Biometrie et antiterrorisme

Un enjeu global

Mémoire de géopolitique
du capitaine Frédéric ETTORI
dans le cadre du séminaire « Géopolitique du terrorisme »

Directeur : monsieur François GERE

Mars 2007

FICHE DOCUMENTAIRE

1 Biométrie et antiterrorisme : un enjeu global

2 2007_memoire_geop_biométrie et antiterrorisme_ETTORI

3 Capitaine, armée de Terre, ETTORI Frédéric, France

4 6 mars 2007

5 Division 6 – groupe A6

6 Mémoire de géopolitique

7 L'utilisation des technologies biométriques pour le contrôle des flux de population apporte des solutions aux problèmes posés par le terrorisme international. Cependant, ces technologies, loin d'être arrivées à maturité, présentent des faiblesses importantes susceptibles d'être exploitées non seulement par les terroristes, mais aussi par divers sortes d'escrocs. La menace terroriste, réelle ou supposée, sur les sociétés occidentales légitime la mise en place accélérée de dispostifs basés sur la biométrie. Cette situation a des effets notables sur les libertés individuelles. En Europe, il se crée un écart grandissant entre les droits théoriquement garantis aux citoyens et leur réalité sous la pression conjugée des Etats-Unis, de l'Union européenne et des gouvernements. Le saut technologique entrainé par l'association des technologies biométriques et des nouvelles technologies de l'information et de la communication constitue un véritable défi pour les sociétés démocratiques.

8 Terrorisme, Biométrie, Union européen, Etats-Unis, démocratie

Biométrie et antiterrorisme : Un enjeu global

SOMMAIRE

:

I. Des technologies immatures aux applications multiples

La biométrie : entre mythe et réalité

La biométrie dans la lutte contre la criminalité et le terrorisme

II Un cadre légal en construction

Une Union européenne frappée de schizophrénie

Des enjeux de puissance économique et géopolitique

III La mise en place de la biométrie : un piège pour la démocratie ?

Quel prix à payer pour des systèmes biométriques efficaces ?

La géopolitique est-elle modifiée par le recours a biométrie dans la lutte antiterroriste?

INTRODUCTION

Les événements du 11 septembre 2001 ont changé la perception de la menace terroriste[1] en matière de sécurité, que ce soit à l'échelle nationale ou internationale. Parce qu'ils estiment essentiel de le faire ou sous la pression des États-Unis – notamment dans le contrôle des voyageurs –, les gouvernements nationaux sont appelés à revoir comment s'exerce la sécurité sur leur territoire et quelles sont les mesures mises en place (ou à mettre en place) pour faire face au terrorisme. Outre le terrorisme, les États doivent également contrer la criminalité sur leur territoire, notamment en ce qui a trait au vol d'identité à des fins de consommation et à l'usurpation d'identité dans l'obtention de services gouvernementaux offerts aux citoyens résidents. L'application de technologies nouvelles dans l'implantation de moyens de surveillance des personnes et de contrôle de l'identité constitue l'essence des nouvelles approches gouvernementales. Ces technologies nouvelles, souvent intrusives – sur le plan du consentement, de la vie privée et de l'intégrité corporelle – reposent majoritairement sur la collecte et le stockage d'informations personnelles

[1] Acte terroriste : Tout acte qui vise à tuer ou à blesser grièvement des civils ou des non-combattants, et qui, du fait de sa nature ou du contexte dans lequel il est commis, doit avoir pour effet d'intimider une population ou de contraindre un gouvernement ou une organisation internationale à agir ou à renoncer à agir d'une façon quelconque. *La France face au terrorisme*, Paris ; La documentation française, 2006, p. 6

et l'utilisation de données biométriques[2]. C'est ce contexte d'une intensification des mesures de contrôle et de la disponibilité croissante de systèmes biométriques de toutes sortes pour établir ou valider l'identité d'une personne qui conduit à s'interroger sur les enjeux éthiques associés à une telle situation.

Le saut technologique est franchi directement par les pays en développement attirés par les économies possibles par la mise en place directes de bases de données numériques. La conséquence mécanique de cette évolution couplée avec les possibilités offertes par les technologies biométriques grâce à la mise en place de bases de données uniques et centralisées aux applications mal définies par la loi. Cette situation est aggravée par des dispositifs de protection des droits de l'homme et des libertés individuelles souvent défaillants et des contre pouvoirs parfois inexistants. Une analyse trop rapide pourrait laisser penser que ces dérives de pays « non-occidentaux » ne sont susceptibles de provoquer, au mieux qu'une modeste réprobation diplomatique, au pire quelques lignes dans les parutions des associations de défense des droits de l'homme et quelles n'ont aucune conséquence pour nos sociétés. Mais, alors que nos pays occidentaux sont normalement bien armés pour protéger les libertés fondamentales des citoyens la conjonction de plusieurs phénomènes jette un éclairage lugubre sur l'avenir. Le terroriste devient un alibi facile pour mettre en place un contrôle « moderne » des populations non seulement lors des franchissements de frontières mais aussi dans la vie courante. L'amélioration des technologies de la communication et du stockage des données, leur faible coût (en comparaison de la mise en place d'un système de fichage papier), la relative facilité d'enrôlement des personnes, offrent de nouvelles perspectives aux dirigeants peu scrupuleux ou soumis à de fortes pressions diplomatiques et commerciales.

Pour comprendre le rôle de la menace terroriste dans ce phénomène, il faut s'attarder sur la notion de sécurité. La définition sociétale de la sécurité ferait référence à trois éléments : la préservation des valeurs fondamentales, l'absence de menace, la formulation de mesures sociopolitiques visant à faire face à des mesures éventuelles. Ainsi, le concept de sécurité est nécessairement lié à celui de danger :

[2] Les technologies et les réglementations évoluent à une telle vitesse qu'il est difficiles de trouver des documents imprimés à jour. Il a donc été choisi de s'appuyer sur Internet, presque toutes les références sont directement accessibles sur le Net.

c'est parce qu'il y a un sentiment de danger face aux trois fondements de la sécurité que des mesures sécuritaires sont mises en place[3] .

Une menace peut-être réelle ou perçue, elle peut aussi avoir des effets directs (destructions ou morts) ou indirecte (mise en place de mesures sécuritaires). En effet, puisque ce sont certaines élites politiques – souvent des spécialistes de la sécurité – qui décident des éléments devant être considérés comme des enjeux sécuritaires et que les menaces sont fréquemment perçues, – pas simplement réelles ou objectives – la sécurisation est un processus qui, bien souvent, est très subjectif. La sécurisation, c'est-à-dire la construction sécuritaire, passe donc nécessairement par un biais de valeurs et d'intérêts d'une élite dominante. Ainsi, la sécurité apparaît à la fois comme un bien à atteindre, un bien indispensable à la vie, mais aussi comme une stratégie mise en œuvre pour que la sûreté soit acquise. Or cette stratégie, soit la sécurisation, suppose toujours des pouvoirs de contrôle qui renvoient à un ou à des enjeux politiques qui sont liés à des perceptions de l'environnement sécuritaire. En prétendant protéger, l'État en vient aussi à contrôler même au-delà du nécessaire. Ce contrôle, présenté comme une réponse à une demande d'accroissement sécuritaire, engendre donc un conflit permanent entre la quête de sécurité de l'individu qui demande au groupe d'assurer sa protection par tous les moyens et sa quête de liberté individuelle.

L'étude démontrera que, si les besoins de la lutte antiterroriste ne sont objectivement qu'une justification secondaire à ce mouvement, c'est la conjonction du besoin de sécurité des populations, des tentations sécuritaires des Etats et le fantastique développement des techniques qui crée une dynamique nouvelle aux conséquences encore mal identifiées. Ainsi, sous couvert de sécurité, la biométrie est devenue un enjeu de puissance et d'influence sur l'échiquier international. Les réglementations et les systèmes mis en place auront des conséquences sociales et éthiques au niveau mondial.

[3] DAVID, Charles-Philippe, La guerre et la paix : approches contemporaines de la sécurité et de la stratégie, Paris ; Presses de science po, 2000, p. 31.

Afin de comprendre les enjeux de la biométrie dans la lutte antiterroriste, il est nécessaire de saisir les principes fondamentaux qui régissent l'emploi de ces techniques. Dans un second temps, une mise en perspective des contradictions entre les législations en place et les mises en application des systèmes en démontreront l'influence profonde sur les gouvernements. Ensuite, il conviendra d'étudier d'une manière plus générale la modification de la notion de frontière et l'évolution vers un état d'urgence permanent des sociétés occidentales.

1 Des technologies immatures aux applications multiples

Bien que les technologies biométriques n'aient pas atteint leur maturité, sous la pression de multiples facteurs, elles sont d'ors et déjà mises en œuvre par de nombreux Etats dans le cadre de la lutte contre la criminalité en général et de la lutte anti-terroriste en particulier. Il existe, actuellement, autour de la biométrie un flou propice aux plus extravagantes promesses des industriels, tentations écuritaires des Etats et aux angoisses des sociétés civiles.

Il apparaît donc indispensable de rappeler quelques données fondamentales sur les technologies biométriques, puis d'étudier des exemples d'applications et de dérives actuelles.

1.1 La biométrie : entre mythe et réalités

Le contrôle des flux, qu'ils soient humains ou financiers, est un des défis majeurs que doivent relever les Etats dans la lutte contre le terrorisme international. Il implique de s'assurer de l'identité des individus. La biométrie offre, a priori, des réponses à ces défis :

- D'une part, elle est, théoriquement, universelle et immuable, chaque être humain pouvant être identifié quelle que soit sa culture et quel que soit son âge ;

- D'autre part, elle garantit l'unicité de la personne en établissant un lien unique entre la donnée biométrique et son porteur. La robustesse de ce lien peut résister, à certaines conditions, à la comparaison de plusieurs centaines de millions d'individus entre eux ;
- Surtout, les progrès de l'informatique ouvrent de nouvelles possibilités pour son utilisation[4].

1.1.1 Généralités sur la biométrie

La biométrie est, au sens étymologique, l'application de méthodes statistiques pour mesurer un objet biologique. Appliquée à l'homme, elle constitue l'anthropométrie. Toutefois, par un abus de langage, la biométrie désigne l'ensemble des technologies de reconnaissance physique ou biologique des individus. Chaque être humain se distingue de ses « semblables » par un ensemble de caractéristiques morphologiques et biologiques qui rendent son identification possible. Ainsi les caractéristiques collectées doivent être **universelles** (exister chez tous les individus), **uniques** (permettre de différencier un individu par rapport à un autre), **permanentes** (autoriser l'évolution dans le temps), **enregistrables** (collecter les caractéristiques d'un individu avec l'accord de celui-ci) et **mesurables** (autoriser une comparaison future)[5].

Les données biométriques sont de plusieurs types, chacune présentant des avantages et des inconvénients en fonction de l'usage qui en est fait. Les principales sont la morphologie du visage, les empreintes digitales ou palmaires, la forme de la main, la reconnaissance de l'iris et les empreintes génétiques. **Les techniques actuelles reposent sur deux types de contrôles** : Le contrôle physique et le contrôle comportemental de la personne.

---

[4] Jean-René LECERF. *Identité intelligente et respect des libertés.* Rapport d'information du Sénat n° 439 (2004-2005). Disponible sur <http://www.senat.fr/rap/r04-439/r04-439.html> (consulté le 21/01/07).

[5] Frédéric MASCRE. *La biométrie comme méthode d'authentification : enjeux et risques*. Disponible sur <http://www.droit-informatique.com/index.htm> (consulté le 21/01/07).

Le contrôle physique s'appuie sur l'analyse des caractéristiques physiques uniques et infalsifiables d'un individu. La biométrie utilise pour l'instant six types de contrôle principaux :

- Les empreintes digitales : A partir du dessin représenté par les crêtes et les sillons de l'épiderme, la numérisation permet d'extraire des caractéristiques (les minuties) telles que les bifurcations de crêtes, les "îles" ou les lignes qui disparaissent. Une empreinte contient environ cent minuties, mais le relevé de douze points suffit pour effectuer un contrôle. Il est, en effet, statistiquement impossible de trouver deux individus présentant les mêmes douze points caractéristiques, même en considérant une population de plusieurs dizaines de millions de personnes.
- La reconnaissance de la main ou empreinte palmaire : la technique consiste à mesurer plusieurs caractéristiques de la main (jusqu'à quatre-vingt dix) telles que la forme générale, la longueur et la largeur des doigts, les formes des articulations ou les longueurs inter-articulations. Ce système présente un taux d'erreurs plus élevé que le précédent (jumeaux, effets de l'âge).
- La reconnaissance de l'iris : l'iris comporte un grand nombre de points caractéristiques qui ne varient pratiquement pas pendant la vie d'une personne.
- La reconnaissance rétinienne : elle se base sur le dessin formé par les vaisseaux sanguins de la rétine. Il est unique pour chaque individu, différent entre jumeaux et assez stable durant la vie de la personne.
- La reconnaissance faciale: il s'agit de réaliser une photographie permettant d'extraire un ensemble de facteurs qui se veulent propres à chaque individu. Ces facteurs sont choisis pour leur forte invariabilité et concernent des zones du visage tels que le haut des joues, ou les coins de la bouche.
- La configuration des veines : cette technique est habituellement combinée à une autre, comme l'étude de la géométrie de la main. Il s'agit ici d'analyser le dessin formé par le réseau des veines sur une partie du corps d'un individu pour en garder quelques points caractéristiques.

