, n'auraient fait l'objet que d'une simple procédure de déclaration, c'est à dire du dépôt par le déclarant d'un dossier complet sans possibilité pour la CNIL d'y opposer un quelconque contrôle pour, par exemple, juger de la dangerosité du traitement. Dans le système actuel, le régime de l'autorisation préalable signifie que la CNIL se réserve la possibilité de juger de la dangerosité du traitement qui lui est soumis par rapport, notamment, au but recherché (principe dit de proportionnalité) et, surtout, de le refuser. Or, aux côtés des traitements de données sensibles, par exemple celles faisant apparaître les origines raciales ou religieuses des fichés, ou des traitements portant sur des données relatives aux infractions et condamnations ou encore ceux susceptibles d'exclure les personnes d'un droit, les fichiers débiteurs par exemple, l'article 25 de la Loi modifié énonce la catégorie des traitements automatisés « *comportant des données biométriques nécessaires au contrôle de l'identité des personnes* ». De tels traitements vont donc requérir l'autorisation préalable de la CNIL avant leur mise en oeuvre. Cette innovation de la Loi nouvelle n'est que la légalisation de la Doctrine de la Commission qui, à diverses occasions, a dit sa méfiance face à de tels traitements. Ainsi, dans deux délibérations rendues le même jour, le 8 Avril 2004<sup>64</sup>, la CNIL a fixé quelques points de repères qui démontrent la vigilance dont elle fait preuve face à cette technologie. Ces deux délibérations devraient en toute logique être reconduites dans le nouveau cadre légal et guider les décisions d'autorisation de la Commission vis à vis des traitements biométriques. Dans la première délibération, le centre hospitalier de Hyères envisageait de mettre en oeuvre un traitement personnel consistant à horodater les entrées et sorties de son personnel en s'appuyant sur un dispositif de reconnaissance de l'empreinte digitale. La CNIL a émis un avis défavorable à la mise en oeuvre de ce traitement. Pour motiver cet avis négatif, la CNIL s'appuie sur deux types d'arguments. D'une part, elle critique la centralisation des données biométriques sur un serveur central y voyant là une solution qui « *n'est pas de nature à garantir la personne concernée de toute utilisation détournée de ses données biométriques* », d'autre part, elle se fonde sur une disposition insérée au Code du Travail selon laquelle « *nul ne peut apporter aux droits des personnes et des libertés individuelles ou collectives des restrictions qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché.* »<sup>65</sup>. Elle considère dès lors que « *seul un impératif de sécurité est susceptible de justifier la centralisation de données biométriques* » y voyant au contraire dans le cas du centre hospitalier de Hyères un

---

<sup>64</sup> Délibérations n°04-017 et 04-018

<sup>65</sup> L'article L 120-2 du code du travail

traitement disproportionné par rapport à la finalité recherchée, soit la gestion du temps de travail . S'agit il pour autant d'une condamnation par avance de toute mise en œuvre d'un traitement biométrique ayant pour finalité la gestion du temps de travail dans une entreprise ? Rien n'est moins sûr : sur son site Internet, la CNIL ne pose pas d'exclusion de ce genre. En revanche, elle insiste sur le fait que les caractéristiques biométriques d'une personne « *doivent être uniquement conservées sur un support individuel (carte à puce, ordinateur...)* et non dans une base de données regroupant les caractéristiques anthropométriques de plusieurs personnes (base centrale ou lecteur biométrique) ». Elle affirme par ailleurs qu'elle n'admettra une dérogation à ce principe que si le demandeur à l'autorisation peut faire valoir un « *impératif* » de sécurité rendant nécessaire la centralisation des données biométriques. Dans la seconde délibération du même jour, la CNIL va en revanche donner un avis favorable à l'établissement public Aéroports de Paris pour un système de contrôle d'accès aux zones réservées de sûreté des aéroports d'Orly et de Roissy. Logiquement et compte tenu de la première délibération évoquée ci-dessus, la Commission retient ici que « *seules sont enregistrées sur le badge le gabarit biométrique, le numéro du badge et le code PIN associé au badge* » notant par là que les données biométriques résident avec la personne et que, au regard de l'application concernée; « *Ces données sont adéquates, pertinentes et non excessives* ».

Ces deux délibérations ont été rendues sous l'empire de la loi ancienne de 1978 mais, quant aux règles de fond qu'elles posent, la CNIL a déjà affirmé et écrit qu'elle reconduira sa Doctrine dans le nouveau cadre légal qui lui donne la haute main pour autoriser ou refuser un traitement comportant des données biométriques. Passer outre l'autorisation de la CNIL risque de coûter cher, puisque, pour mémoire, « *le fait, y compris par négligence, de procéder ou de faire procéder à des traitements de données à caractère personnel sans qu'aient été respectées les formalités préalables à leur mise en œuvre prévues par la loi est puni de cinq ans d'emprisonnement et de 300 000 € d'amende* »<sup>66</sup>. La situation légale de la biométrie soumise à autorisation préalable de la CNIL nous rappelle que toutes les technologies ne sont pas égales devant la Loi. Corrélativement, cette différence de traitement a le mérite de nous rappeler également que les technologies ne sont pas neutres quant à nos libertés de citoyens. De ce point de vue, la biométrie mérite sans doute le traitement particulier qu'on lui inflige aujourd'hui dans la Loi.

**Olivier ITEANU**

\* \* \*

---

<sup>66</sup> Article 226-16 du Code Pénal

## **XVI. Contribution de Patrice FLICHY, Professeur de sociologie à l'Université de Marne-la-Vallée – 13 avril 2005**

Par **Patrice FLICHY**

Professeur de sociologie à l'université de Marne-La-Vallée, co-auteur du livre blanc "*Administration électronique et protection des données personnelles*" (2002).

Il a écrit notamment *L'innovation technique : vers une nouvelle théorie de l'innovation ?* (La Découverte, 2003) et *L'imaginaire d'Internet* (La Découverte, 2001).

### **CARTE NATIONALE D'IDENTITE OU CARTE DE TRANSACTION ADMINISTRATIVE OU COMMERCIALE**

Le titre d'identité que l'Etat délivre à un individu permet à celui-ci de pouvoir attester de son identité, avec le maximum de garanties. Le processus actuel de production de ce titre d'identité relie des registres d'état civil qui comporte le nom, les prénoms et la filiation à des éléments matériels détenus par l'administration (photographie numérisée, empreinte digitale). Ce processus d'identification se fait sans « fichier centralisé ». En effet si les fichiers d'état civil sont numérisés, ils ne sont pas connectés.

Pour lutter contre la fraude et rendre plus sûr la procédure actuelle, le ministère de l'Intérieur envisage d'établir une nouvelle carte d'identité munie d'une puce électronique. Celle-ci comprendra les données écrites sur la carte (nom, prénoms, date et lieu de naissance, sexe, adresse) la photo et les empreintes digitales numérisées. Mais ce nouveau document n'est pas seulement plus sûr et plus difficilement falsifiable, son processus de production a fondamentalement changé. Puisqu'il y aura, à l'avenir, un dispositif centralisé des cartes d'identité et des données biométriques sur les individus.

Le changement qui est envisagé a donc une double nature : fiabilité plus grande de la nouvelle carte, création de fichiers centralisés. Si le premier point paraît a priori peu contestable, le second l'est beaucoup plus. A partir du moment où la carte d'identité électronique est considérée comme quasiment infalsifiable et où les données protégées par la puce peuvent être, dans le cadre des conditions légales, comparées aux caractéristiques de l'individu, on peut très sérieusement se demander si le fichier central est vraiment indispensable, et si on ne peut pas se contenter comme auparavant de fichiers des personnes recherchées. La CNIL rappelle à juste titre qu'un système centralisé « n'est pas de nature à garantir la personne concernée de toute utilisation détournée de ses données biométriques »<sup>67</sup>. Un tel dispositif qui est donc dangereux pour les libertés individuelles ne pourrait donc être justifié que s'il était capable d'apporter une amélioration très forte en matière de sécurité nationale et de lutte contre le terrorisme. La démonstration reste à faire. En attendant, on peut se demander si un tel fichier est vraiment nécessaire et si les pouvoirs publics ne se contentent pas de s'aligner sur la mode du tout sécuritaire.

#### **Carte d'identité et signature électronique**

Dans le projet actuel de carte d'identité électronique, on envisage également de faire de ce nouveau document, le « couteau suisse de l'identité électronique ». Le titulaire de cette carte pourrait l'utiliser pour accéder aux téléservices administratifs, ou pour des transactions électroniques privées. Il pourrait enfin

---

<sup>67</sup> Délibération du 8 avril 2004 cité par Olivier Iteanu, dans ce forum

stocker dans cette puce des données personnelles qu'il souhaite avoir constamment avec lui.

Il est certain que de disposer d'une carte multifonction pourrait simplifier de nombreuses activités quotidiennes, rendre plus routinier et donc plus facile l'accès aux services en ligne tant administratifs que commerciaux. Un tel projet nécessite cependant que les usagers disposent d'un lecteur de carte et on peut d'ailleurs se demander s'il revient au ministère de l'Intérieur de prôner cette solution technologique qui engage les autres administrations, et les fournisseurs de service en ligne. Enfin, pour l'utilisateur, l'intégration a aussi des inconvénients. La perte de cette carte deviendrait beaucoup plus préjudiciable que celle d'une « simple » carte d'identité.

Mais ce n'est pas seulement en terme d'usabilité qu'il faut faire porter le débat, mais aussi en terme de défense des libertés individuelles. Dans le Livre blanc que nous avons remis au ministre de la Fonction publique, en 2002, Pierre Truche, Jean-Paul Faugère et moi-même recommandions qu'un grand nombre de téléservices puissent s'effectuer, comme c'est le cas aujourd'hui, de manière anonyme, sans contrôle d'accès, ni identification<sup>68</sup>. On peut craindre qu'à partir du moment où la carte d'identité comprendra une puce avec la signature électronique, ce mode d'identification/authentification devienne le mode habituel, puis un jour standard, des relations entre l'administration et les usagers. La relation anonyme qui doit être la norme quand il n'y a pas échange de données confidentielles serait ainsi amenée à disparaître. Dans le domaine privé, Thierry Piette-Coudol rappelle également sur ce forum que de nombreuses relations commerciales n'ont pas besoin d'une identification aussi précise que celle que fournit le certificat électronique et qu'il n'est pas souhaitable, là encore, que cette utilisation se généralise.

En ce qui concerne l'utilisation de la carte pour d'autres données que celles touchant à l'identité, il faut d'abord rappeler la jurisprudence de la CNIL qui encadre très strictement l'interconnexion de fichiers. La commission prévoit notamment l'utilisation par les différentes administrations d'identifiants qui leur soient propres et qui soient donc distincts du NIR qui est géré actuellement par l'INSEE et utilisé dans la sphère sociale. Au-delà de la séparation des identifiants, la CNIL souhaite plutôt que l'administration électronique soit organisée de façon distincte dans chaque domaine de l'action publique. C'est ainsi que l'administration fiscale a mis au point un certificat électronique qui n'est utilisable que pour la déclaration d'impôt en ligne. De même lors des audiences de préparation du livre blanc, nous avons étudié différentes pistes pour mémoriser le certificat électronique, la solution à première vue séduisante d'utiliser la puce de la carte la plus répandue dans le public Sesame-Vitale a finalement été abandonnée, par ce que les responsables de ce système ne souhaitaient pas utiliser leur carte ailleurs que dans la sphère de la santé.<sup>69</sup> On peut donc estimer qu'il est souhaitable d'en faire de même avec la CNIE. C'est un instrument qui doit garantir l'identité public et se limiter à cette fonction.

Dans une vision multi fonction encore plus étendue, le programme INES ( Identité nationale électronique sécurisée) envisage d'offrir au citoyen un coffre-fort sécurisé, dit « portfolio personnel » qui permettrait de stocker différentes données personnelles. Cette idée peut paraître là aussi très séduisante pour l'utilisateur. Sa carte d'identité devient ainsi un document aux multiples usages. Ce projet peut néanmoins susciter des craintes (en dépit des garanties de sécurité offertes par le

---

<sup>68</sup> Pierre Truche, Jean-Paul Faugère, Patrice Flichy et Maurice Ronai *Administration électronique et protection des données personnelles*, Paris, La Documentation française, 2002

<sup>69</sup> Ibidem p. 86

projet) d'un contrôle grandissant de l'Etat. Même si toutes les garanties peuvent être fournies, le citoyen peut craindre que la police n'accède ainsi à ces données personnelles, sans même l'en avertir.

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.

**Patrice FLICHY**

\* \* \*

## **XVII. Contribution de Thomas Lamarche, enseignant chercheur à l'université Lille 3 – 21 avril 2005**

Par **Thomas LAMARCHE**

Enseignant chercheur à l'université Lille 3, membre du comité de rédaction de la revue Terminal. Il a coédité le n° 88 de cette revue : « Fichiers et libertés : le cybercontrôle 25 ans après », L'Harmattan, automne hiver 2002-2003.

