



Séminaire de philosophie du droit 2005-2006
Sécurité, Sûreté, Surveillance.
8^{ème} séance, lundi 20 mars 2006

Identité et identification au prisme de la biométrie

par Ayse CEYHAN,
Chargée d'enseignements à Sciences-Po

Les projets de biométrisation des documents de voyage et des cartes d'identité ont soulevé des interrogations non seulement quant à leur nécessité et efficacité mais aussi quant à leur impact sur la notion d'identité, le symbolique de la carte d'identité et les processus d'identification¹. De nombreux observateurs ont souligné que l'utilisation des techniques biométriques mènerait à la distinction entre identité et identification et que cette dernière conduirait à la dé-symbolisation de l'identité assignée par l'Etat.

I - Identité, identification : contextes et enjeux

L'identité a toujours préoccupé les philosophes, les psychologues et les sociologues même si elle fut examinée sous des appellations différentes. Ainsi en philosophie, la question de la conciliation de l'identité et du changement a été soulevée dès les présocratiques. Si pour les uns comme Parménide il était difficile de penser le changement (l'être est un, continu et éternel) pour Héraclite, auteur du célèbre formule « on ne peut pas entrer deux fois dans le même fleuve » tout était, au contraire, en perpétuel mouvement. En fait, l'identité est un concept difficile à définir de façon synthétique. Elle englobe plusieurs éléments : comme le dit Erik Ericson, elle est à la fois conscience et processus². Du point de vue philosophique et psychologique elle est ce qui constitue la subjectivité de l'individu, du point de vue sociologique et philosophique, elle est liée à un ensemble de caractéristiques personnelles et relationnelles qui sont à la fois permanentes et socialement construites. La distinction de Paul Ricoeur³ entre deux pôles d'identité est éclairante à cet égard. Il s'agit de distinguer entre identité *idem*, c'est-à-dire ce qui est permanent comme le groupe sanguin, la filiation, l'âge et identité *ipse*, c'est-à-dire ce qui est changeant comme la définition du Soi par rapport à l'Autre. Dans cette perspective, l'identité n'est pas fixe, mais est constamment en mouvement entre ce qui est permanent et ce qui est changeant.

De même, les processus d'identification, c'est-à-dire l'assignation d'une identité reconnaissable ne sont pas nouveaux. Chaque fois qu'il y a groupement humain, il y a un processus d'identification pour savoir qui est qui et qui a le droit de faire partie du groupe ou de la communauté ou pas. Dans les sociétés traditionnelles, c'était la reconnaissance visuelle qui était la première technique l'identification. Au Moyen Age, on est passé du

¹ **Éléments définitionnels** : **Biométrie** : technologie d'identification et d'authentification qui consiste à transformer les caractéristiques biologiques, morphologiques et comportementales d'une personne comme les empreintes digitales, l'empreinte de la rétine, de l'iris, la voix, la forme du visage et de la main en une empreinte numérique. Son objectif est de permettre d'attester l'unicité d'une personne à partir de la mesure des parties inchangeables du corps (Bios). En fait c'est une technique ancienne utilisée dès la Chine ancienne pour identifier les personnes. De nos jours, ce qui fait sa particularité, c'est son couplage avec les capacités de l'optique, de l'électronique et de l'informatique, ainsi qu'avec les méthodes mathématiques et statistiques.

Identification : processus d'assignation, d'attestation et de reconnaissance d'une identité. Elle se fait de façon administrative par l'Etat, mais aussi de façon relationnelle par les rapports sociaux (conception procédurale). Dans le monde numérique, elle se fait par l'association de codes (codes PIN, mots de passe etc) et des données personnelles.

Authentification : processus de certification permettant d'associer une identité à une personne qui prétend procéder à une action. Elle permet de vérifier que la personne qui détient une carte d'identité ou une carte d'accès, ou qui entreprend une action dans l'Internet est bien le titulaire de la carte ou l'auteur de l'échange sur le net.

² E. Erikson, *Enfance et société*, Neuchâtel-Paris, Delachaux & Niestlé, 1982; *Identity and Life Circle*, New York, International Universities Press, 1967.

³ P. Ricoeur, *Soi même comme un autre*, Paris, Le Seuil, 1990. Voir aussi, l'audition d'A. Garapon par la CNIL le 14 avril 2005.

visuel au support matériel par l'inscription par les curés des naissances et des morts dans les registres. Sous l'Ancien Régime en 1539, l'ordonnance de Villers-Cotterêts a prévu l'ouverture des registres dans tout le royaume. Ensuite l'ordonnance de 1667 a transformé les registres paroissiaux en véritables registres d'état civil. L'acte d'état civil est ainsi devenu la preuve de l'enregistrement officiel de l'identité. Dans le droit français c'est lui qui fonde la personnalité juridique d'un individu. Il y a tout un courant de sociologie politique historique qui s'est attaché à travailler sur ces processus qui sont devenus des processus d'encartement avec la construction de l'Etat-nation (voir les travaux de Gérard Noiriel, Pierre Piazza, John Torpey⁴).

Avec l'Etat-nation, l'identification est devenue une technique de pouvoir et de gouvernement des individus. Dans ce processus, c'est la bureaucratie centrale qui, pour établir le monopole de l'Etat sur la violence légitime, instaurera un contrôle sur les populations à l'intérieur d'un territoire bien délimité par les frontières (Weber). Ce contrôle sera exercé par l'attribution d'une « identité représentée » c'est à dire réduite à un ensemble de signes symboliques pertinents pour les agents de l'administration chargés à la fois de les construire, de les enregistrer et de les vérifier⁵. Ces symboles sont des identifiants à la fois biologiques (l'âge, le sexe, et la taille) filiaux (nom) et sociaux (l'adresse et la profession dans certains cas). Toutefois, rien ne dit qu'ils sont inchangeables, sauf l'âge et la taille tout peut être changé, même le sexe.