Le contrôle comportemental, à l'heure actuelle, trois pistes sont explorées :

- La dynamique des frappes au clavier : Analyse, qui peut être soit statique et basée sur des réseaux neuronaux, soit dynamique et statistique (comparaison continuelle entre l'échantillon et la référence) consistant à évaluer les durées entre les frappes, la fréquence des erreurs, la durée de la frappe elle-même...
- La reconnaissance vocale: Authentification reposant sur la tonalité de la voix de la personne contrôlée, la fréquence vocale et la distance entre la formation des lettres. Elle peut distinguer un homme d'une femme mais reste très dépendante de la qualité de l'enregistrement et du type de message.
- La dynamique du tracé des signatures : Peu utilisé, le procédé est habituellement combiné à une palette graphique munie d'un stylo. Ce dispositif va mesurer plusieurs caractéristiques lors de la signature, tels que la vitesse, la pression et les accélérations, le temps total de la signature.

Plusieurs autres techniques sont en cours de développement. Parmi celles-ci, on peut citer la biométrie basée sur la géométrie de l'oreille, le dessin des lèvres, la forme des pores de la peau, la démarche et les analyses de traces biologiques (odeurs du corps, ADN, salive, sang...).

Tous les systèmes biométriques fonctionnent en deux temps et comportent deux processus :

- l'enregistrement de l'utilisateur ;
- le contrôle de l'utilisateur.

Ces deux processus comprennent cinq étapes essentielles au bon déroulement de l'opération :

1. La saisie de l'information à analyser – lecture de certaines caractéristiques physiologiques, comportementales ou biologiques d'une personne, au moyen d'un terminal de capture biométrique (ou capteur biométrique);
2. Le traitement de l'information – la transformation de l'information en données numériques;

3. La création d'un fichier « signature » et son enregistrement – l'utilisation des données numériques pour créer un modèle ou gabarit qui représente la donnée biométrique captée, c'est-à-dire la signature qui sera conservée sur un support portable (puce ou autre) ou dans une base de données et utilisée à fin de comparaison;

4. La comparaison – les caractéristiques biométriques d'une personne soumise à contrôle (volontairement ou à son insu) sont comparées à la « signature » mémorisée;

5. La décision – l'opérateur du système ou le système informatisé détermine si l'identité de l'utilisateur correspond ou non à l'identité proclamée (authentification) ou recherchée (identification).

Le tableau 1 offre une récapitulation générale des caractéristiques des principales technologies biométriques.

Tableau 1. Tableau récapitulatif des technologies biométriques

Technologie biométrique	Fiabilité	Facilité d'emploi	Acceptation par l'utilisateur	Stabilité	Coût	Transparence[1]	Applications courantes	Convient aux comparaisons	
								1 : 1	1 : N
Reconnaissance de l'empreinte digitale	Élevée ou très élevée	Élevée	Moyenne à faible	Élevée	* à ***	Visible	Autorisation des voyageurs, permis de conduire, aide sociale	oui	oui
Géométrie de la main	Élevée	Élevée	Moyenne à élevée	Moyenne à élevée	***	Visible	Contrôle d'accès, autorisation des voyageurs, soins de jour	oui	non
Reconnaissance faciale	Moyenne à élevée[2]	Moyenne à élevée	Élevée	Moyenne à faible	***	Dissimulé	Casinos, autorisation des voyageurs	oui	potentielle-ment[3]
Reconnaissance de l'iris	Très élevée	Moyenne à faible	Moyenne à élevée	Élevée	*****	Dissimulé	Prisons, contrôle d'accès, autorisation des voyageurs	oui	oui
Reconnaissance de la rétine	Très élevée	Faible	Faible	Élevée	****	Visible	Contrôle d'accès, autorisation des voyageurs	oui	oui
Géométrie du doigt	Moyenne	Élevée	Moyenne à élevée	Moyenne à élevée	***	Visible	Contrôle d'accès, détenteurs de tickets d'entrée aux parcs d'attraction	oui	non
Reconnaissance vocale	Moyenne	Élevée	Élevée	Moyenne à faible	*	Dissimulé	Applications à basse sécurité, authentification par téléphone	oui	non
Vérification dynamique de la signature	Moyenne	Élevée	Moyenne à élevée	Moyenne à faible	**	Visible	Applications à basse sécurité, applications à signature existante	oui	non

Notes :
1. La transparence désigne la mesure dans laquelle un système peut être exploité à l'insu des personnes concernées. Les systèmes visibles ne peuvent prélever un échantillon biométrique à l'insu de la personne concernée, contrairement aux systèmes dissimulés.
2. La reconnaissance faciale pourrait théoriquement être fort exacte (comme le suggère l'essai récent de reconnaissance faciale mené dans des conditions contrôlées – *Facial Recognition Vendor Test*), mais des projets pilotes récents et des essais en conditions réelles ont fait apparaître des taux d'erreurs beaucoup plus élevés et montré qu'il était très difficile d'obtenir des résultats exacts avec ces systèmes.
3. Ibid.

Source : OCDE, Direction de la science, de la technologie et de l'industrie, comité de la politique de l'information, de l'informatique et des communications, *technologies fondées sur la biométrie (DSTI/ICCP/REG(2003)2/FINAL).* 15 juin 2005. p 40. Disponible sur http://appli1.oecd.org/olis/2003doc.nsf/43bb6130e5e86e5fc12569fa005d004c/d15c6d3ea769bc64c1256e84004c42fc/$FILE/JT00186151.PDF. Consulté le 28/12/2006

Pour le grand public, la mise en place de la biométrie semble offrir une solution imparable aux problèmes d'identification et d'authentification, d'autant plus que ses thuriféraires, soutenus par la mode des feuilletons télévisés vantant les exploits d'une police scientifiques toute puissante, évitent d'en révéler les faiblesses et les dérives possibles ou avérées.

En effet, les technologies biométriques sont loin d'être efficaces à 100% en dépit des caractéristiques uniques des données intrinsèques. Ainsi une étude de l'US National Institute of Standards and Technology (NIST) démontre que « la biométrie semble toujours plus facile et fiable en théorie qu'en pratique. Les relevés de données sont difficiles et il est beaucoup plus facile qu'il ne devrait l'être de tromper les systèmes »[6] . Quant à la gestion ultérieure des données recueillies, elle est l'objet de nombreuses interrogations car elle est bien évidemment tributaire des us et coutumes des Etats concernés.

1.1.2 Des technologies complexes non encore abouties ?

Il ne s'agit pas là fondamentalement de remettre en cause la fiabilité de la biométrie. Cependant il est nécessaire, comme l'a fait Christian Cabal, dans un rapport de juin 2003, de mettre en garde contre les excès de confiance à l'égard de la biométrie[7].

En Grande Bretagne, le processus qui doit conduire à la mise en place d'une carte d'identité contenant des données biométriques a provoqué un débat très vif qui a permis la réalisation de nombreuses études riches d'enseignements. En 2005, une des plus complète a été menée par le Service britannique des passeports (UKPS, UK passport Service) en partenariat avec le Programme du ministère de l'Intérieur sur les cartes d'identité (Home Office Identity Cards Programme) et l'Agence des permis de conduire et des cartes grises (DVLA, Driver and Vehicle Licensing

---

[6] JACKSON, William. *NIST identifies good and bad points of biometrics*. Disponible sur < http://www.gcn.com/print/21_25/19773-1.html >. (Consulté le 28/12/2006).

[7] CABAL, Christian (rapporteur). Rapport n°938 sur les méthodes scientifiques d'identification des personnes à partir de données biométriques et les techniques de mise en oeuvre, Office parlementaire d'évaluation des choix scientifiques et technologiques [en ligne]. Disponible sur < http://www.assemblee-nationale.fr/12/rap-off/i0938.asp> (Consulté le 28/12/2006).

Agency). Plus de dix mille personnes ont pris part à cette étude qui s'est déroulée d'avril à décembre 2004[8].

Les résultats obtenus montrent que la reconnaissance faciale ne réussit à reconnaître que 69% des personnes en bonne santé et seulement 48% des handicapés. Les empreintes n'identifient que 80% des personnes. Si la reconnaissance par l'image de l'iris obtient de meilleurs résultats (96%), l'enregistrement des données est beaucoup plus difficile. Si l'on imagine que 330 personnes en parfaite santé achètent un billet d'avion long courrier, la reconnaissance faciale en rejetterait 93, les empreintes 60 et l'iris 12, soit dans la pire occurrence statistique un rejet de 198 personnes. Il est à noter que le croisement de deux systèmes biométriques réduirait de manière très significative les erreurs.

Une étude sur le système d'identification par empreinte digitale mis en place aux Etats-Unis dans le programme « US-VISIT » montre que grâce à des procédés d'altération de l'empreinte digitale (abrasion, brulure, opération chirurgicale », les chances qu'un terroriste dont les empreintes sont stockées dans la base de données soit reconnu tombent de 96% à 53%[9]. Le système dit « IDENT » d'enregistrement sur lequel est basé le programme « US-VISIT » est actuellement basé sur la saisie de deux empreintes. Il pourrait être amélioré à concurrence de 95% de réussite par la saisie de la totalité des doigts, mais il provoquerait un allongement considérable des files d'attentes sur les points d'entrée sur le territoire et entrainerait des coûts prohibitifs[10].

Si la fiabilité des systèmes de reconnaissance biométriques est loin d'être optimale, les bases sur lesquelles sont stockées les données biométriques posent aussi des problèmes. Toute base de données centralisée constitue en effet une cible de choix pour les hackers comme le déclare la société Ubizen en charge du système

---

[8] UK PASSEPORT SERVICE, *Biometrics Enrolment Trial Report May 2005,* p. 55. Disponible sur < http://www.passport.gov.uk/downloads/UKPSBiometrics_Enrolment_Trial_Report.pdf > (consulté le 23/01/07).

[9] Lawrence M. WEIN, testimony at the hearing on "*Disrupting Terrorist Travel: Safeguarding America's Borders through Information Sharing*," US House of Representatives Select Committee on Homeland Security, September 30, 2004. Disponible sur < http://cisac.stanford.edu /publications/disrupting_terrorist_travel_safeguarding_americas_borders_through_information_sharing/ > Consulté le 23/01/2007).

[10] Rey KOLOWSKY. Real *challenges for virtual borders: The Implementation of US-VISIT*. Migration Policy Institute, juin 2005. Disponible sur < http://www.migrationpolicy.org/pubs/Koslowski_Report.pdf > (consulté le 23/01/2007).

supportant la nouvelle carte d'identité biométrique belge[11]. Comme les bases de données sont constituées de fichiers informatiques descriptifs ne contenant pas de références physiques[12], la probabilité de vol d'identité biométrique est réelle. Plusieurs vols massifs d'identité dans des centres de rétention de données montrent la faiblesse des moyens de protection. On peut penser aux affaires Lexis-Nexis[13] (Des informations sensibles portant sur plus de 300 000 personnes ont été volées), CardSystems[14] (A la suite d'une faille de sécurité, 40 millions de numéros cartes bancaires ont été piratés) ou ChoicePoint[15] (vol des données personnelles de 26,5 millions d'anciens combattants). Alors que l'aspect irrévocable de la source même d'information est un truisme (les empreintes digitales l'iris de l'œil ou l'ADN ne peuvent être changés pour raison de « vol d'identité »), rien n'interdit plus le « vol de preuve d'identité ». Car s'il est aisé, pour certains pirates, de subtiliser un lot de numéros de cartes de crédit, il est encore plus facile d'empocher un échantillon de salive, une trace de doigt ou le cliché discret d'un visage. Et il est presque simple d'imiter la signature physique de ces preuves d'identité, à grand renfort d'astuces chimiques ou de bricolages divers. M. Philippe Wolf, responsable du centre de formation de la direction centrale de la sécurité des systèmes d'information qui est placée sous l'autorité directe du Premier ministre, doute de la maturité des technologies biométriques et estime que la meilleure sécurité informatique reste l'utilisation d'un code secret révocable. Or, les données biométriques ne sont ni secrètes, ni révocables[16].

Lorsqu'elles sont stockées dans une mémoire centralisée et non pas sur un disque dur ou sur une micro-puce, les données biométriques « voyagent » et peuvent être couplées avec des données présentes dans d'autres bases de données ayant en mémoire d'autres types d'information sur les mêmes personnes, permettant ainsi de

---

[11] Andy MAC CUE, *UK faces massive ID card challenges*, 01/12/2003. Disponible sur < http://management.silicon.com/government/0,39024677,39117139,00.htm > (Consulté le 28/12/2006).

[12] C'est-à-dire qu'il n'y a pas de support physique à partir duquel il serait possible de comparer en cas d'usurpation d'identité les éléments biométriques réels du plaignant

[13] Philippe GUERRIER, *LexisNexis craint un vol massif de données confidentielles.* Disponible sur < http://www.vnunet.fr/fr/vnunet/news/2005/04/12/lexisnexis-craint-vol-massif-donnees-confidentielles > (Consulté le 28/12/2006).

[14] Hélène PUEL. *Des milliers de Français victimes du vol de leur numéro de carte bancaire 21/06/2005.* Disponible sur <http://www.01net.com/article/282062.html. > (Consulté le 28/12/2006)

[15] Ludovic TICHIT. *Le vol d'identités toujours aussi critique aux Etat 24/05/2006.* Disponible sur < http://solutions.journaldunet.com/0605/060524-vol-basededonnees.shtml > (consulté le 28/12/2006)

[16] Philippe Wolf. *De l'authentification biométrique*, Sécurité Informatique, Octobre 2003 < http://www.cnrs.fr/Infosecu/num46.pdf > (consulté le 27/01/2007).

créer un profil de plus en plus complet d'une personne au fur et à mesure que les renseignements la concernant s'apparient. Plus l'information s'« enrichit » et plus la base de données s'élargit, plus s'excite la convoitise des pirates informatiques. Dans son rapport sur le programme US-VISIT, Rey Kolowsky, encourage le *Department of Homeland Security* à renforcer la sécurité des bases de données biométriques pour s'assurer qu'elles ne puissent être piratées. Il estime, en effet que le risque est sous-estimé[17]. La qualité des bases de données et leur mise à jour est un défi majeur de tout système biométrique. Il ne suffit pas de faire correspondre une identité biologique avec des éléments tels que l'identité, l'adresse ou le casier judiciaire, encore faut-il que les bases soient tenues à jour. Selon Charles Farrier en charge d'un rapport pour le Parlement britannique le dicton anglais « *Rubbish In, Rubbish Out* » reste de mise. Ainsi en 1999 un audit interne de la police londonienne montre que 84% des peines et amendes entrées dans les fichiers ne correspondent pas à la réalité[18].