### **Fichage à tous les étages ?**

Le gouvernement de la République française devrait très sérieusement de faire le point sur la question des libertés confrontées aux systèmes informatiques : libertés dont la situation est tendue car les choix gouvernementaux et européens en faveur d'une logique sécuritaire se sont affirmés.

Les attentats contre le *World Trade Center* et le Pentagone et la menace terroriste en général sont mobilisés pour justifier une série de mesures de renforcement des pouvoirs d'investigation des services de police et autres organismes de contrôle.

Parmi ceux-ci figure en bonne place la carte d'identité électronique.

Le discours sécuritaire surfe sur des peurs réelles et imaginaires, les renforce pour proposer des solutions simplistes et visibles. La démagogie des solutions policières et carcérales cache mal une crise de l'État, de sa légitimité et de ses moyens d'action en dehors de sa fonction sécuritaire.

La mise en avant des peurs et des menaces justifie un renforcement des systèmes de contrôle des citoyens et des organisations. Dans le domaine des réseaux électroniques, et du contrôle en général, la thématique de la sécurité et de la surveillance est favorisée par des outils de plus en plus puissants. Le virus comme le *hacker* ou le terroriste hantent le monde informatique, souvent mythifiés autant par les protagonistes (valorisation de l'exploit informatique), que par les sociétés de surveillance informatique et les médias.

### **Mémoire étendue et non maîtrisée**

Les mémoires informatiques ne servent pas seulement les volontés de contrôle, elles les dépassent en gardant des traces au-delà de l'intention initiale. Comme la CNIL le rappelle régulièrement : "*Jadis nous étions fichés parce que quelqu'un souhaitait nous fiché. Aujourd'hui, nous pouvons aussi être fichés du seul fait de la technologie qui produit des traces sans que nous en ayons toujours pleinement conscience*" (Michel Gentot, alors président de la CNIL, Rapport annuel CNIL 1999).

Un risque majeur de dérapage de la carte électronique ne vient pas nécessairement d'une intention (notamment d'une intention actuelle de fichage systématique, de recoupement de fichiers, de contrôle de la population). La convergence entre les capacités techniques de contrôle et le renforcement d'une vision policière de l'État réduit le champ des libertés publiques. Rien ne garantit sérieusement l'extension du domaine de compétence de la mémoire de la carte d'identité électronique.

La très faible transparence, pour ne pas dire l'opacité fondamentale, de la puce, n'offre pas de droit de regard du citoyen. Le système technique que l'on met en place permet, sans nécessaire intention, d'exercer un suivi d'un nombre incalculable de traces informatiques que nous laissons presque partout. Dans le cas de la carte d'identité électronique le champ de l'information personnelle fournie aux lecteurs semble extensible sans garantie. Aucun dispositif technique, aucune profession de foi ne suffit à limiter les utilisations multiples, variées et finalement incontrôlables des informations disponibles.

La carte d'identité électronique donne corps à des risques majeurs pour les libertés individuelles. L'interconnexion de fichiers et la construction d'une sorte de fichier géant (ou une mise en réseau de fichiers), si elle peut être réfutée a priori, est

rendue possible. Le caractère obligatoire de la carte constitue une évolution très forte des pratiques, et favorise la création d'un fichier global de la population.

Au-delà du questionnement sur la carte elle-même, on se demande ce qui pousse une société à accepter ces contrôles envahissants. Quelle transformation s'est opérée pour que le corps social accepte de se mutiler d'une part de sa liberté et d'autre part de son intimité ? En laissant se développer un contrôle à tous les étages, bien sûr c'est le contrôle de l'autre, du déviant potentiel, de celui qui menace qui est visée. Pourtant la constitution des fichiers autant que l'assouplissement des conditions d'interpellation par la police touche l'ensemble de la population. Il faudrait approfondir les motivations de cet asservissement volontaire.

La carte d'identité électronique est issue d'un rêve technique qui entretient le fantasme d'un contrôle des risques. Il est vain de penser qu'un système informatisé participe sérieusement au suivi des terroristes ; il est plus vain de croire que nos institutions sauront éviter la tentation de recouper tous ces fichiers, et d'ajouter des informations personnelles qui doivent rester confidentielles (santé, opinion, dossiers fiscaux ou judiciaires...)

Il me semblait utile de rappeler ces différents risques et de pointer l'absence de réflexion du pouvoir politique sur les conséquences de l'utilisation de la technique et des fichiers. L'organisation d'un débat public n'est pas si fréquente, il s'agit pour chacun de s'en saisir. Bien-sûr la question est très complexe, car elle mêle technique et droit, philosophie et sociologie des usages, et bien d'autres aspects encore. L'ensemble des contributeurs, j'en suis persuadé, estime nécessaire de mettre en garde la population et les dirigeants contre la construction d'outils que nul ne saurait utiliser sans risque pour la liberté et l'intimité. Le meilleur exemple de la méfiance que nous devons avoir à l'égard d'un usage immodéré des fichiers et des systèmes de contrôle de la population est la prise de position du ministre de l'intérieur lui-même alors que le débat est loin d'être terminé et que les positions qu'il enregistre ne donnent pas signe de blanc-seing. M de Villepin propose en effet une version assez radicale du projet (carte obligatoire et associée à d'autres services). Le débat public vaut bien plus que cela)

**Thomas LAMARCHE**

\* \* \*

## **XVIII. Contribution de Pierre TRUDEL, Professeur à l'Université de Montréal, Canada – 11 mai 2005**

Par **Pierre TRUDEL**

Professeur à l'Université de Montréal, Titulaire de la Chaire L.R. Wilson sur le droit des technologies de l'information et du commerce électronique, Centre de recherche en droit public.

Auteur de nombreux ouvrages dont *Améliorer la protection de la vie privée dans l'administration électronique : pistes afin d'ajuster le droit aux réalités de l'État en réseau*, (réalisé pour le Ministère des Relations avec les citoyens et de l'immigration Montréal, mars 2003) et *Cyberspace and Electronic Commerce law : general principles and legal issues* (Montreal, Canada-China Senior Judges Training Project, Juin 1999).

### **QUELQUES RAPPELS, IDEES ET PRINCIPES**

#### **Un processus inhérent à la vie sociale**

L'identification est un processus inhérent à la vie sociale. Au coeur des pratiques sociales les plus essentielles, les mécanismes d'identification sont une composante du tissu culturel d'une société. La façon dont on s'identifie en dit long sur les tendances lourdes d'une société. Alors que dans certains pays, l'État est perçu comme un acteur majeur de la mise en place de tout processus d'identification, ailleurs, on postulera que c'est un domaine où l'État n'a pas à mettre les pieds!

Mais au delà de ces traits culturels, pour assurer le déroulement de la plupart des activités, tous doivent procéder à l'identification des personnes physiques, des personnes morales et des choses. Il est en effet essentiel, pour la plupart des interactions humaines, de savoir à qui l'on a affaire.

On définit l'identification comme un processus d'information par lequel on compare de l'information afin d'avoir le degré de certitude requis à l'égard des qualités de la personne avec laquelle on entre en contact. Essentiellement, l'identification est un processus destiné à réduire l'incertitude. Il vise à procurer la quantité optimale d'information à l'égard d'une personne afin de pouvoir procéder à la transaction avec un niveau de risque acceptable.

Par exemple, on va requérir plus ou moins d'information selon que l'on se propose de réaliser une transaction avec un inconnu ou avec une personne que l'on connaît de longue date. De la même façon, plus la transaction envisagée comporte des enjeux importants, plus on voudra disposer d'informations afin de s'assurer de l'identité du co-contractant. Inversement, pour les transactions à enjeu mineur ou dérisoire ou encore lorsque l'identité du co-contractant n'a pas d'importance, on ne va pas rechercher les informations relatives à l'identification du co-contractant. Dans ce dernier cas, l'analyse que l'on fait des risques de la transaction porte à conclure qu'il ne faut qu'un minimum d'informations.

Pour effectuer ces évaluations et pour obtenir le degré recherché de certitude, on aura besoin de plus ou moins d'informations. Il sera parfois nécessaire d'avoir recours à des mécanismes de validation ou de corroboration des informations pouvant permettre d'accroître le degré de certitude à l'égard de l'identité d'une personne. Ces rappels montrent bien que l'identification est une activité visant essentiellement à réduire ou gérer les risques inhérents aux interactions. Mais cela met également en lumière le fait que l'identification se présente sous plusieurs facettes puisque les transactions auxquelles nous prenons part ne sont pas toutes de même importance.

## **Les risques de dérives**

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. C'est comme si l'on envisageait la construction de routes en postulant que l'ivresse au volant et ses conséquences désastreuses est une conséquence inévitable de l'acte de conduire une automobile ! Le droit de la protection des données personnelles s'est construit sur les frayeurs suscitées par les technologies de l'information. Rituellement, on exprime des préoccupations sur le potentiel liberticide des technologies de l'information. On escompte que le potentiel d'abus sera nécessairement et universellement réalisé pour justifier un cadre juridique qui est supposé protéger les personnes contre les périls, voire les apocalypses, que laissent craindre les technologies de l'information pour les libertés. Lorsqu'elle est appliquée à l'analyse des enjeux des services gouvernementaux en ligne, cette approche des technologies de l'information prive d'une analyse qui donnerait lieu à la mise en place de cadres juridiques plus adéquats pour assurer l'implantation des services publics en ligne en améliorant effectivement la protection de la vie privée.

Il faut disposer des arguments relatifs à la surveillance policière. La plupart des craintes à l'égard de l'usage des technologies de l'information concernent les opérations de surveillance policière. On invoque les risques très réels d'abus policiers pour s'opposer aux innovations ou pour justifier le renforcement et souvent la bureaucratisation du droit de la protection des données personnelles. Pourtant, les informations que peuvent obtenir et détenir les forces de police et autres forces de sécurité échappent à toutes fins pratiques à la portée des lois sur la protection des renseignements personnels. Dans certains cas, les instances de surveillance compétentes en matière de données personnelles ont le pouvoir d'exercer une surveillance sur les pratiques policières. N'est-ce pas via un contrôle conséquent des pouvoirs de police qu'il serait adéquat de prévenir les possibles dérives ?

## **À la recherche des repères d'identification**

Il y a une nécessité de recourir à des identifiants électroniques qui jouent fonctionnellement le rôle des repères d'identification qui se sont développés dans les relations sociales. Dans les échanges électroniques, il y a perte des repères usuels d'identification. L'identification prend de nouvelles dimensions : les usages et habitudes qui pouvaient satisfaire aux besoins d'identification dans le monde physique ne sont plus nécessairement suffisants.

Le réseau s'interpose en rendant plus difficile la reconnaissance des personnes et en posant d'autres modalités de la confiance. L'environnement réseau peut permettre l'identification ou la création d'identité souvent à l'insu des personnes. Mais également, le réseau rend parfois plus difficile la reconnaissance des personnes et appelle la mise en place d'autres modalités de la confiance.

Des risques accrus, mascarade, répudiation des transactions et atteintes à la vie privée, doivent être assumés dans les transactions électroniques et les mécanismes d'identification participent aux démarches de réduction des risques de transiger dans le cyberspace.

Les identifiants destinés à être utilisés dans le cyberspace répondent à un besoin de sécurisation et visent à reconstituer un environnement sécuritaire, compte tenu des différents niveaux de risques impliqués dans les transactions. Il importe donc de faire en sorte que les mécanismes d'identification dans les environnements

électroniques puissent assurer à l'individu le contrôle des informations utilisées à son sujet.

Les mécanismes d'identification sont donc à ce titre une composante majeure d'une approche cohérente de développement des interactions dans le monde virtuel, en ce qu'ils sont un ingrédient de la confiance nécessaire pour les transactions et pour la prestation de services.

De tels mécanismes sont tributaires de "l'effet-réseau" : leur valeur s'accroît en fonction du nombre de personnes qui en font usage. Comme l'État est un joueur important dans l'émission et la gestion des identifiants, il est en mesure de mettre en place des approches d'identification qui jouiront d'une valeur importante auprès des usagers.

Par exemple, la quasi-totalité des citoyens du Québec disposent d'identifiants fournis par l'État et ce même si la carte d'identité n'existe pas. Si l'État adapte de tels outils d'identification afin qu'ils puissent répondre aux besoins des échanges dans le cyberspace, il est en mesure de le faire avec un haut degré d'efficacité et on peut espérer que les mécanismes recevront un haut degré d'adhésion.

### **Quelques principes incontournables**

Pour assurer le respect effectif des droits des personnes, les processus d'identification doivent être conformes aux principes qui suivent.

- Les informations relatives à l'identification des personnes doivent être adéquatement protégées.

Les dangers que les environnements électroniques posent pour la protection des droits des personnes ont été souvent signalés. Il suffit de rappeler que les possibilités offertes par l'informatisation, la numérisation et le raccordement en réseaux de dimensions planétaires présentent de réels potentiels de poser des préjudices graves aux personnes.

S'agissant des informations relatives à l'identification, le défi est de préserver ce nécessaire équilibre entre le caractère public de plusieurs informations relatives à l'identité avec l'impératif de protections conséquentes pour des informations qui sont une composante de la vie privée.