En même temps, l'Etat créera une nation qui « ne désignait pas seulement une entité abstraite, un « principe spirituel, mais une communauté sociale regroupant des individus qui appartiennent à un même Etat »⁶. Avec la carte nationale d'identité délivrée aux Français, l'Etat accomplira sa tâche d'unification de la nation et d'inclusion des nationaux. Enclenché sous la Troisième République, affirmé sous Vichy, ce processus de longue durée se consolidera véritablement après le régime pétainiste⁷. C'est ainsi que la communauté va revêtir une dimension concrète. Toutefois, il convient de rappeler que ce processus s'est opéré par la distinction entre citoyens et ressortissants étrangers et a donné lieu à des logiques d'inclusion et d'exclusion. Ces logiques ont été accentuées au sein même de la société par la distinction entre « honnêtes citoyens » et criminels qu'il fallait absolument identifier par des méthodes précises pour éviter les récidives ou identifier les catégories à risque comme les nomades (par exemple le bertillonnage sous la Troisième République). Il faut également évoquer la création des documents de voyage comme les passeports qui attestent de l'appartenance d'une personne à un Etat et permettent à son possesseur d'être reconnu comme tel par le pays étranger qu'il visite ou traverse⁸.

⁴ G. Noiriel, Etat, nation, immigration. Vers une histoire du pouvoir, Paris, Belin 2000; P.Piazza, Histoire de la carte nationale d'identité française, Paris, Odile Jacob, 2004, J.Torpey, The Invention of Passport Surveillance, Citizenship and State, Cambridge University Press, 2000.

⁵ G.Noiriel, Op.Cit.

⁶ G. Noiriel, Les origines républicaines de Vichy, Paris, Hachette, 1999, p.62 ; citée par P.Piazza, Op.Cit ;p, 15.

⁷ P. Piazza, Op.Cit., p.12.

⁸ A l'origine des passeports on peut citer les sauf- conduits et les lettres de marque que les rois (d'Angleterre et de France) donnaient aux marchands et aux représentants pour les protéger des pirates et du mauvais traitement des autorités étrangères. Le terme passeport a été utilisé pour la première fois dans un traité signé entre l'Angleterre et le Danemark le 11 juillet 1670. Ce traité reconnaissait le passeport comme preuve de nationalité. Vers 1920, le passeport est devenu un titre universel de voyage et accepté à la conférence de la Ligue des Nations en 1922.

Si les pouvoirs publics ont toujours cherché à améliorer les techniques d'identification, celles-ci n'ont pas toujours été suivies de l'adhésion totale des citoyens. Même si les résistances collectives ont été assez faibles⁹, comme le rappelle Pierre Piazza, il y a eu néanmoins des périodes de reflux : par exemple en 1921, le préfet de police Robert Leullier a institué l'apposition des empreintes digitales sur carte d'identité des Français, mais cette initiative a été vivement dénoncée comme une pratique associant l'honnête citoyen au délinquant. D'autres moments de reflux font suite à des moments où les pouvoirs publics ont durci leurs entreprises d'identification des Français¹⁰. C'est le cas en 1955 lorsque la carte cartonnée est instituée : en réaction à Vichy, on interdit les mentions discriminantes et la mention relative au mode d'acquisition de la nationalité française, la mise en place d'un fichier central des cartes d'identité est rejetée. Chaque fichier est géré au niveau préfectoral. De plus, l'apposition de l'empreinte digitale sur la carte elle-même est abandonnée à partir de 1974.

La France représente l'idéal type du pays où l'identification se fait par un processus d'assignation étatique menant à l'encartement des populations. Toutefois, des pays comme l'Angleterre et les Etats-Unis ont refusé l'instauration d'une carte d'identité pour des raisons philosophiques et historiques et ont inventé d'autres mécanismes pour identifier leurs citoyens (numéro de sécurité sociale, permis de conduire)¹¹.

Avec la biométrie, la question fondamentale est de savoir pourquoi il y a un besoin d'identifier les personnes par ce qui est inchangeable : le « bios » – les parties du corps inchangeables comme l'iris, la rétine, l'empreinte de la main – et de savoir pourquoi celui-ci est accepté comme l'identifiant ultime des individus au détriment des relations sociales et de l'intervention d'un tiers. De même, il s'agira de savoir pourquoi il faut relier l'empreinte captée à des bases de données pour identifier et authentifier les individus.

Pour répondre à ces questions, il convient d'examiner les caractéristiques du contexte actuel. Celles-ci sont la vitesse, la constitution des réseaux, l'affaiblissement des frontières physiques, l'émergence d'un monde virtuel dont la conséquence la plus marquante est l'érosion du territoire national comme source de pouvoir et comme référence structurant les rapports sociaux et économiques et la constitution d'une société mondiale de risque. Zygmunt Bauman décrit la société contemporaine en l'assimilant à un « état de fluide » qui est la qualité propre des liquides et des gaz, caractérisée par la fluidité, la compressibilité l'expansibilité, à l'opposé des solides caractérisés par la fixité, la lourdeur et l'immobilisme¹². Dans le contexte de la « modernité liquide », les processus d'identification se font à distance dans des espaces physiques et virtuels par de multiples acteurs qui ne sont pas des Etats-nations, mais aussi des acteurs privés (les compagnies d'aviation), des organisations internationales (l'OACI – Organisation internationale de l'aviation civile) et des entités régionales (UE). Avec la numérisation des empreintes et leur enregistrement dans des bases de données, l'identification se fait par la conservation et le suivi des traces de ces empreintes. Quant au monde virtuel, l'identification se fait par de nombreux symboles qui sont en constante évolution : les codes PIN, les mots de passe, les blogs etc qui ne dépendent que de l'imaginaire des utilisateurs.

⁹ G. Noiriél, Audition par la CNIL, le 15 février 2005.

¹⁰ Idem, pp. 145 -149

¹¹ Sur les Etats-Unis, voir A.Ceyhan, « La biométrie, une technologie pour gérer les incertitudes de la modernité contemporaine. Applications américaines », *Cahiers de la sécurité*, 2005.

¹² Z. Bauman, *Liquid Modernity*, London, Polity, 2000.