1.2 La biométrie dans la lutte contre les diverses formes de criminalité

La technologie permet à peu près tout, comme l'a affirmé M. Bernard Didier, directeur du développement de la SAGEM[19]. Le panel proposé par les industriels offre une gamme très large de solutions techniques. Du point de vue de la sécurité, les questions essentielles, avant de créer un titre d'identité biométrique, sont : quel degré de sécurité veut-on atteindre ? Quel type de fraude faut-il éliminer ? Quels autres usages de la biométrie veut-on permettre ou ne pas permettre ? Quelle est la taille de la population concernée ? En fonction des réponses apportées à ces

[17] Rey KOLOWSKY, op. cit.
[18] Charles FARRIER. House of commons, Home Affairs Committee Publications session 2003-2004. *Government proposals for identity card scheme*. Disponible sur < http://www.parliament.the-stationery-office.com/pa/cm/cmhaff.htm> (consulté le 28/12/2006).
[19] Le Forum des droits sur l'Internet. *Contribution de Bernard Didier sur les aspects biométrie.* Disponible sur http://www.foruminternet.org/forums/read.php?f=16&i=3106&t=3106 (consulté le 27/01/07).

questions, il est possible de construire un système d'identité biométrique dont l'architecture réponde précisément au cahier des charges.

L'usurpation d'identité est un des défis majeurs, la mise en place de la biométrie offre un panel de réponses qu'il est intéressant d'examiner. En effet, les systèmes sont différents qu'il s'agisse d'authentifier quelqu'un ou de l'identifier. Traditionnellement, un titre d'identité associe une photographie et un nom. Il permet au porteur du titre de prouver son identité**.** On parle alors d'**«** authentification. Trois solutions intégrant la biométrie permettent d'améliorer la qualité de l'authentification **:**

- Une carte à puce biométrique sans fichier central

Les données biométriques ne figurent que sur la puce. Cela permet un troisième niveau de sécurité en authentifiant le porteur par comparaison avec les données biométriques contenues dans la puce. Toutefois, cette utilisation de la biométrie ne permet pas d'assurer l'unicité de l'identité lors de la délivrance du titre**.**

- Une carte à puce biométrique avec un fichier central unidirectionnel dans le sens identité vers biométrie. Avec ce modèle**,** il est possible, à partir de l'identité d'une personne, de retrouver ses données biométriques. Toutefois, l'inverse n'est pas possible. Ainsi, la connaissance de l'identité d'une personne permet d'accéder à sa donnée biométrique et de procéder, si nécessaire, à son authentification. Par rapport au modèle précédent sans fichier, ce modèle présente un avantage majeur : l'unicité de l'identité est assurée à l'occasion de la délivrance du titre. En effet, si l'individu a un titre sous une autre identité, ses données biométriques auront déjà été enregistrées dans la base de données et le système s'en apercevra[20].

- Lorsqu'il s'agit d'identifier une personne, il apparait nécessaire de disposer d'un fichier central qu'il soit possible d'interroger dans le sens biométrie vers identité.

[20] Jean-René LECERF. Op. cit.

1.2.1 Un secteur en plein expansion aux applications multiples

D'ici 2015, plus d'un milliard de personnes pourraient faire partie d'une immense base de données mise en place à la demande de l'OACI[21] à des fins de reconnaissance faciale des voyageurs[22]. Il s'agit d'une situation qui préoccupe grandement des organismes comme Privacy International [23]et The American Civil Liberties Union[24] qui y voient, entre autres, un risque de développement beaucoup plus vaste encore d'une infrastructure de surveillance des déplacements des personnes et de compilation de données accessibles à tous gouvernements – y compris ceux qui sont reconnus pour bafouer les libertés civiles et les droits de la personne.

Dans l'espace Schengen, la prochaine version du système d'information Schengen[25], appelée SIS II, intègrera des données biométriques et en premier lieu des empreintes digitales[26] Près de 35 millions d'interrogations du SIS ont été faites en France en 2004. Ce projet est développé conjointement avec le projet VIS II[27]. Enfin, en vigueur depuis le 15 janvier 2003, **Eurodac**[28] est un système européen de contrôle et de comparaison des empreintes digitales des demandeurs d'asile et des étrangers susceptibles de le devenir un jour. Les Etats membres prennent en effet les

---

[21] Organisation de l'aviation civile internationale. Informations disponibles sur < http://www.icao.int/index_f.html> (consulté le 13/02/07).

[22] BBC NEWS, *Concern over biometric passports, 30 March 2004*. Disponible sur < http://news.bbc.co.uk/1/hi/technology/3582461.stm > (consulté le 17/01/07).

[23] Informations disponibles sur <http://www.privacyinternational.org > (Consulté le 12/01/07).

[24] Voir http://www.aclu.org/ (Consulté le 12/01/07).

[25] Le SIS est un système d'information qui permet aux autorités compétentes des États membres de l'Union européenne de disposer d'informations relatives à certaines catégories de personnes et d'objets. Information disponible sur < http://europa.eu/scadplus/leg/fr/lvb/l33183.htm > (Consulté le 23/01/07)

[26] Parlement européen et Conseil européen. *Règlement sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen de deuxième génération (SIS II)*. Disponible sur < http://eur-lex.europa.eu/LexUriServ/site/fr/com/2005/com2005_0236fr01.pdf > (Consulté le 19/02/01).

[27] Parlement européen et Conseil européen. *Règlement concernant le système d'information sur les visas (VIS) et l'échange de données entre les États membres sur les visas de court séjour*. Disponible sur <http://europa.eu.int/eur-lex/lex/LexUriServ/site/fr/com/2004/com2004_0835fr01.pdf > (Consulté le 18/02/07).

[28] Système de comparaison des empreintes digitales des demandeurs d'asile et des immigrants clandestins afin de faciliter l'application de la convention de Dublin qui permet de déterminer l'État responsable de l'examen d'une demande d'asile. Voir *Règlement (CE) nº 2725/2000 du Conseil du 11 décembre 2000 concernant la création du système «Eurodac» pour la comparaison des empreintes digitales aux fins de l'application efficace de la convention de Dublin.* Disponible sur < http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexplus!prod!DocNumber&lg=fr&type_doc=Regulation&an_doc=2000&nu_doc=2725> (Consulté le 18/02/2007).

empreintes digitales des étrangers de plus de quatorze ans ayant déposé une demande d'asile, franchi irrégulièrement une frontière de l'Union ou se trouvant illégalement sur le territoire de l'un des Etats membres. Il s'agit d'éviter qu'un demandeur d'asile ne présente des demandes multiples dans plusieurs Etats parties. Ce système prévu par le règlement (CE) n° 2725/2000 du Conseil du 11 décembre 2000 concernant la création du système « Eurodac » doit en effet permettre l'application efficace de la convention relative à la détermination de l'Etat responsable de l'examen d'une demande d'asile présentée dans l'un des Etats membres par un ressortissant d'un pays tiers signée à Dublin le 15 juin 1990 (dite « Convention de Dublin »). Cette convention a été récemment remplacée par le règlement (CE) n° 343/2003[29] du Conseil du 18 février 2003 dénommé « règlement Dublin II ».

1.2.2 Du fichier national automatisé des empreintes génétiques (FNAEG) et le projet INES

La mise en place des passeports biométriques dans lesquels est inclus une puce RFID[30]dits « Documents de Voyage à Lecture Automatique » soulève de nombreuses questions. C'est d'ailleurs aussi le cas de la future carte d'identité française (projet INES). Les vulnérabilités des tags RFID avaient déjà été au cœur des débats lors de la dernière conférence Black Hat[31]. En 2006, dans la déclaration dite de Budapest[32], qui fait désormais référence sur le sujet, des chercheurs sur l'identité et la gestion de l'identité (appuyés par un vote unanime lors de la réunion

---

[29] *Règlement (CE) n° 343/2003 du Conseil du 18 février 2003 établissant les critères et mécanismes de détermination de l'État membre responsable de l'examen d'une demande d'asile présentée dans l'un des États membres par un ressortissant d'un pays tiers.* Disponible sur <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32003R0343:FR:NOT> (Consulté le 17/02/07).

[30] Radio Frequency indentification technology, informations disponibles sur http://www.cite-sciences.fr/francais/ala_cite/science_actualites/sitesactu/question_actu.php?langue=fr&id_article=2803&id_mag=0 (consulté le 18/01/07).

[31] Black Hat est une société fondée en 1997 par Jeff Moss, réputée pour organiser un réseau de conférences fournissant des points de vue nouveaux et exclusifs sur la sécurité de l'information. Les Conférences Black Hat (ou *Black Hat Briefings*) sont un évènement unique qui rassemble officiellement des experts des agences gouvernementales américaines et des industries, américaines ou non, avec les hackers les plus respectés de l'« underground »

[32] FIDIS. *Déclaration de Budapest sur les documents de voyage à lecture automatique (MRTD-Machine ReadableTravelDocuments.* Disponible sur < http://www.fidis.net/fileadmin/fidis/press/budapest_declaration_on_MRTD.fr.pdf > (Consulté le 28/12/2006).

du Réseau d'Excellence FIDIS[33] (Futur de l'Identité dans la Société de l'Information) présentent les carences des DVLA. En effet, hormis les fraudes et délits affectant déjà les documents d'identité, les chercheurs du FIDIS rappellent que les DVLA comportent des menaces additionnelles. Les passeports biométriques RFID présenteraient ainsi des risques pour la sécurité et la protection de la sphère privée des utilisateurs et pourraient accroître les vols d'identité. En clair, la version actuelle du passeport européen utilise des technologies et des normes qui n'atteignent pas les objectifs visés.

En effet, selon le FIDIS, les données contenues dans les DVLA peuvent être interceptées et lues jusqu'à une distance de 10 mètres du porteur, et ce de manière totalement invisible. Le comité rappelle également que les informations biométriques pourraient être employées à d'autres fins par les secteurs publics et privés. Parmi les autres menaces identifiées, le FIDIS cite notamment le caractère irrévocable des données biométriques et la validité de 10 ans des DVLA. Deux caractéristiques qui permettront l'utilisation frauduleuse d'informations dérobées durant un laps de temps important. Les systèmes de sécurité qui doivent protéger le contenu des puces sur lesquelles seront stockés les données ne peuvent garantir une protection efficace pour les dix années à venir. Christoph Thiel, spécialiste en cryptographie pour le groupe bancaire allemand Sparkasse va jusqu'à s'interroger sur l'adéquation de techniques biométriques avec les besoins en sécurité du secteur bancaire[34]. En dépit de ces réserves, le 22 novembre 2005, la CNIL a rendu un avis favorable sur le décret instituant le passeport électronique[35].

Le FNAEG est un exemple révélateur à la fois des possibilités offertes par un fichier basé sur des éléments biométriques, mais aussi des changements qui peuvent altérer jusqu'à sa nature même. Conçu à l'origine pour faciliter l'identification et la recherche des auteurs des infractions sexuelles, il concerne aujourd'hui la quasi-totalité des crimes et des délits d'atteinte aux biens ou aux personnes ainsi que les trafics. La liste des personnes susceptibles d'être recensées dans ce fichier s'est

---

[33] Informations disponibles sur http://www.fidis.net/about/

[34] Rick PERERA, *Biometric cards debated (21/12/2002)*. Disponible sur < http://www.pcworld.com/article/id,80392-page,1-c,encryption/article.html > (Consulté le 28/12/2006)

[35] CNIL. *Délibération n°2005-279 du 22 novembre 2005* 22 Novembre 2005 - Thème(s) : Déplacement, Sécurité, Biométrie, Titres d'identité. Disponible sur < http://www.cnil.fr/index.php?id=1992 > (Consulté le 28/12/2006)

considérablement accrue puisqu'il suffit de remplir de conditions procédurales de la mise en examen et non plus d'avoir été condamné.

Cette évolution s'est faite en deux grandes phases. A sa création, le FNAEG recensait uniquement les empreintes génétiques de personnes définitivement condamnées pour des infractions graves présentant un caractère sexuel. Mais, à la suite de la loi du 15 novembre 2001 pour la sécurité quotidienne, la liste de ces infractions a été élargie une première fois à des infractions à caractère terroriste ou d'atteinte contre les biens. La loi du 18 mars 2003 pour la sécurité intérieure a élargi à la fois la liste des infractions pouvant donner lieu à inscription au fichier national automatisé des empreintes génétiques (FNAEG) et la liste des personnes dont l'empreinte peut être inscrite dans le fichier ou comparée avec son contenu. La CNIL a estimé que l'importance de cette double extension du champ d'application du fichier nécessitait des garanties sérieuses destinées à prévenir tout enregistrement non contrôlé, erroné ou abusif des personnes et tout usage d'un tel fichier à des fins étrangères à celles pour lesquelles il a été constitué.

La CNIL a obtenu un certain nombre de garantis parmi lesquelles une durée maximale de conservation des informations relatives aux personnes mises en cause fixée à vingt-cinq années au lieu des quarante prévues à l'origine. Cependant la proposition d'effacement des informations quand la personne a été mise hors de cause par la procédure judiciaire, notamment en permettant l'identification du coupable n'a pas été suivie par le Gouvernement.