- Seules les informations nécessaires aux besoins légitimes d'identification peuvent être utilisées à pareilles fins

Dans le monde non-virtuel, on n'est pas toujours placé dans la situation de devoir livrer toutes une batterie d'informations sur soi-même pour réaliser la moindre transaction. De la même façon, on ne collecte pas d'information à l'insu des personnes (sauf pour les fins de lutte contre la criminalité, etc.). La plupart des transactions de dimensions modestes ou payables au comptant peuvent se faire dans un relatif anonymat.

Une politique sur l'identification doit assurer, dans les environnements électroniques, une diversité d'options comparable à celles qui existent dans le monde non-virtuel. Il n'y a pas de raison d'exiger un quantum d'informations plus considérable pour des transactions d'importance et d'enjeux similaires pour le seul motif que l'une est réalisée sur Internet et l'autre dans un lieu physique.

Il s'agit donc d'appliquer le principe selon lequel seules les informations légitimement nécessaires au déroulement de la transaction doivent être exigées et utilisées. Un tel principe se concilie mal avec une approche qui prétendrait imposer

un niveau identique d'exigences relatives à l'identification pour toutes les transactions, même les plus petites. Il appelle plutôt la mise en place d'approches offrant un large spectre d'options aux personnes en matière d'identification. Il s'oppose évidemment à ce que des informations identifiant une personne soient collectées à l'insu de l'intéressé.

- Les informations relatives à l'identification doivent être de qualité acceptable pour répondre aux différents besoins d'identification

La situation des personnes connaît de fréquents changements : l'information exacte un jour peut se trouver erronée à un autre moment. Il est donc nécessaire de favoriser le maintien de la qualité des informations susceptibles de répondre à des besoins d'identification.

Plusieurs des difficultés à l'égard des informations personnelles relèvent d'un traitement inadéquat d'informations qui ont déjà été exactes ou d'une utilisation maladroite d'informations. Par exemple, il n'y a pas de lien rationnel entre le fait qu'une personne ait été un jour accusée d'une infraction puis acquittée et sa capacité d'occuper la plupart des emplois ou de rembourser ses dettes.

Le fait de tolérer que des personnes ou entreprises se mettent à établir des liens aussi saugrenus est une atteinte à la dignité des personnes. Ce problème concerne la qualité des informations utilisées afin de prendre une décision à l'égard d'une personne. Une politique qui consisterait à bloquer la circulation d'informations au motif que celles-ci peuvent être mal utilisées passe à côté des objectifs d'une politique d'identification respectueuse des droits et libertés des citoyens. Des mesures doivent assurer que l'information n'est pas utilisée à des fins maladroites ou contraires aux finalités légitimes. Il importe donc qu'une politique sur l'identification électronique détermine des standards de qualité afin que l'information relative à l'identification soit maintenue exacte et utilisée de manière adéquate.

**Pierre TRUDEL**

\* \* \*

## **XIX. Contribution de Claudine DARDY, Professeur de sociologie à l'Université Paris XII – 12 mai 2005**

Par **Claudine DARDY**

Professeur de sociologie à l'Université Paris XII.

Auteur de Objets écrits et graphiques à identifier (2004 coll. Logiques sociales l'Harmattan) et Identités de papiers (ed. Lieu commun, 1990).

Il convient tout d'abord de s'intéresser à **la notion d'identité** celle des papiers et de la carte bien sûr. Retourner l'expression « papiers d'identités » en Identités de papiers<sup>70</sup>, cette simple inversion d'une expression ordinaire permettait d'ouvrir des interrogations sur les identités en jeu.

Il apparaissait alors que cette identité n'était pas qu'un mot, mais avait un sens et un contenu socio-politique dont j'esquissais une possible exploration.

L'identité des papiers et en premier lieu celle de la carte d'identité était, en somme, à prendre au sérieux, de quelles sortes d'identités s'agissait-il donc ?

On apercevait ainsi que les papiers étaient preuves et traces d'**inscriptions** multiples des individus dans leurs rapports aux institutions.

J'étais partie du constat que l'existence de chaque individu commençait par les inscriptions d'Etat civil puis se poursuivait par toutes sortes d'autres inscriptions le positionnant vis à vis par exemple des institutions scolaires, médicales, militaires, ou même des banques institutions de l'argent dont on ne saurait aujourd'hui se passer..

En d'autres termes, au delà de l'inscription initiale à l'Etat civil, la notion d'inscription pouvait être étendue, à toutes ces procédures obligatoires, dont on peut faire l'inventaire chronologique dans le cours de l'existence d'un individu.

L'**inscription** est donc à prendre dans son sens littéral et pas du tout comme une métaphore -on a coutume en effet de parler d'inscription sociale ou spatiale par exemple, ce qui est une acception purement métaphorique- en fait l'inscription est à envisager comme un concept rendant compte d'une écriture-action éminemment politique.

Chaque individu appartenant à une société étatique moderne qui est aussi une société de culture écrite, doit avant même d'être né, être inscrit puis constamment s'inscrire tout au long de son existence et garder trace de ces inscriptions. Ces inscriptions sont obligatoires, elles sont la condition d'une **socialisation** dans ce type de société. Il faut s'inscrire et garder traces. Ne pas inscrire un nouveau-né, c'est à dire ne pas le déclarer à l'Etat civil, lui rendra la vie difficile, c'est le vouer à une mort sociale certaine

Les procédures d'inscriptions sont non seulement obligatoires mais l'une conditionne souvent l'autre. L'obligation est aussi celle de garder le papier qui dit, qui prouve que vous êtes inscrit, que vous avez votre place dans cette société.

Les inscriptions et les papiers corollaires de ces inscriptions attribuent, de fait, des places écrites aux individus tout en les pourvoyant en identités.

La fabrication d'**identités de papiers** participe d'un mode puissant d'intervention sociale et politique caractéristique d'une société de **culture écrite** dans laquelle est à l'œuvre aussi un **processus d'individuation**. Celui-ci engage chaque citoyen, pour son compte personnel, dans une gestion administrative par laquelle se constitue aussi un habitus propre aux sociétés étatiques.

Les citoyens ont parfaitement conscience de l'importance symbolique de la carte d'identité, il me semble qu'on peut ainsi interpréter le fait que lorsque l'accès à la

---

<sup>70</sup> C.Dardy Identités de papiers ed Lieu commun 1990 rééd 1998 coll Logiques sociales Ed l'Harmattan.

nouvelle carte dite infalsifiable s'est fait gratuit, les demandes ont été massives, comme si chacun, en dehors de toute obligation, voulait s'assurer de sa place, claire perception donc de la valeur de cette carte.

La nouvelle carte d'identité électronique sera obligatoire, c'est dire aussi que l'Etat assume les caractéristiques d'une société de culture écrite, les individus n'y ont place que par l'inscription et l'écrit.

Les papiers d'identités, loin d'enregistrer des identités préexistantes ainsi qu'on pourrait le croire en première approche, les construisent comme telles et même engendrent un modèle identitaire élisant et privilégiant certaines marques et leur ordre (nom, prénom, âge, sexe etc.)

Le papier, le signe a même tendance à s'émanciper et à fonctionner tout seul, indépendamment de l'individu qu'il concerne au point que c'est ce dernier qui parfois se conforme à ses injonctions.

Au fil de l'histoire de la carte nationale d'identité, comme Pierre Piazza le rappelle l'existence de toutes sortes de carnets, livrets précédant ou accompagnant les cartes : passeports, livret de l'ouvrier, livret militaire, carnet anthropométrique, carnet individuel signalétique, livret de famille...

En réalité, on a donc affaire, à un ensemble administratif plus complexe composé d'objets variés et souvent complémentaires entre eux.

Il s'agit d'**objets** à prendre au sens propre du terme

C'est là ma deuxième ligne de réflexion à propos de papier d'identités, ils sont à considérer comme des **objets écrits**, là encore dans ce terme pas de métaphore ou de sens figuré, il faut les aborder comme des objets.

L'intervention sociale et politique passe d'ailleurs par le recours à des objets écrits

C'est tout à fait sciemment et avec des objectifs réfléchis que cette intervention sociale et politique (avec parfois des intentions pédagogiques)<sup>71</sup> opte par exemple, pour la feuille volante d'un certificat ou d'une fiche ou bien plutôt pour un carnet ou une carte.

Le terme d'objets pour qualifier ces documents permet de souligner l'intérêt à les considérer dans leur matérialité et leurs formes puis à se pencher sur **les** pratiques et usages qu'ils engendrent.

En ce sens, ce qu'on appelle communément les « **papiers** » représentent des **prototypes d'objets écrits**, purs produits d'une société de **culture écrite** : ils sont d'abord à manipuler, à porter sur soi, à produire en certaines circonstances bien plus qu'à lire.

Le **rapport au corps** caractérise le papier d'identité puisque celui-ci est à porter sur soi. Les papiers d'identité ont vocation à être portés sur soi, à même le corps, il faut être en capacité de les produire en toutes sortes de circonstances (c'est vrai de la carte d'identité nationale, du passeport, ou des cartes d'identités professionnelles, mais aussi de toutes sortes de cartes qui valent accès ou privilèges, cartes d'accès à tel ou tel espace, cartes bancaires ouvrant tous les circuits marchands.

Quelques jours prochains l'administration électronique pourra bien avoir éliminé la plupart des supports papiers, reste pour l'instant la nécessité de ces objets écrits, réduits à des cartes même très miniaturisées.

D'une manière générale l'informatique à des incidences sur la matérialité des objets écrits, puisqu'elle a tendance à généraliser ces cartes, porteuses de puces, cartes qui se substituent à des documents papiers du type livret ou carnet et ne

---

<sup>71</sup> Un carnet de santé par exemple, a un contenu et une structure qui doit permettre aux parents de suivre l'évolution de leur enfant et sa prise en charge par les institutions appropriées, en même temps il doit servir la mise en œuvre d'une politique de santé et d'une politique sociale préventive.

produisent pas non plus les mêmes effets pour leurs détenteurs : on peut lire un carnet, contribuer à le remplir, accéder aux informations qu'il contient et qui vous concerne au premier chef, on ne peut le faire pour des cartes, même si les informations contenues sont identiques, le recours à des machines et à des experts spécialistes dans leur lecture et décodage est alors nécessaire<sup>72</sup>.

Bien sûr, il ne s'agit nullement d'inscriptions à même le corps. Les papiers d'identités permettent justement de ne pas recourir à des inscriptions à même le corps, les objets sont traces des inscriptions, mais représentent un support distinct du corps. Je dis cela parce que dans les sociétés traditionnelles étudiées par l'anthropologie, un certain nombre de marques identitaires peuvent être inscrites sur le corps même des individus, tatouages, scarifications, parures et modifications corporelles. Dans les sociétés de cultures écrites ces marquages corporels sont inutiles parce qu'on dispose de ces moyens d'identification que sont justement les objets écrits et graphiques.

Lorsque dans une société moderne de culture écrite on revient à des marquages identitaires à même le corps, c'est en général en situation de crise, de catastrophes, de guerre, et ces marquages sauf s'ils sont gestionnaires (dans des contextes de crise, on peut être amené, à porter sur le corps des individus, un numéro d'identification, parce que de fait le recours aux papiers est transitoirement impossibles, papiers perdus, archives brûlées) mais souvent, l'inscription à même le corps est plutôt un signe régressif, un stigmate volontaire imposé à des individus dans des situations de domination, des numéros et autres marques d'identification portés sur les individus dans les camps de déportations, pour les trier et les distinguer, en général pas pour leur bien imagine-t-on.

On peut donc dire que les objets écrits, d'une certaine manière constituent une médiation utile puisqu'elle évite les inscriptions à même le corps négatives et stigmatisantes.

Il est techniquement envisageable de greffer à même le corps des individus une puce contenant des éléments identificateurs de la personne en question mais ce n'est pas souhaitable à juste titre et pour les raisons qu'on vient d'indiquer, il y a méfiance à l'égard de dispositions qui restaureraient une forme d'inscription à même le corps

Pour autant, certains peuvent d'ores et déjà recourir aux puces informatiques greffées à même le corps pour leur sécurité personnelle.

C'est une pratique en vigueur, paraît-il, dans la riche bourgeoisie mexicaine pour faciliter les recherches lors d'enlèvements des personnes pour rançons. Par la même occasion, des informations à caractère médical peuvent être intégrées à ces puces<sup>73</sup>.

Les techniques biométriques d'identification permettent de faire l'inverse, d'introduire des éléments du corps dans le papier, dans la carte. La biométrie puise dans le corps des éléments d'identification et peut les traduire graphiquement sous forme de code (iris de l'œil, ADN), dans tous les cas c'est un corps objet, qui se trouve mis en jeu, pas ce corps sujet de la personne qui ne se manifeste volontairement par la main par exemple et qui signe, présence manuscrite qui indique la volonté de la personne. La biométrie saisit le corps dans ses modes d'identification, elle peut se passer de l'adhésion du sujet pour ce faire.