Dans ce contexte, il semblerait qu'identifier avec certitude qui est qui et lui assigner une identité fixe, inaltérable et universellement reconnaissable est devenue une préoccupation. Amplifiée avec la globalisation, la transnationalisation et l'émergence de nouveaux acteurs privés, comme les organisations terroristes, sur la scène mondiale et nationale, cette préoccupation a été renforcée avec les attentats du 11 septembre pour devenir un problème de sécurité. Aux yeux des hommes politiques et des spécialistes de la sécurité, les moyens traditionnels d'identification comme la carte nationale d'identité et le passeport en papier ainsi que les identifiants classiques comme le nom de famille, l'âge, le sexe, la filiation etc. seraient devenus de moins en moins pertinents pour prouver l'identité d'une personne. C'est le « bios » – les parties du corps inchangeables comme l'iris, la rétine, l'empreinte de la main – qu'il faudra considérer comme preuve infaillible de l'identité d'une personne. Comment analyser cet engouement pour la biométrie ? Nous verrons d'abord comment le recours à la biométrie est justifié par les pouvoirs publics, examinerons ensuite les différentes approches déployées par les défenseurs et les critiques de ce phénomène et proposerons enfin une piste d'analyse.

II - Eléments de justification avancés par les autorités publiques pour adopter la biométrie.

Pratiquement dans tous les pays qui se proposent de biométriser le document d'identité on rencontre les arguments suivants :

1 – Les normes de l'OACI et la lutte contre le terrorisme :

L'insertion d'éléments biométriques dans les documents d'identité a été décidée en Europe comme au niveau mondial en fonction de normes communes, issues des choix effectués au niveau international par l'Organisation Internationale de l'Aviation Civile (OACI). Dans une résolution datée du 9 mai 2003 (document 9303) celle-ci a décidé l'intégration d'ici 2016 de deux techniques biométriques dans les documents d'identité : une photo numérique de 12 octets et une biométrie à choisir entre empreinte digitale ou l'empreinte de l'iris ou de la rétine. Dans la pratique, il s'agira plutôt de la photographie numérique accompagnée de l'empreinte digitale intégrée dans une puce électronique et reproduites dans une zone de lecture automatique. Tandis que la France opte pour les empreintes digitales, d'autres pays comme l'Allemagne et l'Angleterre étudient la possibilité d'ajouter une sécurité supplémentaire avec l'empreinte de l'iris dont l'efficacité n'est pas encore prouvée à grande échelle. La sécurisation des passeports a été adoptée au niveau de l'Union Européenne par le règlement no 2252-2004 (CE) du Conseil du 24 décembre 2004. Selon ce règlement, les passeports des ressortissants européens doivent comporter une puce électronique intégrant des données biométriques et la photographie numérique de son titulaire.

S'appuyant sur la décision de l'OACI, les Etats-Unis ont imposé la possession des passeports biométriques aux ressortissants des pays étrangers qui veulent se rendre dans leur pays afin de lutter contre la menace du terrorisme. Depuis 2001, la nécessité de protéger la société contre la menace terroriste a été reprise par tous les gouvernements qui ont décidé de doter les documents de voyage et/ou d'identification de leurs ressortissant de technologies biométriques.

Il convient de rappeler que l'argument de lutte contre le terrorisme n'est pas nouveau. Il a été avancé dès les années soixante dix en Allemagne, en France et en Angleterre pour faire face aux divers terrorismes commis sur leur sol. Dans les années quatre vingts, il a été associé à la lutte contre l'immigration clandestine, la criminalité organisée et les incivilités (continuum sécuritaire¹³). Toutefois, les agences de sécurité et de renseignement reconnaissent elles-mêmes qu'il s'agit d'un argument relatif, et rien ne prouve, surtout quand on observe le terrorisme actuel (Al-Qaida) de dire que la sécurisation des documents d'identité est un moyen efficace de détection des terroristes en puissance et de ceux qui passent à l'acte. Un certain nombre de ceux qui ont commis des actes de terrorisme lié à Al-Qaida n'ont pas utilisé de fausses identités, certains ont juste enfreint la loi sur l'immigration aux Etats-Unis. Il semblerait que ces terroristes ont voulu que leurs identités soient connues après leur mort dans les attentats du 11 septembre (besoin de reconnaissance a posteriori).

2 - Lutte contre la fraude à l'identité¹⁴ :

Les spécialistes justifient le recours à la biométrie par l'augmentation de la fraude à l'identité (création d'identité fictive, usurpation d'identité, échange d'identité, utilisation de l'identité d'une personne décédée etc.) qui prendrait des proportions considérables. Dans tous les pays européens et aux Etats-Unis, les techniques de fraude comme le vol de titres vierges, la falsification des données, la contrefaçon, l'usage frauduleux d'un titre authentique volé ou emprunté à une personne, les vrais faux documents seraient en constante augmentation. Il est certain que dans un pays comme les Etats-Unis où il n'y a pas de carte d'identité nationale et où l'identité est prouvée soit par le numéro de sécurité sociale, soit par le permis de conduire, l'obtention frauduleuse de ces moyens est très aisée. Compte tenu de l'ampleur de ce phénomène qui, paradoxalement, n'est pas considéré comme un délit de premier ordre aux Etats-Unis, les chiffres et les origines de la fraude sont connus en raison de l'existence de statistiques. Ainsi selon les statistiques du Federal Trade Commission, la fraude en identité a touché 27.3 millions de personnes durant ces cinq dernières années. Toutefois, contrairement aux Etats-Unis, l'ampleur de la fraude à l'identité n'est pas vraiment évaluée en France. Il n'existe pas à l'heure actuelle de statistiques nationales harmonisées, ni d'unité spécialement chargée de la lutte contre la fraude documentaire¹⁵.

Cependant, selon un rapport d'information du Sénat, le problème de la fraude en France ne serait pas lié à une faille de sécurité de la carte d'identité nationale, mais serait dû à une chaîne d'identité défaillante et se situerait en amont du fait des fraudes à l'état civil qui conduisent à la délivrance de titres authentiques aux mauvaises personnes¹⁶. Il faudrait donc sécuriser l'acte d'état civil plutôt que la carte d'identité elle-même. C'est

¹³ D.Bigo, *Polices en réseau*, Presses de Sciences Po, 1996.