Les débats autour de la création d'un titre d'identité électronique, éventuellement obligatoire, ont fait ressurgir les craintes à propos de la constitution d'un fichier des Français. Depuis la période de Vichy, la France n'a pas connu de projet de fichier national des Français à proprement parler. Depuis la réintroduction d'une carte nationale d'identité en 1955, et en dépit de nombreuses réformes et modernisations de ce document, aucun fichier des Français n'a été reconstitué. Seul un fichier de gestion de la carte nationale d'identité a été créé en 1986 pour la mise en œuvre de la nouvelle carte d'identité sécurisée. Comme le reconnaît la CNIL, il existe en France un fichier nominatif pas comme les autres : le Répertoire national d'identification des personnes physiques (RNIPP). La CNIL est extrêmement réticente à son utilisation et s'est efforcée de la cantonner au domaine de la protection sociale. La

loi subordonne d'ailleurs l'utilisation du NIR pour le compte de l'Etat à une autorisation par décret en Conseil d'Etat après avis motivé et publié de la CNIL[36]. Dans une délibération du 29 novembre 1983, la Commission a recommandé que l'emploi du NIR comme identifiant des personnes dans les fichiers ne soit ni systématique, ni généralisé et qu'en conséquence, chaque traitement automatisé soit doté d'identifiants diversifiés et adaptés à leurs besoins propres[37]. La crainte est que le NIR devienne un identifiant unique rendant aisé l'interconnexion des fichiers.

Le projet INES[38] fait le choix d'un usage intensif de la biométrie pour garantir l'identité des personnes. La carte nationale d'identité devra contenir des données relatives à l'état civil et des identifiants biométriques, la photographie et les empreintes digitales. La même démarche de sécurisation du titre en recourant à la biométrie pourrait être étendue par la suite au permis de conduire. L'ensemble de ce système reposerait sur la création d'une base centrale constituée de plusieurs fichiers. Cette segmentation doit garantir un accès proportionné aux données contenues dans la base. Tous les usages de cette base ne nécessiteraient pas d'accéder aux mêmes types de données personnelles et, a fortiori, à l'ensemble des données. Celle-ci contiendrait :

- un **fichier des six empreintes digitales** recueillies lors de la demande initiale de titre, destinée à éviter la délivrance de titres sous plusieurs identités à une même personne ou sous une même identité à plusieurs personnes ; un **fichier des photographies** ; un **fichier de gestion** des titres avec l'identité, proche du fichier de gestion existant pour la carte nationale d'identité sécurisée ; un **fichier des archives** contenant les justificatifs scannés présentés lors du dépôt de la demande de titre.

Afin de limiter les dérives les données biométriques choisies ne doivent pas excéder ce qui est strictement nécessaire à la bonne exécution de la finalité première, c'est-à-dire garantir l'unicité de l'identité. Le respect du principe de proportionnalité le

[36] Lorsque l'utilisation du NIR ne se fait pas pour le compte de l'Etat, l'autorisation de la CNIL est nécessaire Article 27 de la Loi 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Informations très complètes disponibles sur <http://www.cnil.fr/index.php?id=301 > (Consulté le 17/02/07).

[37] Délibération n° 83-058 du 29 novembre 1983 portant adoption d'une recommandation concernant la consultation du Répertoire national d'identification des personnes physiques et l'utilisation du numéro d'inscription au répertoire. Disponible sur < http://www.cnil.fr/index.php?id=1380&print=1 > (Consulté le 17/01/07).

[38] Identification nationale électronique sécurisée.

requiert. Cela signifie par exemple que les empreintes digitales relevées n'ont pas besoin d'être roulées mais seulement posées. Les empreintes roulées sont uniquement utilisées en police judiciaire. Ce point technique nuancerait certaines critiques considérant qu'un tel fichier d'identité équivaudrait à un fichier automatisé des empreintes digitales[39] (FAED) généralisé à l'ensemble des Français. M. François Giquel, vice-président de la CNIL, a jugé pour sa part que le principe de proportionnalité ne serait pas respecté. Pour la Ligue des droits de l'homme, il y aurait confusion entre ce fichier et le FAED. Plus encore, la Ligue s'oppose à la création pure et simple d'un fichier d'identification. Elle estime qu'une fois le fichier créé il sera impossible de revenir en arrière. Les garanties et limites arrêtées ne résisteraient pas longtemps aux tentations d'utiliser le fichier à des fins de police judiciaire. A l'occasion d'affaires criminelles médiatiques, il serait certainement reproché au législateur d'avoir retiré au magistrat un moyen d'enquête ou d'instruction peut-être déterminant. En somme, créer un fichier reviendrait à mettre le doigt dans un engrenage. Pour appuyer son propos, elle a évoqué l'exemple du fichier automatisé des empreintes génétiques dont le champ d'utilisation n'a cessé de s'accroître depuis sa création en 1998.

Nombreuses et variées les techniques biométriques offrent un éventail de réponses aux défis de l'authentification et de l'identification. Cependant, aucune n'apporte de réponse universelle compte tenu des coûts ou des contraintes de mises en œuvre. Les systèmes ne sont pas intrinsèquement fiables à cent pour cent et peuvent, dans certaines conditions, être abusés par des utilisateurs malintentionnés. De plus la mise en place de bases de données centralisées offre des objectifs de choix à des cyber-attaques En dépit de ces défauts, les Etats mettent en place des systèmes de contrôle de la population qui s'appuient sur la biométrie, ces évolutions sont souvent justifiées par la lutte antiterroriste. Cette situation crée de nouveaux défis qui dépassent largement le cadre de ces « simples » applications techniques. En effet, la portée et les dérivent potentielles dans l'utilisation de bases de données biométriques conduisent à s'interroger sur l'existence d'un cadre légal dans lequel ces applications seraient encadrées.

[39] Le FAED sert à la recherche et à l'identification des auteurs de crimes et de délits, ainsi qu'à la poursuite, à l'instruction et au jugement des affaires dont l'autorité judiciaire est saisie. Informations disponibles sur < http://www.cnil.fr/index.php?1811> (Consulté le 17/01/07)

2 Un cadre légal en construction

La mise en place de systèmes de contrôle des individus basés sur les technologies biométriques, destinés directement ou indirectement à lutter contre la menace terroriste s'inscrit dans un cadre légal existant au niveau national et international. Ces législations, à l'origine très protectrices de libertés fondamentales, peinent à encadrer de manière efficace et cohérente un secteur sécuritaire en plein bouleversement. En effet, dans le cas des pays européens la pression n'est pas seulement dictée par des agences internes de sécurité ou des gouvernements nationaux en quête de solutions pour protéger leurs concitoyens, mais aussi par les demandes sécuritaire de la puissance américaine.

2.1 Une Union européenne frappée de schizophrénie ?

L'union européenne est au cœur de la mise en œuvre des technologies biométriques. Qu'il s'agisse d'harmoniser les normes techniques ou de créer des systèmes communs, il apparait que les institutions bruxelloises jouent un rôle majeur. Cependant, écartelée entre la pression des événements (attentats), les dérivent sécuritaires nationales, la contrainte américaine et la nécessité de s'affirmer en tant qu'acteur crédible au plan sécuritaire, Bruxelles semble frappée de schizophrénie.

Un des dégâts collatéraux des actions des terroristes internationaux pourrait résider dans la décrédibilisation des instances européennes dans leur rôle de défense des droits de l'homme et des libertés fondamentales. Les Etats sont en effet prompts à saisir l'alibi d'une législation européenne contraignante pour justifier en interne des mesures impopulaires.

2.1.1 Un cadre légal garant des droits fondamentaux

La lutte antiterroriste lance nombre de défis aux pays européens, parmi ceux-ci la coopération entre les Etats sous la forme d'échanges d'informations ou d'interopérabilité des systèmes de contrôle aux frontières. Il est donc naturel que l'Union européenne occupe une place primordiale dans la définition du cadre législatif nécessaire. Plusieurs textes fondateurs régissent directement ou indirectement la mise en œuvre des contrôles biométriques, ces textes sont très protecteurs pour les citoyens.

Par la Convention de sauvegarde des droits de l'homme et des libertés fondamentales de 1950[40], le Conseil de l'Europe garantie les droits fondamentaux, et, en particulier, dans l'article 8 (cité en annexe 1) il consacre le droit à la vie privée et à la protection de la correspondance. Toutefois, le Conseil de l'Europe a estimé par la suite que cet article 8 contenait un certain nombre de limites et d'inconvénients au regard du développement nouveau de l'informatique et des technologies de l'information. La portée du terme « vie privée » y est insuffisamment définie et la prise en considération de la protection contre l'ingérence de personnes qui ne sont pas une autorité publique est inexistante. Cette réflexion a conduit à l'adoption en 1981 d'une convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, appelée convention 108 (extraits cités en annexe 2), qui a été ratifiée par 31 États membres du Conseil de l'Europe, dont tous les États membres de l'Union

[40] Conseil de l'Europe, *Convention de sauvegarde des Droits de l'Homme et des Libertés fondamentales*, amendée par le Protocole n° 11, Rome, 4.XI.1950. Disponible sur < http://conventions.coe.int/Treaty/fr/Treaties/Html/005.htm >. Consulté le 12/01/07.

européenne[41]. C'est sur cette base que repose la Directive 95/46/EC[42] (extraits cités en annexe 3) qui constitue le cadre légal du développement de la biométrie au sein de l'Union européenne. En France, la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, a été modifiée par la loi n°2004-801 du 6 août 2004 afin de transposer cette directive 95/46 CE. La loi définit les principes régissant les traitements de données à caractère personnel et les règles destinées à en assurer le respect par une autorité administrative indépendante, la Commission nationale de l'informatique et des libertés (CNIL)[43]. Il est important de connaître les principes régissant le traitement des données à caractère personnel car ils doivent, en principe, servir de base à la mise en place de tous les systèmes biométriques. En accord avec cette réglementation, les données faisant l'objet d'un traitement doivent être :

- collectées et traitées de manière loyale et licite ;
- collectées pour des finalités déterminées, explicites et légitimes et ne pas être traitées ultérieurement de manière incompatible avec ces finalités, sauf pour des fins statistiques ou de recherche scientifique ou historique ;
- adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et de leurs traitements ultérieurs ;
- exactes, complètes et, si nécessaire, mises à jour ;
- conservées sous une forme permettant l'identification des personnes concernées pendant une durée qui n'excède pas la durée nécessaire aux finalités pour lesquelles elles sont collectées et traitées.

Entre temps, la recommandation adoptée le 9 mai 2003 par l'OACI qui prévoit l'intégration avant 2015 d'au moins une donnée biométrique dans les documents de

---

[41] Conseil de l'Europe, *Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel* .Strasbourg, 28.I.1981. Disponible sur < http://conventions.coe.int/Treaty/fr/Treaties/Html/108.htm > (Consulté le 12/01/07).

[42] Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, Journal officiel n° L 281 du 23/11/1995 p. 0031 – 0050. Disponible sur < http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:FR:HTML> (Consulté le 12/01/07).

[43] La CNIL a rendu de nombreux avis sur les questions que soulèvent la biométrie et ses implications sur le respect des libertés fondamentales. En outre toute utilisation d'un dispositif biométrique est soumise à son autorisation préalable. Voir <http://www.cnil.fr/index.php?id=2162> (consulté le 12/01/07).

voyages a contraint les pays européens à légiférer[44]. Le Conseil européen de Thessalonique de juin 2003 a affirmé la nécessité de dégager au sein de l'Union une approche cohérente en ce qui concerne les identificateurs ou les données biométriques utilisés. Une telle approche doit également prévaloir pour la détermination des spécifications techniques des systèmes de manière à assurer leur interopérabilité. Cette approche a été appliquée aux passeports, aux titres de séjour des ressortissants de pays tiers et aux visas. Ainsi, en application d'un règlement du 13 décembre 2004[45], les Etats membres de l'Union européenne doivent, à partir du 28 août 2006, délivrer des passeports incluant une donnée biométrique sur une puce : la photographie faciale. L'introduction d'une seconde donnée biométrique, les empreintes digitales, interviendra dans un délai de 36 mois à compter de l'adoption de spécifications techniques qui ne sont pas encore arrêtées.

La montée de la menace terroriste offre à l'Union la possibilité s'imposer comme un acteur majeur. En effet, si la lutte antiterroriste se trouve au cœur des prérogatives régaliennes des Etats, les caractéristiques du terrorisme international limitent leurs possibilités individuelles d'intervention. Il se crée donc un espace d'action pour les institutions européenne pour coordonner une coopération et apporter une plus value à l'action des Etats.

2.1.2 Les conséquences de l'impératif de coopération

Le but du Conseil européen est de faciliter les échanges de données et d'informations entre les autorités judicaires et administratif. L'objectif serait qu'une information disponible pour l'administration d'un Etat membre le soit aussi pour les administrations correspondantes des autres Etats. L'instrument pour accroître la sécurité au sein des frontières de l'Union repose sur une utilisation des NTIC dont les identifiants biométriques. La Commission européenne estime que « les outils de

[44] OMD/ IATA/OACI. *Directives relatives aux renseignements préalables concernant les voyageurs. Mars 2003*. Disponible sur < http://www.wcoomd.org/ie/fr/Librairie/32%20-%20APIGuidelines_FR.pdf > (Consulté le 12/01/2007).

[45] Conseil de l'Europe. *Règlement n° 2252/2004 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 membre.* Disponible sur < http://eur-lex.europa.eu/LexUriServ/site/fr/oj/2004/l_385/l_38520041229fr00010006.pdf > (Consulté le 12/01/2007).

protection des données et de la vie privée préservent les personnes des mesures d'ingérence excessives de la part des autorités gouvernementales ou des acteurs privés. Ils protègent les individus d'un déséquilibre dans les pouvoirs qui porterait atteinte à leur liberté individuelle, mais aussi de pratiques comme le profilage, l'exploration et le suivi des données qui permettent d'exercer sur eux un contrôle presque total[46]» Il apparaît légitime de se demander si c'est bien le cas et si la législation actuelle permet non seulement d'assurer aux citoyens le niveau de protection auquel ils s'attendent mais aussi d'intervenir rapidement et efficacement auprès des contrevenants dont les terroristes [47].