Les dispositions associées à la nouvelle carte d'identité prévoit notamment pour protéger la personne, la dissociation entre fichier des données biométriques, (banque de données ou seraient stockés empreintes digitales et image du visage numérisée) et fichiers des données d'Etat civil. Disposition technique fonctionnelle

---

<sup>72</sup> Dans un chapitre d'ouvrage collectif publié en 1993 *Illettrismes et cultures* (coll Sémantiques ed l'Harmattan 2000), et intitulé des « carnets aux cartes », j'avais proposé une réflexion à partir du constat de multiplication des cartes à puces informatiques, nouveaux type d'objets écrits se substituant aux carnets et aux livrets, et je proposais un premier bilan des effets induits par cette transformation, et du type de rapports que cela engageait.

<sup>73</sup> Article 1<sup>er</sup> trimestre 2004 supplément monde.

et protectrice certes, il n'empêche, dans le papier lui-même le **corps est objet débité et mis en puces.**

La carte d'identité électronique reste un papier à porter sur soi, mais qu'il ne sera pas forcément nécessaire de produire, de montrer, le fait de l'avoir sur soi peut suffire techniquement, cela permet à chaque citoyen d'être lu, identifié à son insu.

Ce port passif de l'objet carte, rendu possible par l'électronique ne constitue pas une différence anodine, et les associations de protection des libertés auraient raison de s'en soucier car cela touche au rapport que chacun d'entre nous citoyen de culture écrite nous avons établi à ces objets.

J'évoque le rapport au corps comme caractéristique du papier d'identité, j'ai tendance à dire, que le corps associé à ces papiers, est de plus en plus objet, on se passe de plus en plus d'un corps sujet, manifestation d'une volonté de la personne, comme par le truchement de la main qui signe, la signature a été longtemps l'ultime signe de la volonté de la personne, mais elle est en voie de disparition, la signature électronique représente un tout autre acte ;

L'anthropologue J.Goody disait avec les sociétés d'écriture on était passé de la bouche à la main, avec l'écriture électronique on franchit sans doute une autre étape, celui de la saisie d'un corps objets, par opposition à un corps sujet pensant et volontaire.

En apparence, le changement associé à la carte d'identité électronique n'est pas bien grand d'autant qu'on s'emploie à garantir l'accès conditionnel à des fichiers distincts, dont la mise en connexion serait réservée à des situations rares et protégées, mais même apaisées, les craintes à la big brother, l'objet même sécurisé, garanti par l'Etat et ses administrations dans ses usages, et servi en cela par les technologies nouvelles dans sa conception même engage d'autres changements.

Le rapport l'objet carte se trouve en effet, subtilement infléchi. Les puces informatiques n'offrent pas une lisibilité immédiate, avons-nous déjà remarqué, il faut des médiations pour accéder aux informations qui vous concernent. Bien sûr, il est prévu de remettre aux intéressés une liste papier de ces informations insérées dans la puce, on pourra aussi recourir dans un avenir très prochain à des decodeurs de cartes à puces, peu coûteux. Mais, de fait ce nouvel objet carte électronique, à détenir obligatoirement, peut se passer de notre implication, de notre volonté de personnes. Elles sont aussi conçues pour accroître la traçabilité des personnes.

Une traçabilité des personnes qui serait du même ordre que celles des produits marchands, c'est nier le fait que les objets écrits tout en étant objets sont aussi très singuliers puisque ils touchent à de l'identité, et contribuent d'ailleurs à la fabriquer, peut être d'ailleurs sont ils susceptibles d'induire certaines modalités de la conscience de soi, Ainsi cette traçabilité sous prétexte de sécurité s'impose comme une norme et même une valeur assez cohérente avec des engouements, des passions qui trouvent ailleurs leurs justifications, comme le goût des recherches généalogiques, la valeur ajoutée par la transparence des origines (ainsi l'état doit garantir l'accès aux recherches ultérieures de filiations, même en cas d'accouchement dit sous X)

La traçabilité des personnes que sert l'électronique peut bien correspondre à une volonté de protéger l'identité, la sécurité des personnes. Il n'empêche, par la même, elle est confortée comme une valeur en soi, installant en incontournable vérité l'adage selon lequel « c'est quand on sait d'où l'on vient qu'on sait où l'on va » ce qui pourtant est éminemment discutable. Le concept d'identité sous peine d'être totalitaire s'il doit encore être utilisé, ne me paraît n'avoir de sens dans les sociétés modernes qu'au pluriel, permettant encore de la flexibilité, des écarts, de la circulation, jeux encore possibles avec les imperfections des objets papiers traditionnels mais je ne saurais pousser trop loin quelque éloge passéiste des papiers à l'ancienne.

## La matérialité des objets écrits et leurs usages

Pour me faire mieux comprendre à propos de cette notion d'objets écrits, de l'importance à accorder à leur matérialité, je peux donner d'autres exemples de formes, celles dérivées de la forme carnet notamment<sup>74</sup>.

Ainsi le carnet à souches, et feuillets détachables, La forme carnets à souches, avec feuillets détachables peut être utilisée lors des grossesses, on délivre ce genre de carnets aux jeunes femmes ayant déclaré leurs grossesses, il comprend des feuillets détachables, à réexpédier auprès des services sociaux, après chaque visite médicale de suivi de la grossesse. La jeune mère est incitée au bon usage d'un tel carnet, par le fait qu'il conditionne l'octroi d'avantages divers, allocations prénatales, remboursements de consultations, obtention de congés.

L'intervention sociale et médicale, à des fins de prévention passe donc par la mise en circulation et l'invite à usage d'un tel carnet à souches.

Ce savoir « manipuler » n'est encore pas inné, et les débutants doivent s'y initier rapidement. Les cartes à puce du type cartes vitales sont venues révolutionner une bimbeloterie besogneuse, faite de feuilles de soins, de vignettes et d'ordonnances, en permettant des prises en charge quasiment invisibles tout en posant d'autres problèmes associés à l'identification de leur détenteur (s'agit-il des justes ayants droits ?) et à la crainte que les usagers perdent justement la conscience d'une aide, d'un apport en contrepartie de leurs cotisations ce que certaines mutuelles corrigent en ne manquant pas d'expédier aux usagers bénéficiaires l'exact relevé des prestations qui leur ont été versées ou de signaler ce qui a été versé à un tiers, un pharmacien par exemple. Une pratique de courrier qui suppose encore de la part des usagers un savoir lire bien particulier<sup>75</sup>.

Les objets écrits de ce type, engage donc, à la fois, un « savoir manipuler » et un « savoir lire » acquis par osmose mais sans doute inégalement par des individus qui baignent à leur insu même dans une culture écrite.

On vient d'évoquer des objets écrits plutôt archaïques puisqu'ils se présentent sous forme de vignettes à coller, d'autres peuvent être conçus comme un ensemble de timbres, à coller ou à envoyer, ils peuvent représenter des montants de cotisations, à une caisse d'aide ou de retraite ; là encore le système de timbres à manipuler à des moments précis est à la fois, un mode de gestion et de perception des cotisations, et une invite pour les usagers à se représenter comme cotisants, participants actifs d'un système de redistribution.

On a là des objets écrits dont l'usage n'est pas anodin, puisqu'ils sont en mesure d'agir sur des représentations mentales et des sentiments d'appartenance à des communautés particulières (de mutualistes, de travailleurs syndiqués ou de chômeurs reconnus)

A travers ces quelques exemples, je pense avoir clarifié l'idée d'objets écrits, dont la matérialité, la forme même peuvent être réfléchies et utilisées pour guider certaines actions sociales ou politiques.

L'idée est que les sociétés de cultures écrites ont elles aussi leurs objets écrits et graphiques qui méritent attention non, tant par l'écrit qu'il contiennent (les textes souvent assez pauvres) que par leurs formes, leur matérialité qui engagent des usages spécifiques susceptibles d'engendrer des représentations mentales particulières.

---

<sup>74</sup> Thème développé dans C.Dardy Objets écrits et graphiques à identifier coll Logiques sociales. Ed l'Harmattan. 2004

<sup>75</sup> Une démonstration analogue dénombrant toutes sortes d'objets aux formes variées peut être faite à propos de l'argent, de moins en moins espèces sonnantes et trébuchantes, de plus en plus jeux d'écriture à travers les inscriptions bancaires : on y trouve encore des livrets (d'épargne), des carnets à souches (chèque), puis des cartes à puces modifiant nettement le rapport à l'argent, comme le rapport à soi peut se trouver modifié à travers la carte d'identité électronique.

A notre insu peut être, le fait que nous baignons dans une culture écrite suscite des schèmes mentaux et des habitus spécifiques.

Les **cartes**, au premier rang desquelles la carte d'identité, sont donc loin d'être les seuls objets écrits de notre société de culture écrite, il faut pour comprendre leur fonctionnement et leur rôle, y associer d'autres objets que sont les carnets, les livrets (livret de famille) et dont la forme spécifique n'est pas indifférente mais qui sont probablement en voie de disparition

Il est temps de porter sur eux un regard d'ethnologue à l'ancienne, s'empressant de recueillir ce qui peut être voué à l'extinction, un regard analogue à celui des ethnologues de sociétés traditionnelles pour les objets de ces sociétés de l'oralité, les objets écrits et graphiques et les papiers sont les plus exemplaires de nos sociétés de culture écrite.

Ces objets écrits et graphiques propres à une société de culture écrite ne sont jamais réductibles à leur fonctionnalité, ils sont aussi **supports symboliques et imaginaires**.

L'objet écrit et/ou graphique est souvent produit pour conjurer une menace de disparition identitaire : on s'évertue à produire le signe quand ce qu'il veut désigner est vacillant : la carte nationale d'identité par exemple quand l'état nation français est déliquéscent sous le régime de Vichy (Piazza) ou bien à une autre échelle : lorsque le service militaire se trouve remplacé par une seule journée dite de formation à la vie citoyenne, celle-ci est précédée, prolongée, soutenue par divers papiers valorisés en véritables **diplômes**, certificat de recensement, puis certificat de participation qu'il faut sinon encadrer, du moins garder parce que leur production va conditionner d'autres inscriptions, aux examens, au permis de conduire etc....

Autre exemple d'usage symbolique puisé dans le domaine de la politique sociale et familiale

Dans le but de promouvoir, reconnaître la paternité à l'égal de la maternité, on a eu recours récemment à l'édition d'un carnet de paternité, conçu sur le modèle du carnet de maternité et destiné au nouveau père. Cette invention d'un carnet de paternité vient compléter et conforter d'autres modes d'institutionnalisation et de reconnaissance de la paternité, comme par exemple, l'instauration d'un congé de paternité.

S'il peut être productif d'envisager les écrits, comme des objets semblables à d'autres produits culturels pour les raisons que nous avons soulignées, ils sont aussi à saisir dans **leur singularité** précisément parce qu'ils mettent en jeu des **identités sociales**, ils ne sont pas non plus des objets tout à fait comme les autres.

On peut citer à l'appui de cette remarque, le problème des identités professionnelles, telles qu'on peut l'aborder par exemple dans la production des diverses **cartes professionnelles** : Une carte professionnelle en tant qu'objet écrit de travail permet de justifier d'une identité qui garantit l'accès si ce n'est à des privilèges du moins à des droits, un badge, autre objet graphique pouvant avoir le même propriétaire permet éventuellement la mise en œuvre de la réduction du temps de travail, mais n'offre à son détenteur ni les mêmes droits ni les mêmes atouts symboliques que la carte professionnelle support et matérialisation d'une identité professionnelle. On a dans le domaine du travail, un exemple des effets subreptices induits par un changement technique, en apparence fonctionnel, le passage au badge, supposé pouvoir remplir plusieurs fonctions, dont celle de permettre l'exercice d'un temps de travail à la carte, mais qui en fait écrase la symbolique attachée aux cartes professionnelles, et qui peuvent se reconstituer d'ailleurs dans des objets anciens que sont les cartes de visite, professionnelles.

En résumé on aurait tort, sans doute à propos de la carte d'identité électronique de se préoccuper exclusivement de ses effets, de ses conséquences en termes fonctionnels, pratiques. Il est certes utile de s'interroger sur les menaces ou les protections qu'elle présente, mais, sur ce plan d'ailleurs, la technologie électronique d'aujourd'hui offre bien des ressources en ce sens les internautes enthousiastes ont raison, voilà un objet qui promet d'être pratique, mais il faut aussi considérer le fait que tout en restant un objet écrit à porter sur soi, l'électronique introduit de petites différences dans le rapport que nous avons à cet objet.

Cet objet fait aussi et surtout partie d'un ordre symbolique et imaginaire. Les histoires de papiers nombreuses que j'avais eu l'occasion de recueillir, et qui ne sont pas seulement le fait de migrants, racontent ces rapports complexes et riches de sens des individus, à ces objets là, si particuliers. Ils matérialisent un mode de socialisation en culture écrite et recouvrent toujours cette tension féconde entre contrainte sociale, ordre social, et place attribuée dans une société de culture écrite.

**Claudine DARDY**

\* \* \*

## **XX. Contribution de Philippe RIGAUT, sociologue, enseignant à l'université de Picardie - Jules Verne - 12 mai 2005**

Par **Philippe RIGAUT**

Sociologue, enseignant à l'université de Picardie - Jules Verne.