¹⁴ A.Ceyhan, "Comment prouver l'identité d'un individu?. La preuve par les technologies nouvelles", *Revue de la Gendarmerie Nationale*, Décembre 2005.

¹⁵ Quant aux autres pays européens, en Allemagne la fraude en identité concerne peu le passeport qui est considéré comme l'un des plus sûrs au monde, mais porterait plus sur le document d'identité. Il y aurait ainsi chaque année environ 70.000 délits de falsification de documents (faux en écriture). En Angleterre, le coût annuel de la fraude aux fausses identités (en particulier le passeport) serait de 2 milliards d'Euros. Face à l'ampleur de la fraude liée aux fausses identités le Home Office a décidé de se doter d'un service de lutte contre la fraude documentaire. Voir: Rapport d'information du Sénat sur la nouvelle génération de documents d'identité et la fraude documentaire, no 439 (2004-2005) de M. Jean-René Lecerf du 29 juin 2005, p. 18.

¹⁶ *Op.Cit.* p.57.

d'ailleurs ce qui ressort des recommandations de la Commission Internationale de l'Etat Civil (CIEC)¹⁷ reprise par le Conseil de l'Europe.

3 – L'émergence des identités multiples et virtuelles :

Les autorités publiques soulignent l'accroissement de l'utilisation des pseudonymes, des alias, d'identités virtuelles etc qui empêcheraient de procéder à une identification des individus avec certitude. Elles évoquent l'accroissement de l'usurpation de l'identité numérique (mot de passe, nom de compte informatique, codes donnant accès des données à caractère privé) passant par Internet ou par le piratage de lignes téléphoniques ou l'usurpation par téléphone.

Toutefois, il convient de remarquer que ce dernier type de délinquance n'est pas encore encadré par le droit français¹⁸. En effet, celui qui utilise une fausse identité dans un acte authentique ou un document administratif destiné à l'autorité publique est puni par l'article 433-19 du code pénal, ainsi que celui qui prend un faux nom pour se faire délivrer un extrait de casier judiciaire (article 781 du code pénal) tout comme celui qui prend l'identité d'un tiers dans le but de le faire passer pour un délinquant (article 434-23 du code pénal). Cependant celui qui s'empare d'un identifiant numérique sur Internet n'est pas poursuivi pour usurpation d'identité. Dans ce cas, les tribunaux invoquent le délit d'accès frauduleux à un système de données informatiques pour poursuivre le délinquant (article 323-1 et suivant du code pénal)¹⁹.

4 – Mise en place d'une carte service (carte multifonctions)

A l'instar du projet de la carte INES²⁰, les autorités veulent présenter la carte biométrique comme une carte de service pour des échanges dématérialisés. Ainsi, un segment de la puce sera réservé à un certificat d'authentification électronique qui permettra de sécuriser sur Internet des transactions commerciales ou des télé- procédures administratives. Un lecteur de carte à puce *ad hoc* branché à un ordinateur personnel permettra d'utiliser cette fonctionnalité. Au total, la carte INES sera constituée de trois fonctions : 1) fonction vérification et reconnaissance de l'identité (fonction classique); 2) fonction police judiciaire qui se mettrait en place grâce à la mise en place d'une base de données nationale des empreintes digitales, 3) fonction de service: accès aux différents services tels que l'authentification à distance, la signature électronique, la possibilité d'inscrire sur la carte des données personnelles à des fins d'échanges commerciaux ou de services.

Les autorités françaises ont récemment annoncé que la carte biométrique ne serait pas obligatoire. Toutefois, ces services annexes vont nécessairement créer un besoin de l'utiliser, car petit à petit elle deviendra indispensable pour procéder à des échanges non seulement entre personnes/entreprises privées mais surtout avec l'administration. Cette

¹⁷ Organisation intergouvernementale fondée à Amsterdam en 1948 qui facilite la coopération internationale en matière d'état civil.

¹⁸ A.Ceyhan, *Op.Cit.*

¹⁹ Une proposition de loi pour insérer au code pénal d'un article demandant de sanctionner par une année d'emprisonnement et de 15000 E d'amende, le fait d'usurper sur tout réseau informatique de communication l'identité d'un particulier, d'une entreprise ou d'une autorité publique a été déposée par le sénateur M. M. Dreyfus-Schmidt le 4 juillet 2005.

²⁰ Qui n'est pas encore définitif.

façon d'introduire la carte biométrique n'est pas propre à l'administration française. On retrouve le même type d'argumentaire tactique utilisé par les Américains pour les passeports biométriques (« ce n'est pas obligatoire, mais si vous voulez vous rendre aux Etats-Unis, il vous en faut un ») et le permis de conduire, qui par l'adoption du Real ID Act²¹ est devenu une carte d'identité de facto aux Etats-Unis (ce n'est pas obligatoire, mais si vous voulez prendre un avion, il vous en faut un)²².

III - Sur le plan de l'analyse quelles sont les différentes approches proposées pour appréhender ce processus ?

Globalement on rencontre trois types d'approches:

1° - **Une approche économique et sécuritaire** qui part du double postulat que la « technologisation » de l'identité résulte d'un besoin de rationalisation du processus d'identification ainsi que de la globalisation des technologies de pointe et qu'elle est devenue une nécessité pour faire face au risque global de terrorisme. Cette analyse comporte deux volets :

A - **Un volet purement économique**, qui inscrit la diffusion des technologies de sécurité dans une logique de rationalisation du processus d'identification afin de faire face à la fraude et de mettre au point des techniques « intelligentes » d'identification qui permettent d'identifier les individus en temps réel. Toutefois, cette analyse comporte un risque, celui de mener à une logique du « tout technologique ».