Un des problèmes de l'Union et ses responsables politiques semble résider dans le manque de confiance des citoyens dans les capacités des organisations d'emploi et de contrôle à préserver le caractère privé des données. Alors que le rôle joué par l'Union la rapproche, au moins symboliquement, des citoyens, l'incursion des agences gouvernementales dans la sphère privée, grâce notamment à la biométrie, provoque une défiance croissante chez ces mêmes citoyens. Cette situation crée un déficit de communication qui exacerbe cette perte de confiance alors même que les NTIC ont aussi pour objectif de convaincre qu'elles sont indispensables à la protection de leur sécurité. La principale suspicion est que les agences de coopération et leurs instruments n'échappent à tout contrôle démocratique. Il pourrait en résulter des procédures et des pratiques non conformes aux règles éthiques qui mettraient en danger les libertés individuelles et le respect de la vie privée. La saisie, le stockage, la transmission automatique, la propriété est en particulier l'emploi des informations biométriques sont en constante augmentation en l'absence de régulations crédibles et de règles éthiques adaptées. Cette situation présente des risques pour la société civile, le respect des lois et des procédures légales et compromet la confiance des citoyens dans l'Union. Elle compromet certains des objectifs prioritaires de l'Union et mine les principes fondateurs de

---

[46] INSTITUTE FOR PROSPECTIVE TECHNOLOGICAL STUDIES (IPTS), *Sécurité et respect de la vie privée du citoyen à l'ère du numérique après le 11 septembre : Vision prospective*, juillet 2003. Disponible sur <http://cybersecurity.jrc.es/docs/LIBE%20STUDY/LIBE-IPTS%20study%20%20executive%20summary%20French%20version.pdf> (Consulté le 12/01/2007).

[47] Commission de l'éthique de la science et de la technologie. *L'utilisation des données biométriques à des fins de sécurité : questionnement sur les enjeux éthiques*. Document adopté à la 17e réunion de la Commission de l'éthique de la science et de la technologie le 7 décembre 2004, Québec. Disponible sur < http://www.ethique.gouv.qc.ca/fr/ftp/Biometrie-reflexion.pdf > (consulté le 12/01/2007).

l'Union (voir supra). La collecte et le stockage de données biométriques au sein de bases de données interopérables engendre la suspicion quant à la proportionnalité entre les moyens employés et les buts à atteindre. Les gouvernements et les agences de sécurité son perçues comme dénuées de pratiques éthiques et suivent des politiques assez floues ce qui exacerbe le déficit de confiance des citoyens.

Les attentats du 11 mars 2004 à Madrid ont redoublé les tentations sécuritaires des gouvernements, et l'accent a de nouveau été mis sur la nécessité d'une action concertée par l'UE dans ce domaine. Catégorisés sous le titre de « sécurité frontalière », ces projets ont envisagé la transmission de données personnelles des passagers des pays tiers voyageant vers l'UE, et de l'UE aux EU, par les compagnies aériennes aux autorités responsables du contrôle des frontières et de la gestion de l'immigration (données API). Cette intensification de la surveillance du mouvement, réalisée par l'élargissement (en augmentant les échanges des données personnelles) et l'approfondissement (en introduisant la biométrie) des contrôles, semble contredire certaines dynamiques à l'œuvre au sein de l'UE notamment en ce qu'elle se veut un espace de libre circulation et de faible contrôle aux frontières. Les mesures menant à cette intensification de la surveillance, mais aussi la manière par laquelle ces mesures ont été adoptées, posent des questions fondamentales sur la légitimité, la démocratie et la protection des droits de l'Homme au sein de l'UE. Sous le drapeau de l'« interopérabilité », on avance donc vers un système dans lequel les bases de données de l'Union européenne contenant d'importants volumes de données personnelles sensibles peuvent être interconnectés et accessibles à un nombre considérable d'agences étatiques. Ce développement est rendu possible en dépit du fait que les bases de données européennes aient été construites dans des objectifs très divers – de la facilitation de l'examen des demandes de visas et d'asile (VIS, Eurodac) à la coopération policière et à l'anti-terrorisme (aspects du SIS, Europol) – et en dépit du fait qu'elles contiennent des catégories de données variées. Ainsi, l'interopérabilité – notamment si elle est justifiée par la logique de la « guerre anti-terroriste » – peut rendre les garanties sur l'accès et l'utilisation de ces bases de données dépourvues de sens et d'effet.

Le projet de loi sur les transporteurs fut justifié, et en fin de compte adopté, en vertu des articles 62(2) (a) et 63(3) (b) du Traité CE. Ces articles servent de fondement

légal à l'adoption des mesures relatives respectivement aux contrôles des personnes aux frontières extérieures, et à l'immigration clandestine. De même, l'article 1 de la directive 2004/82/CE spécifie qu'elle « *vise à améliorer les contrôles aux frontières et à lutter contre l'immigration clandestine, au moyen de la transmission préalable aux autorités nationales compétentes, par les transporteurs, de données relatives aux passagers* [48]».Certains Etats membres ont essayé de la présenter comme une mesure liée à la sécurité nationale et à la lutte anti-terroriste. L'approche selon laquelle la directive serait une mesure anti-terroriste liée à la sécurité nationale engendre des doutes quant à *la* légalité de son adoption par le Conseil seulement sous le 1er pilier (droit Communautaire). Cette complexité est encore plus forte du fait que les bases de données européennes, à cause de leur diversité, ont été établies sous des bases légales différentes (1er/3ème piliers) et sont réglées par des régimes de protection des données différents. Ces régimes sont très fragmentaires dans le 3ème pilier, où les règles et les systèmes de supervision spécifiques sont applicables pour chaque agence spécifiques (comme Eurojust et Europol) – il n'y a donc pas de cadre commun de législation et de supervision de la protection des données dans le 3ème pilier. Ces garanties fragmentaires paraissent limitées et inefficaces dans un climat où l'accès maximum aux données personnelles est facilité, et la coopération opérationnelle entre les agences de contrôle au niveau européen– mais aussi au niveau national car élément central de l'action de l'Union européenne dans le domaine de la Justice et des Affaires Intérieures est l'interopérabilité.

La directive 2004/82/CE du Conseil du 29 avril 2004 fut d'ailleurs sévèrement critiquée du fait de la disproportion par rapport à la réussite des objectifs cités : améliorer les contrôles frontaliers et combattre l'immigration clandestine. Toutefois, ces objections apparurent moins fortes dès lors que la directive était justifiée par la nécessité de combattre le terrorisme. L'objectif anti-terroriste pourrait être utilisé pour justifier des mesures intensives – en ce cas, la transmission extensive des données personnelles aux autorités frontalières. Ces considérations eurent un effet direct sur les négociations et *le* contenu *de* la directive, notamment dans le domaine de la protection des données personnelles. L'article 6 de la directive (concernant le

[48] Directive 2004/82/CE du Conseil du 29 avril 2004 concernant l'obligation pour les transporteurs de communiquer les données relatives aux passagers Disponible sur < http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX%3A32004L0082%3AFR%3AHTML > (Consulté le 17/02/06).

traitement des données) fut l'objet de négociations longues et controversées reflétant les approches nationales diverses sur la protection des données transmises sous la directive. Du fait de la pression exercée par la Grande-Bretagne, deux importantes « concessions » furent accordées :

- les données seront effacées par les autorités frontalières dans les 24 heures de la transmission « *à moins qu'elles ne soient nécessaires ultérieurement pour permettre aux autorités chargées d'effectuer les contrôles sur les personnes aux frontières extérieures d'exercer leurs pouvoirs réglementaires conformément au droit national et sous réserve des dispositions relatives à la protection des données figurant dans la directive 95/46/CE* [49]»

- les Etats membres peuvent utiliser les données transmises « *pour répondre aux besoins des services répressifs* ».

Il est clair que ces additions rendent les garanties préexistantes concernant l'accès, la rétention et l'usage de données pratiquement sans intérêt. Il n'est pas du tout surprenant que l'insertion de ces clauses additionnelles ait été saluée par le gouvernement britannique – puisque de cette manière la directive s'alignait sur l'approche britannique « *multi-agency* » associant les contrôles frontaliers et la lutte contre l'immigration clandestine, la criminalité et le terrorisme.

Les attentats de Madrid en mars 2004 ont été suivis par une déclaration du Conseil Européen sur le terrorisme, mettant la priorité sur l'adoption de la directive API[50], malgré l'opposition du Parlement européen. Selon le Traité CE, le Parlement devrait être consulté avant que la directive ne soit adoptée – mais finalement la directive fut adoptée sans l'avis du Parlement. En Grande-Bretagne, le gouvernement a décidé de passer outre la réserve d'examen parlementaire (*parliamentary scrutiny reserve*) du comité de l'Union européenne de la Chambre des Lords, qui avait exprimé son opposition à la directive. En liant le contrôle des frontières et de l'immigration

---

[49] Conseil européen. *Directive on the obligation of carriers to communicate passenger data, Brussels, 23 March 2004, 7595/04.* Disponible sur < http://www.statewatch.org/news/2004/mar/eu-pnr-Directive.pdf > (consulté le 12/01/07).

[50] *Les informations API* se rapportent aux données contenues dans les passeports (nom, date de naissance, sexe, numéro de passeport, nationalité, état dans lequel le passeport a été établi) et sont transférées par avance par les compagnies aériennes aux autorités du pays de destination, afin de faciliter le contrôle aux frontières. Voir < http://www.assemblee-nationale.fr/europe/dossiers_e/e2887.asp > (Consulté le 17/02/07).

clandestine à la lutte contre la criminalité et le terrorisme, la directive ouvre la porte à une routinisation de la transmission des données personnelles liées à la vie quotidienne à un nombre considérable d'autorités étatiques, qui peuvent ainsi commencer à construire le profil de tous ceux qui entrent dans l'Union européenne.

Ces développements soulèvent ainsi deux paradoxes pour l'Union européenne et ses Etats membres. Le premier paradoxe concerne la relation entre l'objectif de construction d'une Union européenne sans frontières et sans contrôles à l'intérieur, et l'intensification des contrôles et de la surveillance de l'autre côté. Le deuxième paradoxe concerne la coexistence d'une pression pour créer une identité européenne fondée sur la légalité et la protection des droits fondamentaux, et l'évocation de cette identité par rapport aux relations extérieures de l'Union européenne négociant par « une voix », avec la résignation des institutions européennes de compromettre ces principes quand ils parlent d'« une voix » lors de négociations internationales.

2.2 Biométrie et terrorisme : des enjeux mondiaux

2.2.1 Etats-Unis : l'imposition de normes ?

Premier à réagir pour mieux assurer la sécurité sur son territoire et tenter d'empêcher d'autres attaques terroristes, le gouvernement américain adoptait – 43 jours après l'événement – le Patriot Act qui amplifiait considérablement les pouvoirs de la police et de la justice. Quelques mois plus tard, le 21 mars 2002, était adoptée la National Homeland Security Agency Act [51]ayant pour but de créer une agence nationale pour assurer la sécurité du territoire américain. Le 30 juillet suivant, cette Agence était transformée en ministère, le Department of Homeland Security, avec tous les pouvoirs afférents. Relevant de ce ministère, la Transportation Security Administration[52] (TSA), chargée de la sécurité des moyens de transport, a défini trois applications spécifiques des technologies biométriques :

[51] Disponible sur < http://www.uscg.mil/legal/Homeland_legislation/text/101101%20S%201534.htm> (Consulté le 17/02/07).
[52] Voir le site de cette administration < http://www.tsa.gov/ > (consulté le 17/02/07).

le contrôle d'accès aux aéroports et aux gares, la surveillance et la détection des voyageurs susceptibles de menacer la sécurité, et le contrôle des passagers. En juin de la même année, était également implanté le National Security Entry-Exit Registration System[53] (NSEERS), qui a pour but de mieux contrôler l'entrée aux États-Unis de ressortissants de l'Iran, de l'Iraq, de la Libye, du Soudan et de la Syrie ou d'autres pays qui présentent un risque élevé sur le plan de la sécurité. Le contenu d'une base de données gérée par le service d'immigration, comprenant neuf millions d'empreintes digitales dont celles des criminels et terroristes étrangers, gérée par le service d'immigration, a été intégré au système. Depuis le 31 décembre 2003 , un programme de contrôle des frontières pour les détenteurs de visas, le US Visit Program[54], a également été mis en place. La vérification des entrées et sorties des visiteurs avec visa s'appuiera sur un contrôle d'identité à partir des documents de voyage et la prise d'empreintes digitales.

Le National Institute of Standards and Technology (NIST – États-Unis)a été appelé à coordonner les travaux de normalisation conduits au niveau national au sein de l'InterNational Committee for Information Technology Standards (INCITS) et au niveau international, avec l'objectif d'accélérer les procédures nécessaires pour aboutir à la définition de normes de compatibilité et d'évaluation des performances des technologies biométriques. Dans les faits, les Etats-Unis relèvent les empreintes digitales des étrangers entrant sur le territoire américain et les conservent soixante-quinze ans.

La législation antiterroriste américaine et ses textes d'application ont prévu de manière unilatérale l'obligation pour toute compagnie aérienne assurant des vols à destination des Etats-Unis de donner, aux services de contrôle aux frontières américaines, accès aux dossiers de réservation de leurs passagers dits "Passenger Name Record" (PNR) contenus dans leur système de réservation.[55]. Les données PNR peuvent inclure un grand nombre de détails allant du nom et de l'adresse du passager à son adresse email, en passant par les détails de sa carte bancaire et,

---

[53] Informations détaillées disponibles sur < http://www.brandeis.edu/isso/travel/NSEERS_After_December_2003.pdf > (Consulté le 17/02/07).