Auteur de *Au-delà du virtuel - Exploration sociologique de la cyberculture* (L'Harmattan, 2001).

### **CORPS, IDENTITE, LIBERTE : DES RESISTANCES SYMBOLIQUES A LA GESTION TECHNO-ADMINISTRATIVE DE L'HOMME**

Des clichés anthropométriques d'Alphonse Bertillon à la carte d'identité électronique, la mise en fiche de l'individu, dans nos sociétés démocratiques, semble évoluer vers des scénarios de plus en plus propices à la paranoïa, avec pour thème dominant la "traçabilité" de l'humain dans une forme de contrôle plus subtile encore que celle exercée par le Big Brother de 1984.

L'omniprésence de la bureautique, tant dans le domaine professionnel que dans nos vies d'administrés ou de consommateurs, nous familiarise avec une logique opérationnelle faite de codes alpha-numériques. Nous sommes requis de nous "identifier" plusieurs fois par jour en usant de procédures fondamentalement dépersonnalisantes. Il n'est pas jusqu'au distributeur automatique de boissons chaudes qui n'exige à présent son sésame chiffré.

Notre quotidien est marqué du sceau de la puce électronique. Au-delà des gains de temps, de sécurité, de préservation mémorielle qu'elles nous assurent, les cartes bancaires, cartes Vitale, etc, nous confrontent à une expérience impensable il y a quelques décennies encore ; celle de la numérisation de pans entiers de nos vies.

Ces technologies, pour être matériellement parfaitement ancrées dans nos habitudes, n'en sont pas moins sujettes à caution chez chacun d'entre nous ; objets d'inquiétudes qu'il serait trop aisé de qualifier de simples fantasmes et de rejeter dans la sphère de l'irrationnel. Comme le dit Anthony Giddens, nous avons passé un "pacte" avec la modernité technologique : nous nous en remettons à elle de manière quasi-infantile, en échange d'un bénéfice de sécurité (Consequences of Modernity, 1990). Néanmoins, ce pacte implicite (que contribue à entretenir tout un ensemble de discours laudateurs sur les bienfaits de la science et de la technologie) n'implique pas que nous parvenions à refouler totalement nos peurs et nos doutes.

La crainte d'une dérive politique tyrannique de la techno-science, associée à l'idée que les "ratés" de celle-ci seraient d'ores et déjà tenus secrets par nos dirigeants habite nos imaginaires. Des écrivains comme Georges Orwell ou Aldous Huxley, des fictions cinématographiques comme Bienvenue à Gattaca ou Minority Report, expriment cette crainte d'une façon que le public ne manque pas de percevoir comme prophétique. Les orientations les plus récentes de la techno-science sont envisagées ici dans la perspective la plus effroyable possible : celle d'une bureaucratie à la fois invisible et omniprésente capable de pister chacun de nos déplacements et de compiler en temps réel des informations complètes sur chaque individu : état civil, dossier médical, dossier fiscal, casier judiciaire, etc... Dans les scénarios d'anticipation les plus extrêmes, des thématiques sensiblement différentes sur le plan formel mais d'un certain point de vue assez voisines sont explorées : celle de la modification du psychisme par le biais de substances chimiques et celle de la modification de l'évolution biologique par des manipulations génétiques.

La question du corps et de l'identité est au coeur des angoisses que la Science-Fiction contemporaine révèle en leur donnant un contenu narratif plus élaboré. La réalité anatomo-organique est soumise aujourd'hui à des représentations contradictoires : elle est donnée à penser tantôt comme un capital à entretenir scrupuleusement, car intrinséquement fragile et irremplaçable, tantôt comme un archaïsme à dépasser, ce que David Le Breton nomme le "corps surnuméraire" (L'adieu au corps, 2000). Les adeptes du body art expriment sur le mode acté cette dualité du corps à la fois fétichisé et perçu comme obsolète. Intrinséquement démiurgique, leur démarche se donne aussi à comprendre comme rébellion et comme quête mystique<sup>76</sup>.

Comme les auteurs cyber-punk (Bruce Sterling, Norman Spinrad, ...) le soulignent dans le registre nihiliste qui est le leur, notre paysage technologique quotidien est désormais complètement investi par l'informatique<sup>77</sup>. Or, celle-ci a des impacts cognitifs profonds, sur le plan notamment de nos conceptions du temps et des volumes physiques. Elle redimensionne à l'échelle micro les anciennes unités empiriques qui nous permettaient d'appréhender notre environnement et nous contraint à intégrer dans nos pratiques et nos représentations l'impensable de la dématérialisation et de l'immédiateté. Le miracle de la numérisation fait voler en éclat la distinction ontologique entre image et son.

L'informatique impose également la généralisation à des activités non-professionnelles d'une logique intellectuelle désincarnée. L'efficacité du logiciel renvoie dans la sphère du primitif les aléas de l'affect spontané. Elle s'impose jusque dans le vécu psycho-relationnel, dans notre rapport à la culture, au divertissement, avec pour ligne d'horizon la possibilité de faire commerce de ce qui constitue au plus profond nos existences (Jeremy Rifkin, L'âge de l'accès, 2000). Avec les technologies d'imagerie virtuelle, c'est la notion même de réalité qui est ébranlée par l'informatique moderne, accentuant la crainte de la manipulation de l'information. Quant à la floraison des équipements connectiques, elle génère, au-delà des multiples services rendus à l'utilisateur, une suspicion relative au respect de la confidentialité des données.

Une situation de flottement anthropologique caractérise le rapport que nous entretenons à présent à notre propre corporéité, telle que la constituent notre enveloppe charnelle, notre silhouette et nos fonctionnalités organiques. En l'absence de repères sociaux et symboliques structurants, la catégorie du corporel, et avec elle le sentiment de l'identité personnelle, deviennent disponibles pour des formes de modélisation inédites : modifications corporelles, pratiques de l'extrême, recours aux psychotropes, etc... Dans ce contexte, les fantasmes "cyber-punk" du contrôle de l'humain par des officines étatiques ou par des consortiums commerciaux plus ou moins occultes peuvent aisément investir les consciences, sur un mode plus ou moins latent.

---

<sup>76</sup> On désigne sous le terme body art diverses pratiques de modification corporelle plus ou moins extrêmes : piercing, tatouage, mais aussi implants sous-cutanés, suspensions ou mutilations. Deux grandes tendances organisent cet univers : celle des Modern Primitifs (représentée par Fakir Musaphar) et, sur un versant plus High Tech, les Extropiens, les post-évolutionnistes (Stelarc, Lucas Zpira, ...). La première cherche à renouer avec une nature spirituelle perdue, à travers des rituels "ethniques". La seconde s'enthousiasme pour le "perfectionnement technologique" de l'Homme (Cf. Stéphanie Heuze, *Changer le corps*, éd. La Musardine, 2000).

<sup>77</sup> L'univers romanescque (mais aussi cinématographique, avec par exemple Johnny Mnemonic) cyber-punk fait fusionner plusieurs thèmes chers à la Science-Fiction, en relation à des éléments bien réels de notre présent. Parmi ces thèmes, celui du cyborg, être mi-humain, mi-machine, occupe une place essentielle. Nombre de scénarios cyber-punk s'élaborent à partir de l'idée de numérisation de l'esprit, ou d'interfaces électroniques entre le corps et le réseau électronique. Les créateurs cyber-punk proposent une vision extrêmement noire de ce qui constituera selon eux notre futur : confusion généralisée entre réel et le virtuel, piratage informatique, marchandisation du vivant.

La perspective des techniques d'identification biométrique exacerbe des craintes sous-jacentes relatives tout à la fois aux fondements de l'intégrité physique de l'individu et à sa liberté face à une technostructure dont les pouvoirs de contrôle semblent désormais infinis. La société "panoptique" magistralement analysée par Michel Foucault est désormais en mesure de s'affranchir d'une limite ultime en encapsulant la singularité biologique.

L'argument de la lutte contre le terrorisme et la criminalité risque fort de n'être pas suffisant pour que cette nouvelle étape dans le fichage des individus soit acceptée sans résistances ; trop d'incertitudes pèsent sur nos consciences. Incertitudes quant au sens que revêtent les notions mêmes de corporéité, de réalité physique ; incertitudes également quant aux finalités véritables de ce type de dispositif techno-administratif. Un véritable débat démocratique autour des enjeux et des conditions d'exercice s'impose pour que l'individu-citoyen puisse consentir à l'enregistrement numérique de ce qui le constitue dans son essence. La tâche est d'autant plus ardue que ce consentement n'est pas seulement de nature politique, mais qu'il touche aussi à une dimension psycho-symbolique sans doute beaucoup plus complexe.

En préalable, et au niveau qui est spécifiquement le sien, l'Etat se doit de prendre la mesure de l'image d'opacité que lui attribuent, de manière instinctive peut-être, nombre de citoyens, et de comprendre par conséquent qu'exiger de ces derniers d'être transparents devrait l'engager au même effort. C'est alors, au-delà même de la question du contrôle démocratique exercé sur la science et ses applications, celle du débat autour des modes de gestion des populations et des individus qui est posée. Or ces questions semblent bien avoir déserté le discours des dirigeants politiques qui semblent privilégier une politique sécuritaire, réveillant ainsi des suspicions légitimement formulées et que les débats (internet et régions) permettent utilement de mettre en valeur...

**Philippe RIGAUT**

\* \* \*

**XXI. Contribution de Eric CAPRIOLI, Avocat et membre de la délégation française auprès des Nations-Unies sur les questions de commerce électronique – 1<sup>er</sup> juin 2005**

Par **Eric CAPRIOLI**

Docteur en droit

Avocat à la Cour d'Appel de Paris

Membre de la délégation française auprès des Nations-Unies sur les questions de commerce électronique

**CONTRIBUTIONS JURIDIQUES A L'ETUDE DE LA CARTE NATIONALE D'IDENTITE ELECTRONIQUE**

Les activités de l'homme le conduisent à se faire reconnaître<sup>78</sup> dans la société, à s'identifier auprès des autres. On oppose identification à anonymat. Avec le temps, l'identité est devenue de plus en plus plus complexe, associant aux nom, prénom, et lieu géographique des identifiants physiques (taille, couleurs des yeux, empreinte digitale) et sociaux (nationalité, profession, filiation, ...). Cependant, les moyens d'identification des individus utilisés varient selon le contexte.. Sur les réseaux numériques, les besoins de sécurité ont conduit les Etats à l'adoption de textes adaptés à la prévention des actes illicites (terrorisme, blanchiment, pédophilie, ...).

**Identifier consiste à exprimer l'identité d'une personne.** Celle-ci recouvre «*l'ensemble des composantes grâce auxquelles il est établi qu'une personne est bien celle qui se dit ou que l'on présume telle (nom, prénoms, nationalités, filiation...)*»<sup>79</sup> ainsi que tous «*les traits juridiquement pertinents qui se retrouvent aussi bien dans le numéro national d'identification attribué par l'INSEE que sur la carte nationale d'identité délivrée par le ministre de l'intérieur ou sur les actes de l'état civil.*»<sup>80</sup>.

Concernant une personne physique, Gérard Cornu définit l'identité comme «*ce qui fait qu'une personne est elle-même et non une autre ; par extension ce qui permet de la reconnaître et de la distinguer des autres ; l'individualité de chacun, par extension, l'ensemble des caractères qui permettent de l'identifier.*»<sup>81</sup>. L'identité civile constitue «*l'ensemble des éléments qui, aux termes de la loi, concourent à l'identification d'une personne physique (dans la société, au regard de l'état civil) : nom, prénom, date de naissance, filiation etc.*»<sup>82</sup>.

---

<sup>78</sup> «*Lorsqu'un individu circule dans le monde physique, il est susceptible de faire l'objet de contrôle d'identité tant sur le territoire qu'aux frontières de l'Etat. Pour les besoins de la cause, l'intervention de l'Etat a progressivement transformé le nom en institution de police.*», E. A. Caprioli, *Anonymat et commerce électronique*, Actes des 1ères journées internationales du commerce électronique, organisé par l'EDHEC et l'Ecole du droit de l'entreprise, Litec, 2002, p. 149 et s., article publié sur le site : [www.caprioli-avocats.com](http://www.caprioli-avocats.com).

<sup>79</sup> Termes juridiques, éd. Dalloz, 1999, p.280. L'identité de la personne «*rejoint le sens banal du terme, qui fait devoir à chacun, le cas échéant, de justifier de son identité, par exemple à l'aide d'un document officiel (la «carte d'identité») qui garantit que cet individu est bien un tel ou un tel, en raison d'une certaine permanence d'être, physiquement et socialement reconnaissable*» ; Sous la direction de S. Auroux, *Les notions philosophiques*, Dictionnaire, I, V ; Identité, PUF, 1990. Tel est le sens présupposé par la notion de «contrôle d'identité», de «carte d'identité».

<sup>80</sup> A. Supiot, *L'identité professionnelle* in Les orientations sociales du droit contemporain. Ecrits en l'honneur du Professeur J. Savatier, PUF, 1992, p. 409 et s.