B - Un volet qui inscrit l'adoption des technologies biométriques comme une nécessité pour faire face au terrorisme, au crime organisé et à l'immigration clandestine. Plutôt que d'une analyse, il s'agit d'une rhétorique de justification mise en avant pour faire adopter la biométrie comme une nécessité pour faire face à une menace potentielle. Le risque d'une telle justification est de faire de la sécurité un méta - concept, un élément de rhétorique politique ou de marketing, mais pas d'analyse.

2 – Une approche sociologique

A- **Un volet libéral** qui établit une corrélation entre l'apparition de la carte d'identité et les droits sociaux dès la fin du XIX^e siècle²³. Selon ce courant, la libéralisation des sociétés et le développement des droits sociaux a donné lieu à un besoin d'identification des individus, notamment pour savoir qui a droit ou pas à l'attribution des droits sociaux. Ce courant examine le lien entre l'élargissement de la gamme des droits sociaux et la vérification de l'identité des personnes. Une variante de ce courant plus centrée sur l'étude de la crise du *Welfare state* prend en compte le développement des actes de fraude et la nécessité de faire des économies pour faire face à l'augmentation des dépenses de protection pour justifier l'exigence accrue de vérification des personnes. Le problème avec ce type d'analyse c'est qu'à l'extrême, il risque de tomber dans un

²¹ Cette loi prévoit la numérisation des bases de données du DMV (Department of Motorised Vehicules - organisme qui émet les permis de conduire) et leur accessibilité par chaque Etat. En d'autres termes, les Etats qui jusqu'à maintenant avaient leurs propres bases de données doivent les conformer à une norme commune afin que leurs données soient accessibles par les autres Etats.

²² A.Ceyhan, *Op.Cit.*

²³ Voir l'audition de M.Gauchet par la CNIL, le 24 février 2005.

conservatisme moral et de justifier la mise en place des critères d'exclusion d'un certain nombre de personnes du bénéfice des droits sociaux en raison de leur nationalité, statut d'immigration ou statut de travail et de résidence²⁴.

B- Un volet sociologique qui étudie l'irruption de la technologie dans tous les aspects de la vie par le développement d'une société de réseaux. Développé en particulier par Manuel Castells²⁵, ce type d'analyse examine les conditions sociales, économiques, politiques et internationales d'un « paradigme de technologie » qui mène à l'intégration des modes de communication et d'information dans un réseau interactif. Le mérite d'une telle analyse est d'examiner l'introduction des technologies de pointe dans la vie de tous les jours (effet de diffusion) par les dynamiques de la globalisation telle que la mise en réseau, l'interconnectivité, la flexibilité et de soulever les problèmes liés à leur sécurisation.

3 - A l'opposé une analyse critique en termes de « Big Brother ».

Globalement cette analyse affirme que la « technologisation » de l'identité s'inscrit dans la logique de la constitution d'un « Big Brother » sous la direction des Etats-Unis et de leur « allié contraint », l'Europe, et implique une sécurisation maximale faisant fi des droits fondamentaux. Si cette analyse paraît tentante pour critiquer la politique des Etats-Unis, elle est imparfaite pour deux raisons. D'abord, parce qu'elle considère la sécurité comme un concept figé qui ne porte que sur les peurs et la défense contre les menaces, sans pour autant examiner ses différentes composantes comme la sûreté, la sécurité économique et la protection qui s'inscrivent dans une logique plus contextuelle, dynamique et relationnelle et non-répressive. Ce faisant, elle reproduit le même type de discours qu'elle critique, c'est à dire un discours anxigène basé sur des peurs (peur du tout sécuritaire). Ensuite, parce que cette démarche accepte la métaphore du « Big Brother » sans examiner si ce système est bien celui qui se met en place à travers les mesures de sécurité adoptées actuellement. En fait, cette analyse se nourrit rarement d'une étude empirique sur le terrain qui lui permettrait d'observer l'élaboration de plusieurs systèmes de surveillance hétérogènes, combinant des méthodes privées, publiques et transnationales.

Ce qui se met en place correspond plus de la société de contrôle de Deleuze²⁶ qui s'établit par un processus « rhizomique », qu'à une reproduction limitée de Surveiller et punir de Foucault : la mise en place d'un panoptique au niveau mondial²⁷. Par ailleurs, on ne peut dire que dans ce processus, il y a d'un côté l'Etat, de l'autre la société, mais qu'au sein même de la société il y a des intérêts contradictoires (par exemple une demande de technologies de sécurité des parents d'élèves pour suivre l'itinéraire de leurs enfants). En matière de surveillance on assiste plutôt à la mise en place d'un assemblage de surveillances²⁸ ayant ses propres logiques et dynamiques, mis en place par des acteurs

²⁴ Voir les critiques de K.Calavita sur le « conservatisme de budget équilibré » comme conséquence de ce type d'analyse : « Balanced-Budget Conservatism and the Symbolism of Prop.187 », *Social Problems*, 43,3, 1996. Sur le risque d'exclusion sociale par identification des bénéficiaires des droits sociaux, voir : A.Ceyhan, « Etats-Unis, frontière sécurisée, identité(s) contrôlé(e)s », *Cultures&Conflicts*, nos 26/27, 1997.

²⁵ M. Castells, *La Société en réseau*, Paris, Fayard, 1997.

²⁶ G.Deleuze, *Pourparlers*, Paris, Editions de Minuit, 1990, pp: 229-240.

²⁷ Voir A.Ceyhan, Sécurité, frontières et surveillance aux Etats-Unis après le 11 septembre, *Cultures et Conflicts*, no; 53, 2004.

²⁸ Cette expression a été introduite par David Lyon, *Surveillance Society. Monitoring Everyday Life*, Buckingham, UK, Open University Press, 2001 et *Surveillance After September 11*, Oxford, Polity Press,

de sécurité et des acteurs non-sécuritaires (comme les entreprises de marketing ou de traitement des données).

IV - Une Piste d'analyse :

Il me semble qu'on pourrait analyser ce processus dans une problématique de « modernité liquide » et de la société du risque qui permettent d'expliquer la combinaison des logiques de confort et d' (in)sécurité²⁹.