[54] Informations détaillées disponibles sur le site de Departement of Homeland Security < http://www.dhs.gov/xtrvlsec/programs/content_multi_image_0006.shtm > (Consulté le 17/02/07)

[55] Titre 49, US Code, section 44909(c)(3) et titre 19, Code of Federal Regulations, section 122.49b. Disponible sur < http://www4.law.cornell.edu/uscode/uscode49/usc_sec_49_00044909----000-notes.html> (Consulté 17/02/07).

même, ses préférences alimentaires pendant le vol. Les données PNR sont donc plus générales que les données API. La législation des EU a aussi été examinée par le groupe article 29, très critique des demandes américaines[56].

Les négociations entre la Commission et les Etats-Unis présentent, comme en d'autres occasions, le dilemme de la coopération de l'Union européenne avec des pays tiers au risque de compromettre le droit et les valeurs de l'UE. Dans le cas du PNR, la Commission a saisi l'opportunité de représenter les Etats membres (en considérant les échanges PNR comme une question relative au marché intérieur/1er pilier) et peut prétendre que l'accord UE/EU n'est pas inégal, puisque les engagements américains contiennent une clause de réciprocité. Cette clause est cependant conditionnelle à la mise en place par l'Union européenne d'un système de transmission des données PNR identique au modèle américain. Cela peut anticiper la décision par les institutions européens rendant un tel système souhaitable dans l'Union européenne (ou même compatible avec le droit communautaire et les droits fondamentaux). La Commission a requis une démarche globale de l'Union européenne sur les transferts PNR. Concernant les transferts entre l'UE et les EU, la Commission a proposé comme solution le développement d'un cadre légal réglant les transferts existants de PNR aux Etats-Unis. Ce cadre prendrait la forme d'une décision adoptée par la Commission certifiant la protection adéquate des données PNR par les EU, suivie par un accord international « léger » entre la Communauté européenne et les Etats-Unis. Le système de transmission des données PNR couvre des catégories très étendues de données personnelles et renforce l'argument du groupe selon lequel cette transmission constitue la surveillance généralisée par un Etat tiers et participe à la construction de profils d'individus. Les demandes de la législation américaine sont disproportionnées et semblent être contraires aux droits fondamentaux relatifs à la vie privée et à la protection des données personnelles bien établis dans le droit communautaire. La Commission a mis l'accent sur les concessions obtenues des Américains, mais la force légale des engagements est douteuse. Les préoccupations sur la protection de la vie privée et des données personnelles sont renforcées par le fait que l'accord permet la transmission de PNR

[56] Avis 4/2003 sur le niveau de protection assuré aux Etats-Unis pour le transfert des données des passagers, doc. 11070/03, WP 78. Le groupe a conseillé à la Commission d'assurer *inter alia* que les objectifs de transfert des données et les autorités ayant accès à ces données soient spécifiés et le principe de la proportionnalité respecté

provenant de l'UE par les autorités américaines aux pays tiers laissant ainsi en effet les autorités américaines seules juges de l'adéquation de la protection des droits de l'Homme offerte par ces pays.

Le 30 mai dernier, la Cour de justice européenne de Luxembourg a prononcé l'annulation de l'accord conclu le 28 mai 2004 entre la Communauté européenne et les Etats-Unis autorisant le transfert de données passagers aériens (PNR). La Cour a conclu à l'annulation de la décision d'adéquation au motif que le traitement lié au transfert des données PNR aux autorités américaines (CBP - Bureau des douanes et de la protection des frontières des États-Unis -) a pour objet la sécurité publique et les activités de l'État (américain) relatives à des domaines du droit pénal qui ne relèvent pas du champ d'application de la directive de 1995 sur la protection des données[57].

Cette décision est particulièrement symbolique des contradictions entre la volonté des Etats de faire jouer aux institutions européennes un rôle majeur dans la lutte anti-terroriste en parfaite contradiction avec les fondements légaux sur lesquels est bâtie l'Union.

2.2.2 Un secteur économique stratégique en pleine expansion

La croissance internationale des communications, tant en volume qu'en diversité (déplacement physique, transaction financière, accès aux services...), implique le besoin de s'assurer de l'identité des individus. L'importance des enjeux, motive les fraudeurs à mettre en échec les systèmes de sécurité existants. Il y a donc un intérêt grandissant pour les systèmes d'identification et d'authentification. Leur dénominateur commun, est le besoin d'un moyen simple, pratique, fiable, pour vérifier l'identité d'une personne, sans l'assistance d'une autre personne.

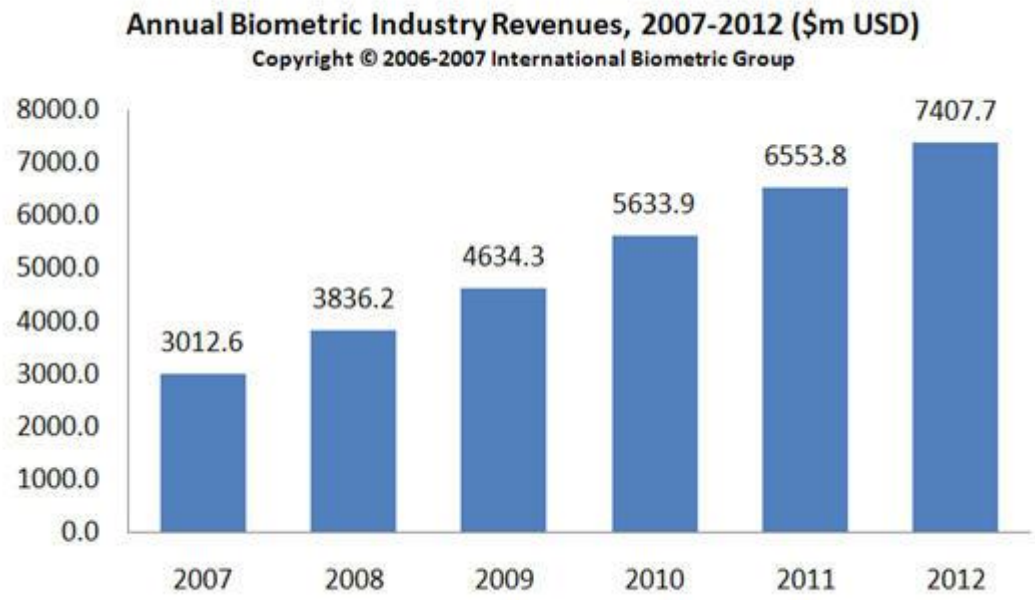
[57] Groupe de travail «ARTICLE 29» sur la protection des données. *Avis 5/2006 sur l'arrêt de la Cour de justice du 30 mai 2006 dans les affaires jointes C-317/04 et C-318/04 relatives au transfert de données PNR aux Etats-Unis.* Disponible sur < http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp122_fr.pdf> (Consulté le 17/02/07).

Ce marché est en pleine expansion et peut exercer une pression sur la prise de décision relative à l'utilisation des données biométriques à des fins de sécurité. Le marché est reconnu pour être difficile à appréhender dans sa globalité car il est fragmenté en fonction des données biométriques privilégiées et du type de système développé (grands systèmes d'identification portant sur les empreintes digitales, par exemple, qui représentent environ 50 % du marché, et petits terminaux ou capteurs biométriques destinés à différentes données biométriques). Compte tenu des objectifs de modernisation et d'harmonisation des instruments d'identification judiciaire afin d'assurer une meilleure coopération entre les États, mais aussi dans la perspective où plusieurs gouvernements envisagent de doter leurs citoyens et résidents de titres biométriques, l'industrie de la biométrie a le vent en poupe. Certains estiment, cependant, que le besoin de normalisation du secteur pourra jouer un rôle dans la compétition. La normalisation (ou standardisation), dont les objectifs répondent aux préoccupations du gouvernement américain, a pour but de faciliter les échanges et l'interopérabilité (accès à de l'information ou à des bases de données par différents systèmes) des systèmes biométriques – et donc la comparaison de données, d'éviter que les utilisateurs soient dépendants de systèmes propriétaires, d'harmoniser les méthodes et les principes d'évaluation des performances et de déterminer les outils nécessaires pour assurer la sécurité des frontières[58]. Les enjeux de la normalisation sont à la fois politiques et économiques; il est d'ailleurs permis de croire que les pays disposant des meilleures technologies seront sans doute à même d'imposer leurs propres exigences en matière de protection des renseignements personnels et de respect de la vie privée. L'International Biometric Group[59] prévoit une augmentation de plus de 500% en 5 ans du revenu de cette industrie. Selon le cabinet Frost & Sullivan, le marché de la biométrie pourrait atteindre les 900 millions de dollars en 2006 contre 66 millions 2000. Les sociétés nord-américaines dominent actuellement le marché des équipements biométriques à hauteur de 75%.

---

[58] Office parlementaire d'évaluation des choix scientifiques et technologiques, *Les méthodes scientifiques d'identification des personnes à partir de données biométriques et les techniques de mise en œuvre*, Rapport présenté au Sénat par Christian CABAL, député, Assemblée nationale, juin 2003. [en ligne]. Disponible sur http://www.senat.fr/commission/offices/office030616.html#toc3. (Consulté le 18/01/06).

[59] Pour plus d'information sur le développement de l'industrie des technologies biométriques voir http://www.biometricgroup.com/



L'Europe veut s'affirmer comme un acteur majeur dans le domaine de la biométrie, ainsi un centre européen d'excellence des technologies biométriques **European Biometrics Centre of Excellence (CoE)**[60] a été crée à Bruxelles. Plus encore qu'une vitrine des savoir-faire européen dans les domaines de l'authentification, il offre des opportunités non seulement pour évaluer les plus récents progrès techniques mais aussi un cadre de discussion en experts de haut niveau.

[60] Pour plus d'informations voir http://www.europeanbiometrics.info/

3 La mise en place de la biométrie : un piège pour la démocratie ?

La mise en place de documents infalsifiables permettant le fichage (sans connotation péjorative) de l'ensemble des citoyens constitue le « saint graal » de tous les services de police et de renseignement. L'histoire est émaillée de tentatives pour assurer la sécurité du corps social[61] au moyen d'un contrôle et d'un fichage de la population. La côte très élevée du terrorisme à la « bourse de menaces » pourrait permettre de remettre en cause les fondements de la liberté individuelle et du respect de la vie privée. Cette influence indirecte des terroristes sur la vie des citoyens se double d'une remise en cause du rapport des Etats avec leur territoire.

3.1 Quel est le prix à payer pour des systèmes biométriques efficaces ?

Si la valeur intrinsèque des technologies biométriques ne peut pas fondamentalement être remise en question, leur efficacité directe dans la lutte

[61] Xavier CRETTIEZ et Pierre PIAZZA dir. *Du Papier à la biométrie, identifier les individus*. Presses de Science Po. Paris 2006. 331p.

antiterroriste reste difficile à démontrer. Il existe un problème de proportionnalité entre les résultats attendus de la biométrie dans ce domaine et les conséquences sur le respect des droits fondamentaux et de libertés individuelles des citoyens européens.

3.1.1 Peut-on établir un lien d'efficacité objectif entre la biométrie et la lutte antiterroriste ?

Les autorités politiques peinent à justifier la mise en place de systèmes de contrôle biométriques sans remettre en cause les notions fondamentales de droit sur lesquelles reposent, non seulement la législation nationale mais aussi les accords internationaux signés par la France. En effet, l'utilisation du marquant biométrique n'apporte une plus-value que dans le cas où les fichiers sont interconnectés et où les individus sont contrôlés dans leurs déplacements et leurs actions. Il devient ainsi possible de mener des actions de « profilling » et de cibler des comportements à risques. L'interconnexion des fichiers est clairement interdite par la législation actuelle la question se pose donc du rapport coût efficacité de technologies qui peuvent remettre en cause les fondements sociaux pour répondre à un problème d'importance relative.

En France, en 1986 dans son discours programme, sous le titre «le défi du terrorisme » J. Chirac, nommé Premier ministre, évoquait la création de documents infalsifiables. En Grande Bretagne, en 1985, une proposition de loi du député conservateur John Biggs-Davison se prononçait en faveur de l'institution d'une carte nationale d'identité dont, précise-t-il, un des objectifs sera de combattre plus efficacement l'IRA. Aucune de ces tentatives visant à lier instauration d'un dispositif national d'identification et lutte anti-terroriste n'a abouti dans ces deux pays. Cela s'explique sans doute par les coûts induits par une telle entreprise (énorme investissement financier, bureaucratisation accrue, risque de détérioration des relations entre police et population, etc.), mais aussi parce que pas un de leurs promoteurs n'est parvenu à expliquer clairement et précisément comment la carte d'identité améliorerait la lutte contre le terrorisme. Aux lendemains des attentats du 11 septembre, les autorités britanniques et françaises ont de plus en plus souvent fait appel à l'argument de la lutte anti-terroriste pour expliquer combien apparaissaient

indispensables leurs projets de carte nationale d'identité électronique contenant des données biométriques. C'est parce que les nouvelles cartes d'identité dont l'institution est envisagée constituent un remède à la fraude identitaire, c'est-à-dire un « moyen simple et sécurisé de vérifier les identités[62]», qu'elles seront précieuses pour combattre le terrorisme. En effet, cette fraude est présentée comme « associée à toutes les formes de grande criminalité, du terrorisme au trafic de drogue et d'êtres humains». Et, en nourrissant ainsi « à grande échelle[63] » le terrorisme, elle met en péril la sécurité de l'État, puisque le terrorisme « profite des lacunes des systèmes actuels pour se jouer des contrôles». Ces dernières années, les pouvoirs publics ont avancés un autre argument pour convaincre l'opinion publique du caractère judicieux de leurs projets de mise en carte des nationaux : le poids des contraintes internationales. Cette idée selon laquelle la France et la Grande-Bretagne doivent désormais prendre en considération les standards élaborés par l'Organisation de l'Aviation Civile Internationale et les règlements européens relatifs à l'introduction d'éléments biométriques dans les passeports[64] a été exprimée, plus ou moins clairement, pour suggérer combien devenait impératif le recours à ces mêmes éléments dans les cartes nationale d'identité. Afin de lutter contre le terrorisme, il a été décidé au niveau international d'introduire de la biométrie dans les titres de voyage. Sont concernés en premier lieu les passeports. Le règlement européen du 13 décembre 2004 impose d'insérer dans une puce la photographie du titulaire d'ici à juin 2006, et ses empreintes d'ici à décembre 2007[65]. Si les CNI ne paraissent pas concernées par ce règlement, de par leur fonction de titre de voyage, il serait cependant logique qu'elles intègrent les mêmes fonctionnalités. Dans le cas britannique, c'est bien davantage le registre de l'évidence ou de la fatalité que le Premier ministre Tony Blair mobilise en affirmant qu'il s'agit « d'avoir un coup d'avance (a step ahead) sur les terroristes que de toutes façons nous allons bien devoir être obligés de suivre les évolutions des exigences techniques américaines et

---

[62] Commentaire de David Blunkett sur le rapport du Select Committee de la Chambre des Communes relatif au projet de carte d'identité biométrique, 27 octobre 2004

[63] Intervention sur le Forum des droits sur Internet de Fabrice Mattatia (Chargé de mission du projet INES au ministère de l'Intérieur), février 2005. Disponible sur < http://www.foruminternet.org/forums/descr.php?f=16> (Consulté le 18/01/06).