<sup>81</sup> G. Cornu, *Vocabulaire juridique*, Ass. H. Capitant, PUF 2000, J-F. Renucci, *L'identité du cocontractant*, RTD Com, 1993, p. 441 et s.

<sup>82</sup> G. Cornu, *préc.*

Une pièce d'identité est quant à elle « *un document écrit (généralement une carte) qui énonce et atteste l'identité civile d'une personne physique* »<sup>83</sup>.

Rappelons par ailleurs que **certains procédés d'identification électronique ne se réfèrent pas forcément à l'identité civile**. Ainsi, des traces informatiques permettent de reconnaître une personne déterminée, ou à tout le moins son ordinateur (par le biais de l'adresse IP), à l'occasion de ses navigations sur l'Internet<sup>84</sup>. Elles favorisent une forme nouvelle d'atteinte à la vie privée. Elles permettent de créer un parcours tracé sur l'Internet.

La notion de traçabilité a été reprise notamment dans le cadre d'une directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques<sup>85</sup>. L'article 5-3 de cette directive impose aux fournisseurs de services sur l'Internet d'informer les internautes de l'utilisation de procédés permettant de stocker des informations dans leur ordinateur ou d'accéder à des informations stockées dans leur ordinateur, et de leur indiquer par quels moyens ils peuvent s'opposer à l'utilisation de tels procédés<sup>86</sup>.

De telles **traces informatiques peuvent être conservées et utilisées en matière pénale<sup>87</sup> ou civile<sup>88</sup>**.

La Carte nationale d'identité est un document portatif individuel, délivré par l'Etat, permettant de vérifier l'identité de son porteur, voire de le contrôler. Les enjeux sociaux, culturels et juridiques du passage à l'électronique sont très importants. C'est dans cette optique que le programme INES (Identité Nationale Electronique Sécurisée) a été lancé par le Ministère de l'Intérieur. Ce programme consistera à<sup>89</sup> :

- fusionner les procédures de demande de carte d'identité et de passeport ;

---

<sup>83</sup> G. Cornu, *préc.*

<sup>84</sup> On voit toutefois la difficulté d'identifier une personne physique sur le réseau par les seules données collectées sur le dernier. Lorsque l'ordinateur est en libre accès et qu'une infraction est commise par une personne malveillante, la justice peut localiser l'ordinateur en cause mais cela ne sert à rien si de nombreuses personnes peuvent y accéder. Ainsi, dans une affaire où une personne avait acheté des biens en ligne avec une carte de crédit volée par le biais d'un ordinateur mis à disposition dans une bibliothèque municipale, la justice n'a eu aucune difficulté pour retrouver l'ordinateur mais retrouver l'utilisateur était une autre gageure. Aucun registre d'utilisation avec l'heure et le nom de la personne n'était tenu par le personnel communal. C'est grâce à l'adresse physique de livraison des biens achetés que le délinquant a pu être interpellé. Cette affaire est citée par E. A. Caprioli, *Anonymat et commerce électronique*, Actes des 1ères journées internationales du commerce électronique, organisé par l'EDHEC et l'Ecole du droit de l'entreprise, Litec, 2002, p. 149 et s.

<sup>85</sup> J.O.C.E. L.201 du 31 juillet 2002, p. 37 et s.

<sup>86</sup> Pour des développements concernant cette question, voir E. Drouard, *Directive «Communications électroniques» : la prospection et la traçabilité en question*, Expertises, octobre 2002, p. 338 et s.

<sup>87</sup> V. en ce sens, l'article L. 34-1 du Code des Postes et Communications Electroniques. Ainsi, les opérateurs de communication électronique pourront ou devront (suivant le cas) différer l'anonymisation de toute donnée relative au trafic pendant une durée maximale d'un an pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales ou pour les besoins de la facturation et du paiement des prestations de communications électroniques. Un décret en Conseil d'Etat, pris après avis de la CNIL, est attendu. Il doit déterminer les catégories de données et la durée de leur conservation, selon l'activité des opérateurs et la nature des communications ainsi que les modalités de compensation, le cas échéant, des surcoûts identifiables et spécifiques des prestations assurées, à ce titre, à la demande de l'Etat, par les opérateurs. V. en ce sens, E. Caprioli, *L'identification de l'internaute délinquant*, Colloque du CEJEM (Paris II), à paraître.

<sup>88</sup> V. en ce sens, E. Caprioli, *La qualité de fournisseur d'accès à l'internet : un nouveau risque juridique pour l'entreprise*, Journal des sociétés, n°21, Mai 2005, p.47 s. Disponible sur le site [www.caprioli-avocats.com](http://www.caprioli-avocats.com).

<sup>89</sup> V. Le programme INES, émis par le Ministère de l'Intérieur, de la Sécurité Intérieure et des Libertés Locales, version 2 du 1 mars 2005.

- améliorer la gestion des titres dans de nouvelles applications ;
- délivrer des titres conformes aux exigences internationales<sup>90</sup> ;
- offrir des moyens d'identification et de signature électroniques aux citoyens.

## **I – L'identité électronique**

La définition classique de la pièce d'identité semble confortée par certaines fonctionnalités de la Carte Nationale d'Identité Electronique (CNIE) qui devrait voir le jour prochainement. Bien évidemment, elle comprendra les principales données relatives à l'état civil de son titulaire (nom, prénom, sexe, date et lieu de naissance), la mention de sa nationalité, son adresse, la date de délivrance et de caducité de la carte, le numéro d'identification du document, le code de la commune qui l'a délivré, ainsi que la signature numérisée du titulaire. Mais elle contiendra également des informations imprimées sur la carte, en particulier la photo numérisée et deux empreintes digitales numérisées.

La CNIE a notamment pour objectifs de :

- mieux garantir l'identité contre les risques d'usurpation ou de détournement ;
- lutter contre le terrorisme (Règlement du 13 décembre 2004) ;
- autoriser l'authentification du porteur en vue de l'utilisation de téléservices dans les relations avec les administrations et la signature électronique pour les services commerciaux sur l'internet ;
- simplifier les demandes de documents d'identité électronique (un seul dossier pour la CNIE et le passeport) et leur renouvellement.

**En résumé, l'utilisation de la C.N.I.E. sur les réseaux reviendra à déclarer de manière active son identité et s'ajoutera aux autres moyens d'identification et de localisation existants tels que le téléphone portable ou la carte de crédit. Ce raisonnement par analogie a ses limites : les choses sont équivalentes mais ne sont pas identiques.**

**La signature manuscrite scannérisée comprise dans la CNIE n'est pas suffisante pour s'assurer de l'identité d'une personne.** La Cour d'appel de Besançon<sup>91</sup>, dans un arrêt du 20 octobre 2000<sup>92</sup>, met en avant l'incertitude quant à l'identification du signataire de l'acte lorsqu'une signature manuscrite scannérisée est utilisée : *«[...]La fiabilité du procédé utilisé en l'espèce par l'avocat est au demeurant toute relative dans la mesure où le code permettant d'accéder à la signature peut être détenu par une autre personne du cabinet. L'identification de la personne ayant recours à la signature informatique est dès lors incertaine.[...]»*. La signature scannérisée, protégée par un simple code d'accès, n'était pas suffisante pour garantir la fiabilité du procédé.

La carte d'identité traditionnelle ne signe pas à proprement parler mais elle permet de vérifier l'identité. Dans l'électronique, la CNIE permettra de signer avec la clé privée contenue dans la puce. La fonction de vérification est assurée à l'aide du certificat d'identification électronique (contenant la clé publique), alors que la fonction de signature sera remplie par l'utilisation de la clé privée de signature. En d'autres termes, la CNIE devrait contenir deux certificats différents, l'un pour

<sup>90</sup> Règlement (CE) n°2252/2004 du Conseil 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 Etats membres, JOUE du 20 décembre 2004, L. 385/1.

<sup>91</sup> E. A. Caprioli et P. Agosti, note sous arrêt, JCP éd. G, 2001, II, 10606, p. 1890 et s.

<sup>92</sup> Confirmé par un arrêt de la Cour de cassation du 30 avril 2003 (Bull. civ, II n° 118 p. 101).

l'authentification de la personne et de la carte, l'autre pour signer des téléprocédures et des achats (on peut également envisager d'intégrer deux moyens de signature distincts selon que l'on se trouve dans la sphère publique ou privée).

## **II – L'identité risquée**

Aux termes de l'article 2 de la loi du 6 janvier 1978 modifiée par la loi du 6 août 2004, constitue une donnée à caractère personnel, « *toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose et auxquels peut avoir accès le responsable du traitement ou toute autre personne* ». Les empreintes digitales comme la photographie et les autres données propres à la personne contenues dans le nouveau support de carte d'identité constituent des données à caractère personnel. Si ces données suivent un régime juridique spécial, les données biométriques sont particulièrement sensibles<sup>93</sup>.

En matière biométrique, la loi Informatique et Libertés trouve à s'appliquer<sup>94</sup>. Ainsi, un jugement du TGI de Paris en date du 19 avril 2005<sup>95</sup> traite de la mise en place d'une pointeuse biométrique pour contrôler le temps de présence des salariés dans une entreprise. Invoquant de nombreux problèmes de décomptes des heures de présence, en vue de l'établissement des bulletins de paie, cette entreprise, chargée des services en gare aux voyageurs, avait opté pour un système de lecteur biométrique. Ce lecteur fonctionne par validation de la correspondance entre l'empreinte digitale du salarié mémorisée sur une carte à puce et celle du doigt appliqué sur l'appareil. Opposés à un tel dispositif, les salariés de l'entreprise ont assigné l'entreprise pour le faire interdire. Les conditions préalables à la mise en œuvre ont été respectées (informations des salariés, déclaration à la CNIL, présentation au Comité d'Entreprise). Les juges rappellent que l'empreinte digitale n'est pas une donnée comme les autres puisqu'elle « *permet d'identifier les traits physiques spécifiques qui sont uniques et permanents pour chaque individu* ». Elle doit donc être traitée avec une grande vigilance. « *Son utilisation qui met en cause le corps humain et porte atteinte aux libertés individuelles peut cependant se justifier lorsqu'elle a une finalité sécuritaire ou protectrice de l'activité exercée dans les locaux identifiés* ». Pour ce faire, le tribunal se fonde sur l'article L. 120-2 du code du travail qui prévoit que l'on ne peut porter atteinte aux libertés sauf si c'est justifié par la nature de la tâche à accomplir et proportionné au but recherché. En l'espèce, le système devait permettre de comptabiliser les heures de travail et d'améliorer l'établissement des bulletins de salaires. Il n'a pas été considéré comme proportionné au but recherché. La sécurité de l'accès aux lieux aurait été admise, mais les lieux étant publics, cet argument ne pouvait être retenu. Les juges s'appuient également sur la

---

<sup>93</sup> V. notamment certaines délibérations de la CNIL à ce sujet :

- [Délibération n° 80-019 du 3 juin 1980](#) portant avis relatif à la création d'un traitement automatisé d'informations nominatives concernant la fabrication de cartes nationales d'identité ;
- [Délibération 86-76 du 01 juillet 1986](#) portant avis sur un projet de décret relatif à la création d'un système de fabrication et de gestion informatisée des cartes nationales d'identité ;
- [Délibération 86-105 du 21 octobre 1986](#) portant avis sur le relevé d'une empreinte digitale à l'occasion d'une demande de carte nationale d'identité ;
- [Délibération 92-026 du 17 mars 1992](#) portant avis sur un traitement automatisé d'informations nominatives mis en oeuvre par le ministère de l'intérieur relatif à la gestion automatisée de la délivrance des cartes nationales d'identité et des passeports.

<sup>94</sup> Loi n°78-17, Informatique, Fichiers et Libertés, modifiée par la loi du 6 août 2004.

<sup>95</sup> Disponible sur le site [www.legalis.net](http://www.legalis.net).

directive européenne sur la protection des données personnelles qui reprend ces principes pour refuser le recours à cet identifiant.

Par ailleurs, l'article 25 de la loi Informatique et Libertés dispose que « *Sont mis en œuvre après autorisation de la CNIL[...] 6° Les traitements automatisés comportant des données biométriques nécessaires au contrôle de l'identité des personnes* ». La CNIL a souligné, à de nombreuses occasions, les risques liés à la biométrie.

L'utilisation des empreintes digitales dans la C.N.I.E. génère des risques en termes d'atteinte à la vie privée ou de respect des libertés individuelles. Ils devront être pris en compte au moment du déploiement de la C.N.I.E. Ce projet intéressant l'ensemble de la société française devra être proportionné et limité quant à ses effets.

Par exemple, des mesures de sécurité devront être prises pour que les données biométriques soient embarquées dans la puce de la C.N.I.E. La gestion de ces données ne devrait pas être centralisée au sein d'une base de données, sauf à imposer des garanties techniques et juridiques aptes à assurer la sauvegarde des droits fondamentaux des citoyens.