Modernité liquide et incertitude

Inventée par Zygmunt Bauman, l'expression « modernité liquide » est employée pour représenter l'actuelle forme de la modernité qui se caractérise par la fluidité, la légèreté, le mouvement, le glissement et le non-respect des frontières traditionnelles³⁰. Elle correspond à ce qu'Ulrich Beck appelle la « seconde modernité ». Selon Beck, « nous sommes témoins oculaires –sujets et objets –d'une rupture survenue à l'intérieur d'une modernité qui s'émancipe des contours de la société industrielle classique pour adopter une forme nouvelle – que nous appellerons ici la société (industrielle) du risque ». « Au XIX^e siècle, la modernisation a détruit la société agraire prisonnière du système féodal pour esquisser la structure de la société industrielle ; aujourd'hui la modernisation efface les contours de la société industrielle et on voit apparaître dans la continuité de la modernité une configuration sociale tout autre »³¹. Il s'agit pour Beck du passage de la modernisation simple à la modernisation réflexive, c'est à dire à la modernisation qui s'en prend à elle-même, en d'autres termes aux prémisses et principes de fonctionnement de la société industrielle³². Cette déstabilisation de la société industrielle mène à des bouleversements dans toutes les sphères de la vie. « Le système de coordonnées dans lequel s'inscrivaient la vie et la pensée à l'ère de la modernité industrielle – les axes de la famille et de la profession, de la foi dans la science et progrès – se mettent à vaciller, et on voit apparaître une structure nouvelle et trouble faite d'opportunités et de risques... »³³

Cette structure nouvelle s'inscrit pour Bauman dans le passage de la « modernité solide » à la « modernité légère et liquide » où la société est organisée à l'image des microprocesseurs et des ordinateurs. Ainsi, plutôt que de grands systèmes économiques, politiques et organisationnels, ce sont de plus en plus des choix individuels et privés qui contribuent à rendre liquide la modernité et génèrent, comme le décrit Beck, des risques jusque-là inconnus ou inattendus. Bauman précise que « De nos jours, les modèles et les configurations ne sont pas donnés à l'avance, ni évidents. Ils sont juste très nombreux » et différents. En conséquence, on assiste à une situation d'hétérogénéité que l'on retrouve dans tous les aspects de la vie. Dans la vie de tous les jours elle transforme les catégories traditionnelles de sociabilité comme la famille, les amis ou la classe sociale,

2003, ainsi que par Kenneth Haggerty et Richard Ericson, "The Surveillant Assemblage", *British Journal of Sociology*, 51 (4), 2000.

²⁹ Voir le développement de cette problématique plus en détails dans A.Ceyhan, "La biométrie, une technologie pour gérer les incertitudes de la modernité contemporaine: applications américaines », *Cahiers de la Sécurité*, INHES, 2005.

³⁰ Z.Bauman, *Liquid Modernity*, London, Polity, 2000.

³¹ U.Beck, *La société du risque*, Paris, Albin Michel, 2001, pp. 20, 21.

³² Idem, p.28.

³³ Idem pp.30-31.

catégories que Beck appelle de « zombies »³⁴. Sur le plan international, cette hétérogénéité résulte de l'émergence de nouveaux acteurs privés en quête de pouvoir (diasporas, acteurs religieux ou économiques, groupes terroristes etc.) qui se caractérisent par la mise en réseau et le mouvement et qui poursuivent des logiques stratégiques propres.

Ces transformations produisent une nouvelle problématique de l'(in)sécurité qui, même si elle n'est perçue par les autorités politiques que dans une grille de lecture hobbesienne, prend en réalité des contours beaucoup plus différents. En fait il ne s'agit pas d'une insécurité générée uniquement par le terrorisme et la montée de la criminalité, mais d'une insécurité transversale qui traverse le spectre entier de la société, allant de la sphère de la vie privée à la géopolitique en passant par la sphère de l'emploi, la sphère de l'innovation et la sphère politique. Ce type d'insécurité est généré par l'incertitude, la perte des repères, le doute et l'affaiblissement de la sécurité ontologique. C'est une insécurité qui porte sur les références qui étaient devenues des routines. Au fond, on dira qu'il ne s'agit pas d'une problématique de sécurité au sens réaliste du terme, mais d'une problématique de l'incertitude qui se dégage à travers ce processus.

Le concept de sécurité ontologique a été développé par Anthony Giddens à la suite des travaux d'Eric Ericson. La sécurité ontologique est la confiance en l'attitude du monde et de soi qui s'ancre dans la durée de la vie quotidienne : c'est la confiance que les mondes naturel et social sont tels qu'ils paraissent être, y compris les paramètres existentiels de base de soi et de l'identité sociale. Elle est assurée de manière plus fondamentale par la prévisibilité des routines, malgré les situations critiques qui perturbent cette dernière d'une façon radicale³⁵. L'insécurité en tant que manque de confiance, de certitude, est un phénomène de la modernité contemporaine. Elle résulte de la transformation des relations sociales et intimes qui sont devenues des relations de compétition, de l'égoïsme, de « careerself ». Bauman caractérise les relations sociales contemporaines par leur focalisation sur la connectivité « au lieu d'entrer en relation, nous apprenons à nous connecter » dit-il³⁶. La modernité liquide crée une incertitude dans la sphère de l'individu et de la famille, la sphère du social (emploi, crime), la sphère de la nature (technologie, l'environnement). La solution est recherchée dans la communauté (repli sur soi et ses semblables) et la focalisation sur le corps comme objet de soins et de protection : « Le corps et la communauté sont les dernières lignes de défense dans un front de guerre pour la certitude, la sécurité et la sûreté... »³⁷. L'importance attribuée au corps reflète la volonté de remodeler l'image de la société (la communauté) à la lumière de la certitude.

C'est dans cette grille d'intelligibilité que l'on peut examiner la transformation du corps en une preuve d'identité et une source d'information.