[64] Conseil européen. « *Règlement (CE) n° 2252/2004, op.cit.*

[65] Pour plus d'informations voir le site du ministère de l'intérieur sur http://www.interieur.gouv.fr/misill/sections/a_l_interieur/la_police_nationale/dossiers_et_documents/securite-aeroportuaire8055/surete-transports-aeriens/view (Consulté le 18/02/07).

européennes vers l'adoption de passeports biométriques[66]. Aucune intervention d'un quelconque responsable politique de l'hexagone ne prend la peine d'évaluer l'importance qu'il convient d'accorder à l'argument de la lutte antiterroriste dans la justification du projet INES, alors que cette question préoccupe les pouvoirs publics britanniques. Bien plus soumis à la pression des média à l'heure où la Grande-Bretagne est un des derniers pays ne disposant pas de carte nationale d'identité en Europe, ces derniers ont plusieurs fois été conduits à présenter l'encartement des nationaux comme n'étant pas la panacée. Ainsi, en novembre 2004, lors de sa conférence de presse mensuelle, Tony Blair a tenu à souligner à propos de la carte : « Bien entendu, elle ne constitue pas la solution miracle contre le terrorisme et la criminalité organisée, personne ne dit cela, mais elle constituera une arme importante dans la lutte contre les menaces modernes que posent le terrorisme et la criminalité organisée[67] ».

3.1.2 Quel prix à payer pour des systèmes biométriques offrant une véritable plus-value ?

Une carte nationale d'identité biométrique pourrait éventuellement revêtir une utilité incontestable dans la lutte contre le terrorisme si les informations qu'elle permet de se procurer sur les détenteurs de ce titre (l'ensemble des nationaux dans le cas où ce document devenait obligatoire) étaient interconnectées avec d'autres données personnelles détenues par les autorités à des fins administratives, fiscales, policières ou judiciaires et une multitude de renseignements exploités à des fins de surveillance. Dans un tel cas de figure, le fichier informatique centralisé élaboré grâce à l'ensemble des données recueillies sur les porteurs d'une carte constituerait un outil supplémentaire d'un vaste dispositif technologique autorisant non seulement le repérage d'individus déjà identifiés comme dangereux, mais aussi l'élaboration, dans le cadre des analyses de la menace terroriste, de profils à risque. Or, les gouvernements britannique et français s'évertuent à rappeler que leurs projets actuels de mise en carte des nationaux ne s'inscrivent nullement dans une logique de traçage ou de profilage susceptible de porter atteinte à la liberté

---

[66] Point de presse du porte-parole du Premier ministre, 25 mai 2005, Disponible sur <http://www.pm.gov.uk/output/page7548.asp>.

[67] Conférence de presse mensuelle du 1er ministre, 29 novembre 2004. Disponible sur < http://www.number-10.gov.uk/output/page6687.asp>.

individuelle. Beaucoup de pays pourraient être « tentés par un fichage effréné pour lutter contre le terrorisme, pratique qui risque de devenir prétexte lorsque l'on finit par considérer que tout opposant est un terroriste par « complicité »[68] ». Ce point de vue est partagé par le sociologue canadien David Lyon pour qui le projet britannique de carte d'identité « intelligente » augmentera la capacité des instances étatiques à se livrer au « tri social » en discriminant certaines catégories de la population au comportement stigmatisé comme indésirable. Au-delà de ces craintes, se pose également le problème de la production de discours policiers sur l'anticipation des comportements terroristes qui ne reposent sur aucune forme de savoir scientifique. Ce type de discours a pour seule fonction de justifier l'introduction de dispositifs « *high tech* », tel le projet INES, dont pourtant rien ne garantit qu'il sera opérationnel pour combattre le terrorisme : « Utiliser l'argument de la lutte anti-terroriste pour la constitution d'un registre de population est extrêmement discutable. En outre, de telles mesures passives ne vont pas changer quoi que ce soit ; mieux vaut mettre l'accent sur l'infiltration d'organisations clandestines pour lutter contre le terrorisme»[69]. Ce type de mesure technologique sophistiquée ne peut avoir qu'un intérêt relatif car, seul, il ne peut suffire à empêcher certains individus déterminés à commettre un acte terroriste : le plus important pour les services de renseignement est de pouvoir repérer ces mêmes individus préalablement, alors que la carte d'identité ne servira généralement qu'à établir leur identité une fois l'attentat commis. Au vu des évènements récents, les terroristes peuvent se recruter au sein des communautés nationales française et britannique. Dès lors, en quoi une carte nationale d'identité, serait-elle d'une extrême fiabilité, pourrait-elle être d'une quelconque utilité pour combattre des terroristes à même d'obtenir ce document en toute légalité ? Dans les premiers attentats commis à Londres en juillet 2005, les terroristes disposaient de papiers en règles qui ont d'ailleurs été retrouvés, pour certains d'entre eux, sur les lieux de leurs forfaits. Il apparaît illusoire d'envisager de combattre efficacement des terroristes à la fois membres d'une communauté nationale et ennemi idéologique de celle-ci grâce à un outil renvoyant exclusivement à l'un des deux termes de l'équation : l'appartenance nationale.

---

[68] Audition par la CNIL, projet INES, 8 mars 2005, http://www.cnil.fr/fileadmin/documents/approfondir/dossier/CNI-biometrie/CRAUDITIONJOINET.pdf.

[69] Audition par la CNIL, projet INES, 11 mars 2005**,** <http://www.cnil.fr/fileadmin/documents/approfondir/dossier/CNI-biometrie/CRAUDITIONBIGO.pdf.> (Consulté le 17/02/07)

Dans son rapport rendu public en juin 2005 sur le projet INES, le Forum des droits sur l'Internet (mandaté par le ministre de l'Intérieur pour organiser un débat citoyen sur ce projet) n'hésite pas à souligner que l'argument de la lutte anti-terroriste n'a pas convaincu la grande majorité des internautes. D'une part, le discours associant lutte contre le terrorisme et contraintes internationales concernant le passeport « a pu donner l'impression que la France subissait des pressions étrangères, européennes et surtout américaines[70]». En France, certains ont créé des sites Web de contestation spécifiquement consacrés à cet enjeu, en s'inspirant directement de la longue expérience d'ONG britanniques telles que Statewatch[71], et plus particulièrement Privacy International[72].

Selon le sociologue Patrice Flichy, le projet INES aurait certainement été mieux accepté par les français si le gouvernement s'était attaché à démontrer qu'il permet d'améliorer significativement la lutte contre le terrorisme. Or, constate-t-il : « La démonstration reste à faire[73] ». En effet, non seulement l'absence d'argumentation donne du poids à la contradiction, mais elle l'amplifie aussi en plaçant les responsables des projets de mise en carte dans une posture délicate. Ainsi, succédant à Dominique de Villepin à la tête du ministère de l'Intérieur, Nicolas Sarkozy a dû se résigner à geler momentanément le projet INES en reconnaissant, en juin 2005, que si des dispositions européennes nous obligent à mettre rapidement en œuvre un passeport biométrique, il n'en va pas de même pour la carte d'identité électronique.

Quelques semaines plus tard, le même ministre mobilisait l'échelon supranational comme ressource. En effet, les 4 et 5 juillet 2005, la réunion du G 5 à Evian a été l'occasion pour lui et ses homologues britannique, espagnol, italien et allemand de se mettre d'accord afin d'œuvrer non seulement en faveur de la délivrance de cartes d'identité électroniques compatibles et « interopérables », mais aussi d'étendre la biométrie à tous les documents d'identification[74]. La mobilisation de la « ressource

---

[70] Rapport sur le Forum des droits sur l'Internet sur la carte d'identité électronique, juin 2005. disponible sur <http://www.foruminternet.org/telechargement/documents/rapp-cnie-20050616.pdf > (Consulté le 17/02/07).

[71] Voir <http://www.statewatch.org/> (Consulté le 17/02/07).

[72] Voir http://www.privacyinternational.org/ (Consulté le 17/02/07).

[73] Patrice Flichy est professeur de sociologie à l'université de Marne-La-Vallée et co-auteur du livre blanc Administration électronique et protection des données personnelles (2002). Intervention sur le Forum des droits sur Internet, 13/04/2005, http://www.foruminternet.org /forums/read.php?f=16&i=2559&t=2559.

[74] « Une Europe plus sûre, une Europe plus solidaire », Figaro du 12 mai 2005.

supranationale » n'est pas l'apanage des gouvernants français puisque les autorités britanniques font, quant à elles, aussi de plus en plus appel à un registre discursif désormais « classique » : l'invocation de la nécessité de respecter les obligations européennes… Quitte à les créer soi-même lorsque le moment apparaît politiquement opportun. Ainsi, le 13 juillet 2005, une semaine à peine après les attentats de Londres, le ministre de l'Intérieur britannique, Charles Clarke présidait une session extraordinaire du conseil Justice et Affaires Intérieures réunissant l'ensemble des ministres de l'Intérieur et de la Justice des 25 pays membres. La déclaration condamnant les attentats émise à l'issue du conseil demandait aux États-membres d'adopter des « normes communes pour les éléments de sécurité et des procédures sûres de délivrance des cartes d'identité » pour décembre 2005, et ce afin de lutter contre le terrorisme[75].

Depuis près de trente ans, les gouvernants français et britanniques invoquent la nécessité de lutter contre le terrorisme pour justifier de projets « high-tech » d'encartement de leurs nationaux. Pourquoi les pouvoirs publics tentent-ils ainsi de lier mise en carte des nationaux et lutte anti-terroriste, alors même que le « remède » suggéré semble inadapté à la « maladie » ? Les technologies de pointe, comme la biométrie, sont au cœur de multiples enjeux stratégiques autour desquels s'affrontent notamment l'Europe et les Etats-Unis. Il n'est, à cet égard, pas illégitime de se demander dans quelle mesure ces enjeux économiques, industriels, financiers, etc. pèsent sur la prise de décision politique et les registres discursifs qui la soutiennent. On trouve, par exemple, sur le site Internet du GIXEL un *Livre bleu* publié, en juillet 2004, au nom des industriels de la « Filière électronique et numérique ». Ce rapport commence par affirmer : « Les Industries Électroniques et Numériques employaient en France 300 000 personnes en 1998. Aujourd'hui, seulement 220 000. Tombera-t-on à 100 000 en 2008 ?[76]» Puis, plus loin, précise : « L'effort pour lutter contre le terrorisme doit être comparé à un effort de guerre comme celui que nous avons consenti pendant la période de guerre froide. Mais avec une nuance d'importance, le bouclier américain ne protègera pas l'Europe !

---

[75] Conseil de l'Union européenne : « Communiqué de presse, Session extraordinaire, Justice et affaires intérieures », Press Office, Bruxelles, 13 juillet 2005, p. 7« Note from the Presidency to Strategic Committee on Immigration, Frontiers and Asylum on Minimum common standards for national identity cards », Brussels, 11 July 2005.

[76] Livre bleu. Grands programmes structurants. juillet 2004, Disponible sur < http://www.gixel.fr/Portal_Upload /Files/ASSISES%202004/LB300604.pdf > (consulté le 17/02/07).

[…] La sécurité est très souvent vécue dans nos sociétés démocratiques comme une atteinte aux libertés individuelles. […] Pour faire accepter les technologies de surveillance et de contrôle, il faudra probablement recourir à la persuasion et à la réglementation en démontrant l'apport de ces technologies à la sérénité des populations et minimisant la gène occasionnée[77] »

3.2 La géopolitique est-elle modifiée par le recours a biométrie dans la lutte antiterroriste ?

3.2.1 Le terrorisme est-il l'alibi utilisé pour résoudre le défi de la mobilité ?

Le recours accru à l'outil technique et plus spécifiquement à l'identifiant biométrique transforme la relation à l'espace et aux territoires. Pour pénétrer l'espace Schengen, mais aussi le Homeland américain, il est exigé des individus qu'ils soient équipés de passeports électroniques comportant leurs données biométriques d'identification. Leur mise en œuvre a suscité des résistances, mais souvent, au sein des arènes de décision, ce que l'on cherche à identifier c'est la meilleure technologie (empreintes digitales, iris, ADN…), il n'est alors question que d'efficacité, de coût, de temps de mise en œuvre, d'amortissement.