### **III – L'identité sécurisée**

La C.N.I.E. ne saurait se résumer à une pièce d'identité. **La mise en place de nouveaux fichiers contenant l'état civil ou remplaçant les fichiers nationaux existants de cartes d'identité et de passeports (sous certaines conditions de sécurité) devrait permettre une meilleure gestion des titres et en faciliter la demande.** Elle devrait également servir au développement du passeport INES, de manière sécurisée. Les données nécessaires seront collectées dans les mairies au moment du dépôt de la demande. Le développement de nouveaux services d'e-gouvernement (tels que la déclaration fiscale ou les demandes de documents en ligne) et la dématérialisation des échanges de documents commerciaux justifie le besoin d'un moyen d'authentification sécurisé et de signature électronique. L'authentification consistera à vérifier l'identité d'une personne grâce à la possession d'un support, à l'activation de données connues du seul titulaire de la carte et à l'identification biométrique<sup>96</sup>. C'est le moyen le plus sécurisé qui soit, encore plus que les outils de signature électronique à clé publique actuels du marché qui n'utilisent pas de données biométriques. De plus, le certificat permet de s'assurer de la validité du document électronique.

La C.N.I.E. permet donc d'autres fonctions assurant une plus grande sécurité pour l'administré dans le cadre de ces relations électroniques. A ce titre, la C.N.I.E. comprend :

- un bloc « authentification de la carte », permettant de prouver l'authenticité de la carte ;
- un bloc « identification authentifiée du porteur » ou « *identification certifiée* » (activé par un code PIN secret connu du seul titulaire) permettra d'accéder à des téléprocédures publiques ou privées (par exemple accès à son compte en banque, ... ) ;
- un bloc « signature électronique » permettra (le procédé devrait être activé au moyen d'un code PIN secret) de signer électroniquement des documents,

---

<sup>96</sup> L'identification d'une personne en environnement électronique résulte de la réunion de trois moyens, à savoir ce qu' :

- elle est (et qu'il déclare être) : caractéristiques physiques, administratives ou techniques qui se trouvent dans le certificat, qui lui est propre ;
- elle connaît : il s'agit d'un code personnel et/ou d'un mot de passe permettant de déclencher le procédé de création de signature ;
- elle possède : carte à piste magnétique ou à micro-processeur ou tout autre support sur lequel sont stockés la clé privée et le certificat du signataire.

soit à l'intention d'une e-administration, soit pour toute transaction électronique privée ;

- un bloc « portfolio personnel » : cette fonction optionnelle doit permettre de stocker, à titre personnel, des informations complémentaires dans la carte, soit pour faciliter leurs transactions électroniques (par exemple : stocker de manière « exportable » nom, prénom, adresse, pour remplir des formulaires), soit pour remplacer d'autres papiers (ex : numéro de permis de conduire, numéro fiscal, etc). Le projet d'ordonnance prise en application de l'article 3 de la loi n°2004-1343 du 9 décembre 2004 de simplification du droit prévoit dans son article 6 un dispositif répondant aux mêmes caractéristiques.

Ces fonctionnalités supplémentaires sont fondées sur l'usage de certificats électroniques : « *l'identification authentifiée du porteur ou titulaire de la carte et de la signature électronique sont réalisées par le recours à des certificats électroniques émis par l'Etat, garantissant l'identité du titulaire de la carte et permettant à l'interlocuteur (commerce ou administration par exemple) de s'assurer électroniquement qu'il a affaire au bon usager et que celui-ci est pleinement d'accord avec la transaction en cours* »<sup>97</sup>. Dans cette perspective, il est à remarquer que la Politique de Référencement Intersectoriel de l'A.D.A.E. (PRIS, V.2)<sup>98</sup> distingue plusieurs politiques de certification : authentification, signature électronique et confidentialité. On peut observer, en cet endroit, que la C.N.I.E. ne contiendra pas de moyen de cryptologie pour assurer la confidentialité des échanges électroniques.

Cette situation s'inspire largement des usages qui sont en train de voir le jour sur le marché. Les définitions du certificat et de la signature électronique existent en droit privé. Ainsi, selon l'article 1316-4 du code civil, la signature « *identifie celui qui l'appose. Elle manifeste le consentement des parties aux obligations qui découlent de cet acte.* » En outre, l'article 1316-4 alinéa 2 du code civil définit la signature électronique comme « *un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache.* ». Le certificat, quant à lui, s'entend « *d'un document sous forme électronique attestant du lien entre les données de vérification de signature électronique et un signataire* »<sup>99</sup>.

**L'identité sécurisée en droit privé** se construit autour de la notion de fiabilité du procédé d'identification. Cette notion nécessite certains approfondissements. L'article 2 du décret n°2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du Code civil<sup>100</sup> pose les conditions permettant de présumer fiable un procédé de signature électronique. Ainsi, ce procédé doit mettre en œuvre une *signature électronique sécurisée*, établie grâce à un *dispositif sécurisé de création de signature électronique* et la vérification de cette signature repose sur *l'utilisation d'un certificat électronique qualifié*.

La **signature électronique sécurisée** doit être propre au signataire, être créée par des moyens qu'il puisse garder sous son contrôle exclusif et garantir avec l'acte auquel elle s'attache un lien tel que toute modification ultérieure soit détectable. Cette signature est établie grâce à un dispositif sécurisé de création de

---

<sup>97</sup> V. le programme INES dans son glossaire technique.

<sup>98</sup> Disponible à l'adresse : [www.adae.pm.gouv.fr](http://www.adae.pm.gouv.fr).

<sup>99</sup> Article 1.9 du décret n° 2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique, J.O. du 31 mars 2001 p. 5070 et s. E. Caprioli, *Ecrit et Preuve électroniques dans la loi n°2000-230 du 13 mars 2000*, J.C.P. éd. E, Cahiers de droit de l'entreprise, n°2, 2000, p. 1-11.

<sup>100</sup> JO du 31 mars 2001, p. 5070 et s. E. Caprioli, *Commentaire du décret n°2001-272 du 30 mars 2001 relatif à la signature électronique*, Revue de Droit Bancaire et financier, Mai/juin 2001, p.155 s.

signature. Suivant les dispositions de l'article 3-II du décret du 30 mars 2001, ce dispositif devra être certifié conforme par le Premier ministre, dans les conditions prévues par le décret n°2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information<sup>101</sup>, ou encore par un organisme désigné à cet effet par un Etat membre de la communauté. Le décret du 18 avril 2002 met en place les procédures d'évaluation et de certification tant pour les produits que pour les systèmes des technologies de l'information (dans le cas qui nous intéresse, les dispositifs de création de signature électronique). Cependant, la procédure générale d'évaluation et de certification ne concerne que l'aspect administratif de la démarche ; l'aspect technique étant précisé dans des documents normatifs. Ainsi, pour les dispositifs de création de signature, les référentiels servant à les évaluer sont publiés au Journal Officiel des Communautés européennes<sup>102</sup>. Toute certification de dispositif de création de signature devra respecter la démarche décrite dans le décret du 18 avril 2002 auprès d'un centre d'agrément qui respectera lui-même les exigences de la Direction Centrale de la Sécurité des Systèmes d'Information (D.C.S.S.I.).

Ces exigences techniques vont de pair avec une sécurité juridique importante dans le monde électronique : l'identification du signataire. Celle-ci est assurée – indirectement – par le Prestataire de Services de Certification Electronique. La qualification qu'il a demandée à un organisme accrédité selon la procédure décrite à l'arrêté du 26 juillet 2004 relatif à la reconnaissance des prestataires de services de certification électronique et à l'accréditation des organismes qui procèdent à leur évaluation<sup>103</sup> permet aux demandeurs de certificats de s'assurer de la fiabilité de ses services, et notamment du respect des exigences de l'article 6-II du décret du 30 mars 2001. Cette garantie d'identification du signataire est essentielle. Ceci explique sans doute pourquoi le régime de responsabilité civile du Prestataire de Services de Certification Electronique est particulièrement exigeant en matière de certificats présentés comme étant qualifiés (article 33 de la Loi pour la confiance dans l'économie numérique<sup>104</sup>). S'agissant de la responsabilité, étant donné que l'Etat devrait jouer le rôle d'autorité de certification, une sage précaution consisterait à limiter la valeur d'usage du certificat de signature embarqué dans la carte à une valeur de transaction ne dépassant pas par exemple un montant de 10.000 euros. Cette mesure permettra de limiter la responsabilité de l'Etat si la C.N.I.E. est utilisée dans les transactions d'achats privés. Pour les téléprocédures, la problématique se pose en des termes différents dans la mesure où c'est l'Etat qui est le destinataire de la signature.

**Une identité sécurisée doit donc répondre à différentes conditions afin de prouver la fiabilité du procédé d'identification.**

La loi n°2004-1343 du 9 décembre 2004<sup>105</sup> prévoit dans son article 3 une ordonnance dont l'objectif est d'assurer la sécurité des informations échangées par voie électronique entre les usagers et les autorités administratives ainsi qu'entre autorités administratives et de permettre et de favoriser la signature électronique

---

<sup>101</sup> JO du 19 avril 2002, p. 6944.

<sup>102</sup> Décision de la Commission 2003/511 du 14 juillet 2003 relative à la publication des numéros de référence de normes généralement admises pour les produits de signatures électroniques, conformément à la directive 1999/93/CE du Parlement européen et du Conseil, JOCE L. 175 du 15 juillet 2003, p. 45 et s.

<sup>103</sup> J.O du 7 août 2004, p. 14104 et s.

<sup>104</sup> Loi n°2004-575 du 21 juin 2004, J.O. du 22 juin 2004, p. 11168 et s. V. l'ouvrage à paraître aux éditions L.G.D.J., en 2005 sur la LCEN commentée article par article, sous la direction de E. Caprioli.

<sup>105</sup> J.O. du 10 décembre 2004, p. 20857 et s.

des actes des autorités administratives. Le projet d'ordonnance a pour visa le Code civil et notamment son article 1316-4.

Toutefois, l'équivalence semble se limiter aux fonctions attendues de la signature. Un référentiel général de sécurité prévu dans son projet d'article 7 définit des exigences de sécurité pour différentes fonctions qui contribuent à la sécurité des informations échangées par voie électronique, notamment les fonctions d'identification, de signature électronique, de confidentialité etc. (la PRIS). Au vu des fonctions de la C.N.I.E. telles qu'elles ont été exposées, la question se pose de savoir si la C.N.I.E. entre dans le cadre de ce référentiel de sécurité.

Enfin, si les certificats électroniques utilisés par les autorités administratives semblent devoir être émis par une autorité de certification « *publique* » comme l'énonce le projet d'article 10, rien n'est dit concernant les certificats utilisés par l'administré lui-même. On peut penser que certains prestataires du secteur privé pourront émettre des certificats qui seront contenus dans la CNIE dans le respect des conditions du projet d'article 7. Le fait que la C.N.I.E. puisse contenir un certificat de signature pour les usages privés nous semble opportun pour le développement des échanges sécurisés, à l'instar de ce que la Belgique a réalisé en la matière. La C.N.I.E. nous paraît être une chance pour le déploiement des moyens de signature à l'échelle de l'ensemble de la population et ce serait une action de lutte de l'Etat contre la fracture numérique si le coût de la C.N.I.E. n'est pas trop élevé.

**La CNIE nécessitera par conséquent la combinaison de plusieurs facteurs : un encadrement législatif assurant la mise en place de moyens techniques permettant de garantir les droits des citoyens**

**Eric CAPRIOLI**

\* \* \*

**XXII. Contribution de Thierry AUTRET, expert en sécurité informatique et Marie-Laure LAFFAIRE, Avocat à la Cour d'Appel de Paris – 1<sup>er</sup> juin 2005**

Par **Thierry AUTRET**

Expert Sécurité, Groupement des Cartes Bancaires

Co-auteur de l'ouvrage « *Sécuriser ses échanges informatiques avec une PKI – solutions techniques et aspects juridiques* », Eyrolles, 2002

Et

**Marie-Laure LAFFAIRE**

Avocat à la Cour d'Appel de Paris

Co-auteur de l'ouvrage « *Sécuriser ses échanges informatiques avec une PKI – solutions techniques et aspects juridiques* », Eyrolles, 2002

Auteur de l'ouvrage « *Protection des données à caractère personnel – tout sur la nouvelle loi Informatique et Libertés* », Eyrolles, 2005.

Le projet INES et le débat national sur la carte d'identité électronique qui s'en suit appellent de la part de l'expert en technologies et de l'expert juridique maintes réflexions. Tour à tour complémentaires, combinées, superposées ou encore opposées, ces interrogations posent avec force **la question de la compréhension actuelle des technologies par le droit et du droit par les technologies**. Telle est la richesse inspirée de ce débat centré sur le citoyen sous ses deux mots d'ordre : plus de facilité, plus de sécurité.

La carte nationale d'identité électronique (CNIE) aurait pour objectif de définir et de relier les hommes, tous citoyens et sujets de droit, par des technologies et des procédures garanties sécurisées par l'administration, permettant de les identifier et plus encore, de signer des transactions en ligne ou encore de porter un « portfolio personnel », et ce pour des usages variés simplifiés et, serait consultable par des entités et des personnes dûment habilitées à cet effet, sous forme bi-mode (sans contact ou par l'intermédiaire d'un lecteur de carte).

La CNIE ne serait semble t'il pas obligatoire...mais payante.