Le corps comme preuve d'identité et source d'information

Afin de retrouver de la certitude perdue dans le monde de la modernité liquide, le corps devient l'élément focal d'identification. En se fondant sur le « bios », la biométrie ne fait que contribuer à cette quête de certitude perdue. Ainsi, en réduisant les empreintes des parties inchangeables du corps à des codes numériques, la biométrie construit le corps en même temps comme source de certitude et comme flux d'information. Il ne s'agit pas

³⁴ U.Beck, *Op.Cit.*

³⁵ A. Giddens, *La constitution de la société*, Paris, PUF, 1987, p.99.

³⁶ Z.Bauman *Liquid Love*, Polity, 2003

³⁷ Z.Bauman, *Liquid Modernity*, *Op.Cit.*, p.184

de la représentation du corps anatomique et médicalisé du XIX^e siècle, mais du corps comme information qui se transforme en donnée numérique.

Le corps devient signe d'unicité, mais elle est dématérialisée. C'est dans ce processus qu'on assistera à la dé-symbolisation de la carte d'identité : l'identité ne s'établit plus par une nomination par la puissance publique, mais se reconnaît sur le corps transformé en un code numérique³⁸. Un autre problème provient de l'utilisation du « bios » comme le lieu du marquage de l'illégalité (la biométrie permettant d'identifier les demandeurs d'asile, les illégaux, les criminels récidivistes) et étendue aux citoyens. Même si la police vérifie les identités pour s'assurer que les « bons citoyens » ne figurent pas sur les fichiers des criminels et des indésirables, c'est le corps qui constituera la mesure de la légalité ou de l'illégalité.

La primauté de l'information comme outil tactique et stratégique de premier ordre.

Parallèlement à la focalisation sur le corps, la modernité liquide fait de l'information une matière brute facilement transmissible, échangeable et manipulable qui constitue l'outil tactique et stratégique de premier ordre. L'enregistrement des données concernant la vie privée et publique des individus dans des bases de données participe au processus de fabrication de l'information qui s'opère via la manipulation de ces données par des acteurs publics et privés nationaux ou transnationaux. C'est ce processus qui permet d'identifier les individus. La question est de savoir comment l'information est obtenue, par qui et dans quelles conditions, comment prouver sa véracité et comment protéger les individus contre l'extraction des informations qui les concernent, mais qui s'opère à leur insu ? Comment est-ce qu'on passe de l'information à une donnée ? Qui est autorisé à le faire, à le manipuler et à l'échanger ? Comment contrôler la transformation de l'information en une donnée numérique et son inclusion dans des bases de données ?

La question des bases de données³⁹

Dans la modernité liquide, les « technologies de sécurité » comme la biométrie, doivent alors servir au « traitement de l'aléatoire »⁴⁰ par la mise en œuvre de méthodes plus appropriées d'identification, de localisation, de suivi et de surveillance. Avec le déploiement de logiciels spécifiques, les bases de données permettent l'élaboration de profils de comportement à risque ou dangereux. Ainsi, se développent des procédés d'estimation des risques qui sont au cœur des technologies d'anticipation et de prévention des risques. On retrouve ici l'analyse de Foucault sur les technologies de sécurité, lesquelles reposent, selon lui, sur des statistiques, des mises en série d'évènements probables, des recoupements, des comparaisons, des calculs du coût, etc. qui répondent au problème du traitement de l'aléatoire⁴¹. Pour réaliser ces opérations, la biométrie est liée à une ou plusieurs bases de données qui créent une association entre l'individu et les données via le recueil, le stockage et l'analyse des informations qui le concernent. Il convient de remarquer que le risque est ici de recouper ces informations avec d'autres dont on ne connaît pas bien la véracité et l'origine. A l'instar des Etats-Unis, où les pouvoirs publics sollicitent souvent la contribution des organismes privés pour participer à

³⁸ Audition d'A. Garapon par la CNIL, le 14 avril 2005.

³⁹ Pour plus de détails voir : A.Ceyhan, « La biométrie: une technologie pour gérer les incertitudes de la modernité contemporaine: applications américaines », *Op.Cit.*

⁴⁰ M. Foucault, *Sécurité, territoire population, Cours au Collège de France, 1977 –1978*, Paris, Gallimard. /Seuil, 2004, p.13.

⁴¹ Idem pp.8-10.

l'identification des personnes, on peut voir des organismes privés créer, disséminer, vendre, échanger etc des informations concernant les individus, ce qui confère à l'individu une identité prédéterminée par des données dont il n'a pas connaissance. On peut dire par-là que la biométrie fragilise les fondements traditionnels de l'identité comme *ipse* en la définissant à partir de données et de codes qui la dématérialisent.

Par exemple selon la dernière mouture de son projet, la carte INES intégrera deux ensembles de données : celles déjà présentes sur les cartes actuelles (nom, date de naissance etc) et les identifiants biométriques, à savoir deux empreintes digitales numérisées (a priori l'index des deux mains). Ces données seront stockées dans la puce intégrée à la carte et centralisées dans deux bases de données distinctes. L'accès à la base de données, dit-on au Ministère de l'Intérieur, se fera avec l'autorisation du juge⁴². Il convient de noter que le volet identification sera accessible par la police nationale et par les polices d'une trentaine de pays partenaires

Par la collecte, le stockage, le traitement et l'échange des données concernant les individus, la biométrie soulève la problématique du respect de la vie privée. Celle-ci devient plus inquiétante avec la collecte des données sur de longues périodes et leur possible échange entre agences publiques et privées sans que la personne ne s'en aperçoive et sans qu'un contrôle réel ne soit prévu.

L'impact sur l'identité

L'objectif visant à créer des documents d'identité qui intègrent des identifiants biométriques attestant de l'unicité de la personne soulève la question de la construction de l'identité par la technologie. Celle-ci mène à une conception particulière de l'identité : elle doit être fixe, donnée à l'avance et valable pour toujours. Plutôt que de déterminer une identité préexistante au processus d'identification, la biométrie assigne une identité fixe à une personne. Cette identité unique, essentialiste et déterminée à partir d'identifiants génétiques, biologiques ou morphologiques s'oppose à l'idée d'une identité multiple déclinable différemment en fonction des espaces et des contextes. Cela soulève un certain nombre de problèmes comme l'affaiblissement de la confiance en la parole de l'autre et en l'interaction sociale. La société n'aura plus de rôle à jouer dans le processus d'identification : l'identification d'un individu par l'intermédiaire d'un tiers semble être amenée à disparaître.

On pourrait poser ici la question de savoir comment les individus appréhendent la construction de leur identité par la biométrie ?

On peut dire que les réactions sont multiples⁴³ : si certains ne craignent pas de voir leur identité définie par le « bios », d'autres estiment qu'il y a là une atteinte à leur droit à l'anonymat et à leur dignité. Cette différence est représentative des revendications en matière d'identité qui se sont produites depuis une vingtaine d'années. En effet, il y a à la fois un désir de conserver des identités anonymes dans l'espace public et une revendication politique de reconnaissance des différentes identités qu'elles soient sexuelles, ethniques, linguistiques ou culturelles (le multiculturalisme).

⁴² "L'identité biométrique à la française", *Le Monde*, 29 décembre 2005.

Cependant identifier les individus par les parties du corps entre en contradiction avec la construction contemporaine des identités dans le Net qui devient de plus en plus virtuelle et imaginaire. L'identité est une représentation sans référence au corps dans les on-line constructions, les blogs comme My Space, IM, Social Networking, Facebook etc. Dans ce monde du virtuel, les individus entrent en interaction entre eux à travers des identifiants qui sont imaginés plutôt que totalement réels.

La dématérialisation de l'identité par la biométrie ne permet pas de voyager dans le monde virtuel de l'Internet et de se connecter aux autres à travers des identifiants inventés, car l'objectif même de la nouvelle technique d'identification est de faire face à des identités multiples et virtuelles. On peut à cet égard donner l'exemple de la signature électronique conçue pour sécuriser les échanges sur Internet en identifiant avec certitude les auteurs des échanges électroniques et en garantissant l'authenticité des actes.

Les limites juridiques :

L'utilisation de la biométrie atteint également des limites juridiques. Comme le rappelle Christian Cabal dans son rapport rendu à l'Assemblée Nationale⁴⁴, encadrée à ce jour par la loi Informatique et Libertés, la biométrie n'a pas de cadre juridique suffisant. Soutenu par de nombreux chefs d'entreprises, le rapport Cabal recommande un encadrement juridique spécifique pour ces technologies et la création d'un organisme chargé de leur normalisation.

Quant au niveau européen, il convient de rappeler que l'UE a choisi le recours à la biométrie pour les visas et pour les passeports des ressortissants européens, selon des normes OACI, ainsi que pour ses grandes bases de données (SIS I, SIS II – EURODAC – VIS). Ces choix sont repris par les Etats membres, y compris aujourd'hui par le Royaume-Uni non seulement en matière de passeports mais aussi en matière de document d'identité⁴⁵.

En ce qui concerne la question de la protection de la vie privée et des données personnelles, même si l'Europe est plus avancée que les Etats-Unis grâce à la directive du 24 octobre 1995, cette question est loin d'être réglée car elle se heurte au dilemme « sécurité & protection de la vie privée » et à la raison d'Etat. Malgré l'objectif de « protection équivalente » mis en place par la directive de 1995, il n'existe pas de cadre juridique homogène dans tous les pays, en raison de la multiplicité et de la diversité des technologies.

La biométrie soulève des questions quant à la protection des droits fondamentaux et à la liberté de circulation. Elle crée de multiples risques en termes de libertés puisque aucun contrôle ne s'exercera sur, par exemple, des fichiers « clandestins » qui se prolifèrent à une grande vitesse et dans le cadre de la coopération policière européenne (Europol).

⁴⁴ Christian Cabal, *Méthodes scientifiques d'identification des personnes à partir des données biométriques et les techniques de mise en œuvre*, Office parlementaire d'évaluation des choix scientifiques et techniques, Rapport no. 938, 16 juin 2003

⁴⁵ Règlement CE no 2252 du Conseil européen du 1^{er} décembre 2004 établissant les normes pour les éléments de sécurité et les éléments biométriques intégrés dans les passeports et les documents de voyage délivrés par les Etats membres. Lors du sommet du G5 d'Evian des 4 et 5 juillet 2005, les ministres de l'Intérieur français, britannique, espagnol, italien et allemand ont décidé d'œuvrer en faveur de la délivrance des cartes d'identité électroniques compatibles et inter opérables, et aussi de l'extension de la biométrie à tous les documents d'identification ?

Que faire ?

Il semble difficile d'envisager une résistance collective dans le contexte actuel, en particulier en raison de l'effet de diffusion de la technologie dans la vie de tous les jours. En effet, la logique de confort permet d'intégrer les microprocesseurs dans les objets de la vie quotidienne et de permettre à ces objets de communiquer entre eux et avec l'utilisateur. Ce qui facilite l'introduction dans la vie de tous les jours des technologies qui sont a priori des techniques policières comme les empreintes digitales (dans les ordinateurs, les voitures, les habitations). De ce fait, une résistance individuelle ne semble pas non plus avoir d'impact sur le plan collectif, elle risque d'isoler les citoyens et de rendre impraticable leur vie de tous les jours.

Dans ce contexte, on pourrait envisager une résistance par le droit en développant un droit de protection de l'information portant sur les individus à la manière de la protection du droit à l'image qui est très sévèrement encadrée en France. Il s'agira de développer un droit de la protection de la circulation de l'information donnant aux individus un droit exclusif de contrôle des informations qui sont produites à leur égard par des organismes privés et publics, circulant à la fois sur le net et stockées dans les bases de données sous forme de données personnelles. Au niveau européen, la protection des données personnelles est une réelle préoccupation, toutefois elle est juridiquement devenue très sophistiquée, sans toutefois être effective. Des modifications et une plate-forme de réflexion doivent être mises en œuvre rapidement pour protéger les informations concernant les individus, compte tenu des enjeux actuels liés aux décisions européennes et nationales de recourir de manière prioritaire à la biométrie pour identifier les individus.