**Qu'entendons-nous par carte nationale d'identité ?**

Si l'étymologie raconte l'histoire des mots, il est toujours plaisant de se plonger dans un vieux « Nouveau Petit Larousse Illustré » datant de 1939 – en général celui de nos grands-parents – par pure curiosité et parce que **la vérité**, si ce n'est **la logique**, ou à tout le moins **le bon sens**, devraient forcément ressortir de cette lecture.

C'est ainsi que tout bonnement **le terme « identité » est défini sous trois angles :**

- un angle générique : « ce qui fait qu'une chose est la même qu'une autre »
- un angle juridique (Dr.) : « ensemble des circonstances qui font qu'une personne est bien telle personne déterminée : *découvrir l'identité d'un criminel ; produire une pièce d'identité.* »
- un angle technique (Math.) : « égalité dont les deux membres sont identiquement les mêmes ».

Et qu'aujourd'hui, le « Petit Larousse Illustré » de 2005, 100<sup>ème</sup> éditions, sans s'écarter de ces définitions, donne celle de **la pièce d'identité** en ces termes :

«En France, document officiel qui comporte une photographie et des indications d'état civil. »

**Postulat** : nous sommes d'accord pour dire que l'identité se rapporte à un individu et que la carte nationale d'identité, qui est une des formes officielles de cette identité, doit se placer sur le plan purement juridique.

### **Que comprenons-nous des techniques et du droit ?**

Le postulat de départ est bien ici que la technique est au service du droit. **Le problème majeur** que nous avons pu identifier depuis plusieurs années et qui apparaît de la même manière dans le cadre du projet INES **est celui de l'adéquation entre une fonction technologique donnée et une fonction juridique recherchée**. L'un place toutes ses espérances dans l'autre et l'autre tente de se rassurer sur le bien fondé du « mandat » qu'il vient ainsi de donner ...

L'exemple par excellence est celui de la **signature électronique** qui, en tant qu'exigence ou besoin juridique selon le cas, fait aujourd'hui majoritairement appel à une technique particulière, non neutre, celle de la cryptographie asymétrique.

Celui qui est capable de produire une transformation d'un écrit électronique combiné à un secret possédé, délivré et utilisé selon des règles définies par la loi, et qui est vérifiable par tous ses correspondants, exprime son accord sur la chose signée en affichant clairement son identité par le biais du certificat. La **cryptographie asymétrique** offre aujourd'hui le seul moyen combinatoire des exigences exprimées par le législateur si tant est que **les règles organisationnelles** qui l'accompagnent sont bien respectées.

Le chemin parcouru entre une technologie donnée et l'exigence juridique souhaitée est plus que direct (« *straight* » diraient les anglo-saxons). Ainsi, à grand renfort d'idées de « génie » et d'assurances réciproques (souvent liées à l'absence ou la mauvaise connaissance des métiers de chacun), le tout fondé sur des distorsions malheureuses de vocabulaire (voir sur ce point le mini-glossaire du projet INES), l'amalgame entre une fonction juridique et une fonction technique de sécurité est vite fait. De là, naissent des incompréhensions, des doutes et des peurs, bien légitimes il faut l'avouer.

Cet écueil malheureux doit absolument être évité. Les technologies les plus attaquées, comme celle de la **biométrie**, ne sont pas selon nous les moins sûres sur le plan juridique dans leur concept si tant est qu'elles aient comme pivot l'individu lui-même et non des substituts externes, tels que bases de données ou autres moyens comparables.

Pour autant, la question de l'adéquation d'une technique de sécurité à la finalité de son objet, que ce soit sur le plan éthique, social ou philosophique, reste entière.

### **Quels sont les principaux centres de préoccupations : qualité, quantité et dépendance ?**

Une fois les possibilités arrêtées, quelques préoccupations se dessinent.

#### **1. La qualité dans le chaînage technologique, juridique et des usages**

Le projet CNIE pourrait être schématisé sous la forme de **trois sous-ensembles de chaînes**, eux-mêmes liés entre eux.

- **la chaîne technologique ;**
- **la chaîne des usages ;**
- **la chaîne juridique.**

### La chaîne technologique

Les informations techniques qui ont été publiées sur le projet INES laissent supposer l'emploi de **plusieurs technologies** qui, même si elles ne sont plus pour certaines de l'ordre des nouvelles technologies, lorsqu'elles sont chaînées rendent paradoxalement **l'ensemble raisonnablement sensible**. Sous l'angle de la sécurité au quotidien, le peu de recul sur les techniques du « sans contact » ou de la biométrie seront des éléments qui nécessiteront la plus grande attention quand aux détournement que ne manqueront pas d'en faire les *hackers* potentiels et autres délinquants organisés. Les besoins contradictoires de l'ergonomie d'une part et de la gestion de la sécurité d'autre part seront également une source de **complexité** à gérer avec le plus grand soin. D'emblée la durée de vie annoncée du support nécessite l'emploi de solutions permettant l'évolution des données de sécurité en post-personnalisation. Le recul sur les techniques de cryptographie bien maîtrisées aujourd'hui montrent le besoin d'adaptabilité rapide des paramètres des algorithmes, voire des algorithmes eux-mêmes.

Après plus de vingt ans de pratique sur le terrain, la carte à microprocesseur est désormais un outil éprouvé dont la technologie intrinsèque et la chaîne de production sont bien maîtrisées. Néanmoins cette base fait l'objet d'**évolutions multiples** tant sur le plan des techniques « liées au silicium », que sur les interfaces de communication (sans contact) ou sur les couches applicatives, qu'elles soient masquées ou sur base d'OS.

Le **challenge technologique** sera donc très important au regard du peu de recul sur la stabilité des standards sur lesquels il s'appuie. Si le socle IAS<sup>106</sup> est retenu pour INES, celui-ci a déjà fait l'objet de deux versions en un an et une troisième est en préparation. La normalisation du *middleware* pour l'interface carte (ISO 24727) est également en cours de stabilisation. Quant à la biométrie, même si les normes de l'OACI semblent emporter l'adhésion, c'est plus la pratique sur le terrain qui manque de recul.

### La chaîne des usages

La deuxième concerne le chaînage des usages qu'il sera possible de faire avec la CNIE. La finalité institutionnelle la destine en premier lieu à prouver de son identité face à des représentant de l'autorité. Mais sa **conception multifonctionnelle** la destine également à assurer l'identification de son porteur dans le cadre de relations dématérialisées avec les institutions gouvernementales au travers des portails des différents ministères. Dans ces deux cas la responsabilité de l'Etat est engagée quand à la fiabilité du support utilisé dans la perfection de l'acte. Mais l'annonce officielle étend l'usage de la CNIE à « *tous les services financiers et commerciaux sur Internet* ». Quelle sera alors la prise de responsabilité de l'état en cas de problème lié à une transaction électronique contractualisée entre un citoyen et un acteur privé ? Les exigences issues de la loi devront s'appliquer à l'état en tant qu'émetteur de certificats que l'on peut imaginer être « *qualifiés* » même si les informations disponibles ne le disent pas. Si tel est le cas, le **marché des émetteurs de certificats** du secteur privé, et en premier lieu celui des autorités de certification bancaires, disparaîtrait de fait. Un scénario alternatif qui avait été imaginé était celui de la prise en compte de la CNIE comme justificatif d'identité fiable par une autorité d'enregistrement/autorité de certification qui a son tour émettrait un certificat pour la finalité requise, par exemple par une banque pour des transactions financières ou commerciales.

---

<sup>106</sup> Identification, Authentication and electronic Signature : spécifications techniques pour une plateforme commune pour l'eAdministration réalisée par le GIXEL pour l'ADAE.

### **La chaîne juridique**

La troisième tient aux tenants et aux aboutissants de la CNIE. Quelles implications juridiques dans l'usage de la CNIE ? **Comment le chaînage juridique est-il assuré compte tenu des imbrications complexes qu'elle appelle ?** Entre le porteur de la carte, les procédures mises en place pour la délivrance, les incidents (vol, perte, ...), le retrait, les individus habilités à intervenir, les applicatifs qui seront émuloés par la carte et les technologies sous-jacentes ou sur-jacentes, les plans bis et autres plans de secours, le chaînage juridique ne peut qu'être malmené.

A une autre échelle, ce type de projet implique systématiquement l'analyse des rôles, des obligations et des garanties et enfin, des responsabilités des différents intervenants. C'est ce que nous pouvons appeler, le **Schéma des Responsabilités**. Ce schéma induit l'**encadrement juridique** à organiser (garantie fixée à une période donnée par exemple) et suppose la **sensibilisation corrélative des acteurs** (information, formation et accompagnement).

## **2. La quantité dans le cumul des technologies, des usages et des ressorts juridiques**

Notre observation sera ici assez liminaire. Il est constant que **la multiplication des technologies**, dont certaines sont encore peu éprouvées ou soulèvent des préoccupations tardivement identifiées, militent pour la prudence chez l'homme de l'art.

A titre d'exemple l'**archivage des documents électroniques signés** est un domaine où les expériences de plusieurs métiers doivent se coordonner et en premier lieu sur le vocabulaire des uns et des autres : les archivistes (issus de la gestion de l'archive papier), les gestionnaires de documents électroniques (GED), les juristes et professions réglementées, les experts de la cryptographie/horodatage, etc. Certaines problématiques sont bien identifiées, d'autres beaucoup moins, certaines solutions existent, mais celles-ci correspondent-elles bien aux problématiques, majoritairement juridiques ? **Le droit doit selon nous s'adapter à ce nouveau mode de raisonnement**, car la conception technologique de base (le mode binaire des 0 et des 1) en constitue le socle.

Dans le même ordre d'esprit, **la multiplicité des usages** liés à la CNIE et le **nombre important de données** qu'elle contient et surtout qu'elle génère (définitivement des données à caractère personnel) ne peuvent que créer un sentiment de crainte.

En effet, non seulement **ces usages ne sont pas clairement et précisément identifiées** (ce sera donc toute fonction d'identification existante et des nouvelles, telle que l'auto-identification de la carte) mais encore, le projet INES ajoute de **nouvelles fonctions** jusqu'alors inconnues sous cette forme et dans ce cadre : accès à des télé-procédures publiques ou privées, signature électronique (au sens de signature manuscrite) de transactions sur Internet ou de documents authentiques, gestion d'un espace personnel de stockage (le « portfolio personnel »), et d'autres à venir...

Enfin, **les fonctions et les implications juridiques** qui en découlent sont de taille. L'identité est au cœur des préoccupations de notre droit car elle permet de faire **le lien entre un individu et un fait ou un acte juridique** : c'est l'essence même du droit, le point de départ de tout raisonnement juridique, l'essence même de l'imputabilité.

Le juriste, rigoureux par nature, prudent en toute situation et imaginatif confronté à un contexte nouveau ne peut que militer en faveur d'une **mise à plat de ces ressorts juridiques**, complexes et nombreux, par usage identifié selon les technologies employées (cf. notre Schéma des Responsabilités). Un « trop d'usage » génère un « trop de conséquences juridiques » et des risques juridiques inhérents.

### **3. La liberté face aux questions de dépendance technique, juridique et pratique**

**Sur le plan technologique**, les principales inquiétudes tiennent au cumul des dépendances, à la corrélation potentielle de faiblesses, à l'interopérabilité, à la certification d'un produit additionnant les technologies. Dans la théorie de la complexité on peut penser que la résultante du cumul de telles technologies respectera plus probablement une progression géométrique qu'arithmétique.

**Sur le plan juridique, la dépendance est interne** : quelles sont les garanties données ? Qui sera en charge des contrôles (auto-certification...) Quelles preuves seront générées et admissibles d'un côté comme de l'autre ? Quelles sont les responsabilités encourues, notamment au niveau du gouvernement lorsque tout simplement il s'agira de « **remonter** » **la chaîne juridique** ?

**La dépendance est aussi externe, par le biais de lois étrangères** de plus en plus actives sur le territoire français et européen (on se souvient de la loi dite de « blocage » du 26 juillet 1968 adoptée afin de protéger les entreprises françaises contre les enquêtes menées à tout va dans le cadre d'actions étrangères). La dépendance externe est aussi celle de l'individu lui-même qui pourra, par pression ou en donnant son consentement (soit au moyen d'un mécanisme juridique de base, à la fois atout et faille juridique) faire droit à toute sorte de demande...

**Sur le plan pratique**, cet état de fait a été parfaitement résumé par l'expression de « **fracture socio-technologique** ». Lorsqu'un français est encore identifié comme tel parce que c'est le seul à taper avec quatre doigts sur son clavier d'ordinateur, les inquiétudes ne sont pas chimères. Une telle innovation implique une forte sensibilisation et un accompagnement de la population toute entière.

**Nul citoyen ne pourra se prononcer sur une CNIE opaque, qu'il ne connaît pas et ne maîtrise pas mais qu'il doit utiliser et qu'on lui oppose.**

**Si notre contribution devait se résumer en quelques mots, ils seraient les suivants : simplicité technique, juridique et pratique à l'image de la confiance du citoyen et de la transparence qu'il attend.**

**Thierry AUTRET et Marie-Laure LAFFAIRE**