Par-delà la « guerre au terrorisme » et les appels à un recours accru aux dites « nouvelles technologies », par-delà ce que certains perçoivent comme une inquiétante généralisation de la surveillance, que d'autres encore disent nécessaire à la sécurité des populations, toutes ces questions semble trouver un dénominateur commun : la relation contrariée au territoire qu'entretiennent les agences de sécurité. Cette relation est aujourd'hui bouleversée par la possibilité technologique et animée d'une forte angoisse, celle de la mobilité. On peut s'interroger à la manière de l'auteur de « surveiller et punir »[78] pour savoir si l'Etat n'est « plus [alors] essentiellement défini par sa territorialité, par la surface occupée, mais par une masse : la masse de la population avec son volume, sa densité, avec bien sûr, le

[77] *Idem*
[78] Michel FOUCAULT, *Sécurité, Territoire, Population. Cours au Collège de France, 1977-1978*, Paris, Seuil/Gallimard, 2004, p. 112.

territoire sur lequel elle est étendue, mais qui n'en est en quelque sorte qu'une composante »[79]. Michel Foucault suggérait ainsi un double glissement : celui d'un « Etat de territorialité » vers un « Etat de population » et celui d'un « pacte de territorialité » vers un « pacte de sécurité » entre le souverain et le peuple. Dans le premier cas, le Prince assure en premier lieu la sûreté et l'unité d'un espace territorial, contre des intrusions extérieures, et par le renforcement de la frontière, définissant ainsi progressivement l'espace territorial d'exercice illimité du pouvoir souverain. Dans le second cas, la « sécurité » n'est pas tant celle du territoire que de la population en elle-même conduite au travers de technologies biométriques. Les développements à l'œuvre en matière de numérisation des documents d'identification, la manière dont est aujourd'hui envisagée le recours à l'outil technique biométrique, semblent tous prolonger et approfondir les logiques historiques de contrôle et de surveillance mise en évidence par Michel Foucault dans ses cours au collège de France à la fin des années 1970.

Les développements centrés autour de l'introduction de l'outil numérique dans les pratiques d'authentification des papiers et d'identification des individus prennent corps dans un tissu épais de textes, d'énoncés, de discours, de rapports qui décrivent, qualifient et spatialisent la « menace terroriste ». C'est dans la manière dont la menace se voit progressivement articulée à la technique, depuis une dizaine d'années aux Etats-Unis et plus récemment en Europe, qu'émerge de lourdes convergences d'approche. Depuis la fin des années 1960, il s'est en effet opéré, aux Etats-Unis, un glissement progressif dans l'énonciation de la menace terroriste. Il est possible de définir trois mouvements dans la description de la menace terroriste. Le premier articule la menace sur les coordonnées spatiales traditionnelles la territorialisant, l'associant à des aires géographiques bien précises et/ou des Etats souverains (Syrie, Afghanistan…). Le second tend à l'inverse à le déterritorialiser et le re-localiser dans un ordre social. Il décrit alors des individus regroupés en cellules terroristes, inscrites en réseaux, distribuées à la surface de la planète, et dotées d'une certaine autonomie par rapport à un organe de commandement. Le troisième mouvement est venu offrir un nouveau support à cette rationalité, l'associant à la technique, définissant alors des menaces d'un nouveau type, dont les cibles, les

[79] Foucault M., *op. cit.*, p. 113.

infrastructures critiques et autres systèmes informatiques ne sont plus nécessairement matériels, mais dont la destruction engendrerait les plus graves dommages pour la nation.

Les deux premiers mouvements de territorialisation et de déterritorialisation coexistent dans les analyses américaines sur le terrorisme depuis vingt-cinq ans. Mais la « guerre au terrorisme » dans laquelle est engagée l'Amérique de Georges Bush, les rhétoriques de l'Axe du mal, ou bien encore les nouvelles mesures de contrôle aux entrées et sorties du territoire national, ne peuvent être comprises que si l'on considère ce double processus de territorialisation-déterritorialisation et ses enjeux : pour engager la force militaire dans la lutte contre le « terrorisme », un Etat doit être désigné, désigné comme menaçant ; désigné comme le sont depuis 1979 les « Etats dits sponsors du terrorisme » encore appelés Rogue States ; désigné comme l'a été l'Afghanistan dans les jours ayant suivi les attaques sur New York et Washington. Inversement, une analyse en termes de réseaux, qui déterritorialise la menace implique un engagement plus marqué du renseignement dans toutes ses dimensions et ne va pas sans le risque d'une mise sous surveillance généralisée des individus. Le troisième mouvement, associant donc menace et technique, est à la fois plus ample et plus lourd de conséquences. Il ne vient plus seulement articuler la menace sur le squelette des frontières territoriales, mais sur celui, bien technique, des systèmes informatiques qui présentent cette double caractéristique d'être à la fois encrés dans l'ordre territorial (des serveurs, des disques durs, des rooters, des détecteurs, des capteurs, des stations d'acquisition, des scanners, des caméras… accumulés dans des bâtiments, dispersés en divers point de la surface de la planète) et générateur d'espaces d'échanges et de communication (cyberespace).

La menace revêt alors deux formes principales : celle d'attaques portées contre des infrastructures critiques et celle d'attaques électroniques, portées au moyen de puissants programmes informatiques contre les systèmes eux-mêmes. La menace terroriste ne se résume plus seulement à des « Etats sponsors du terrorisme », non plus seulement à des réseaux de « cellules terroristes » dispersées à travers la planète. Aux Etats-Unis, la Maison Blanche a progressivement élevé la sécurité du cyberespace et des systèmes informatiques au rang de problème de sécurité

nationale, en publiant la Stratégie nationale de sécurité du cyberespace[80]. Le territoire n'est plus ici seulement considéré dans sa dimension géographique ; il est aussi câbles et faisceaux d'ondes transportant des données numériques et supportés par des infrastructures nationales dites critiques. Cette stratégie – d'ailleurs dite nationale et de sécurité – légitime ainsi l'intervention de l'Etat, le réinvestit dans sa figure de souverain face à un espace discontinu, à délimiter, à légiférer et, à en croire certains hauts responsables militaires américains, à pacifier. En France, le récent rapport « Chantier sur la lutte contre la cybercriminalité » révèle l'étrange la relation entre cyberespace et technique.

Du Système d'Information Schengen (SIS I et II) aux programmes de contrôle des entrées et sorties du territoire américain US VISIT ; des bases de données d'Europol au nouveau Visa Information System (appelé à être branché sur le SIS II), le cyberspace est ici considéré dans sa dimension non territoriale certes, mais surtout pour le dispositif de contrôle et de surveillance qu'il constitue. Par le recueil et surtout l'accumulation des données (traces) digitales qu'il autorise, ces pratiques visent non seulement l'identification des individus, mais leur localisation dans l'ordre territorial géographique, et la reconstitution de leurs trajectoires, ceci au moyen du recueil et du recoupement des traces numériques, certaines biométriques. Et tout ce qui peut ainsi être collecté doit être enregistré, conservé, accumulé dans ces bases de données. Mais en recourant ainsi de manière active aux bases de données, entièrement constitutives de ce « cyberespace », les agences de sécurité participent activement de sa construction. L'interconnexion croissante de ces bases est entièrement guidée aux Etats-Unis par le souci de partage de l'information entre agences de sécurité (militaires, polices, renseignement, douanes) mais aussi entre secteurs privé et public.

[80] « Le cyberespace est essentiel à la *homeland security* et à la *national security* ; sa sécurité et sa fiabilité soutiennent l'économie, les infrastructures critiques et la défense nationale » *The National Security Strategy to Secure Cyberspace*. Disponible sur < http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf > (consulté le 17/02/07).

3.2.2 Vers une transformation radicale de la notion de frontière et un état d'urgence permanent ?

La technique biométrique vient établir ce lien crucial entre, d'une part, le contrôle des individus en un point d'un espace territorial donné et repérable dans les coordonnées euclidiennes de la plus simple des géométries et, d'autre part, ces systèmes de bases de données en voie d'intégration détenant les éléments nécessaires à l'identification des individus. Il se dessine un dispositif de contrôle et de surveillance, incarné dans ces systèmes informatiques intégrés et s'activant à plusieurs niveaux, à la fois sur et par-delà les espaces territoriaux/nationaux.

« Le programme INES – identité nationale électronique sécurisée – est un projet global qui consistera à : Fusionner, simplifier et sécuriser les procédures de demande de passeport et de carte nationale d'identité; Améliorer la gestion de ces titres dans de nouvelles applications ; Délivrer des titres hautement sécurisés conformes aux exigences internationales ; Offrir aux citoyens les moyens de prouver leur identité sur Internet et de signer électroniquement, afin de favoriser le développement de l'administration électronique »[81]. I

Il apparaît légitime de penser que l'outil biométrique ne débouchera pas sur les effets escomptés (fin des fraudes, arrestation des « terroristes » et autres migrants déclarés illégaux), le recours au contrôle biométrique n'est toutefois pas dépourvu d'effets. Au-delà de l'illusion de la nouveauté, il approfondit en fait les logiques historiques de contrôle en les systématisant et en les automatisant. Il transforme aussi la frontière et incline la trajectoire historique de l'Etat dans ses activités de contrôle et de surveillance. La réhabilitation de la frontière dans sa fonction de démarcation depuis le 11 septembre cohabite avec la technicisation du contrôle et des documents d'identification. Observable à travers la mise en place du *Homeland Security Department* aux Etats-Unis et les velléités proches en Europe, elle redessine une carte des territoires à sécuriser pour mieux protéger les populations

[81] Le programme INES, Secrétariat général, Direction de programme INES, ministère de l'Intérieur, de la Sécurité intérieure et des Libertés locales. Disponible sur < http://www.interieur.gouv.fr/sections/a_la_une/publications/rapports-d-activite-du-ministere/rapport-d-activite-2004/downloadFile/attachedFile_4/RAMadm.pdf >

des dangers de l'extérieur. La frontière passe d'une forme linéaire et continue à un ensemble discontinu de points, de points de contrôle à l'embarquement qui sont autant de points de connexion à ces bases de données (registres digitalisés) dans lesquelles sont progressivement enregistrées les identités supposées des individus contrôlés. Dans le cas de l'individu dont le profil répondrait à celui, préétabli, d'un « terroriste » par exemple, la numérisation du contrôle ouvre la possibilité d'une surveillance plus poussée, d'une traçabilité accrue, chaque contrôle générant sa trace numérique, dont le recueil et la conservation autorisent, désormais, éventuellement, la reconstitution des *trajectoires*.

La carte nationale d'identité biométrique permet la dispersion de ces points de contrôle à l'intérieur même du territoire. Ils viendront s'ajouter à ceux déjà existants du maillage technique serré qui innerve nos sociétés (borne de retrait d'argent, connections à l'Internet, carte magnétique d'accès aux transports en commun…). Le projet d'équiper, à terme, les forces mobiles de police britanniques de systèmes de lecture adaptés aux documents biométriques d'identification, vient s'ajouter aux obligations données aux fournisseurs d'accès Internet de conserver les données de connections des internautes.

Il devient possible de retracer la trajectoire des individus. Dans cet ensemble en mouvement à plusieurs échelles (locale, nationale, globale ; urbaine, régionale, planétaire), le processus de numérisation et les adaptations des pratiques de contrôle et de surveillance d'Etat qu'il génère redessinent les lieux et les modes d'exercice de l'autorité souveraine, en opérant une démultiplication de la capillarité du pouvoir. Il en découle une redéfinition des lieux d'application du pouvoir souverain et des adaptations dans l'ordre géopolitique. La frontière se trouve dès lors prise dans ce mouvement de pixellisation qui correspond à la distribution de ces points de contrôle à la surface de la planète, contrôle mis au service d'une politique de protection à distance du Homeland d'une part, et de l'espace Schengen d'autre part.

La mise en place de puce RFID dont les aspects négatifs ont été étudiés dans la première partie renforce les capacités de contrôle des Etats. D'autre part, la lecture des titres à distance pourrait être le fait des autorités publiques**.** Les personnes seraient contrôlées à leur insu sans qu'il soit procédé à un contrôle d'identité

individualisé. L'ensemble des règles relatives aux contrôles, aux vérifications et aux relevés d'identité pourrait s'en trouver bouleversé.

Depuis le 11 septembre 2001, plusieurs gouvernements ont saisi l'occasion qui se présentait pour introduire ce que certains appellent un « nouveau paradigme sécuritaire »[82] et agir à l'égard de la sécurité de leur territoire en adoptant des politiques ou des mesures qui ont pour effet global de modifier l'équilibre sécurité/vie privée en faveur des intérêts sécuritaires du pays[83]. L'utilisation de systèmes informatiques qui facilitent la saisie de données et leur partage entre de multiples sources afin de faciliter la collecte d'informations s'inscrivent dans les mesures adoptées. De façon générale, selon une étude réalisée pour la Commission européenne, « les initiatives ainsi prises en matière de sécurité ont également renforcé les pouvoirs des gouvernements et des organismes d'application des lois qui peuvent désormais accéder aux données à caractère personnel à d'autres fins que celles pour lesquelles elles ont été initialement fournies.

Tous ces développements, qu'il s'agisse de l'interconnexion des bases de données des appareillage bureaucratiques ordonnés au renseignement et à la lutte contre le terrorisme, du recours aux identifiants biométriques et de l'accumulation d'information sur les individus par le recueil des traces numériques qu'ils génèrent quotidiennement, renvoient tous et pour partie à la notion d'espace. Ce qui est en train de s'opérer, c'est la recherche d'une correspondance via les identifiants biométriques entre, d'une part, les squelettes techniques des réseaux de bases de données contenant les informations relatives aux individus et autour desquels les administrations se réorganisent et, d'autre part, le squelette bien géographique des frontières. Et tandis que la frontière glisse de la ligne au point, le mouvement historique de transformation de l'Etat et de l'art même de gouverner connaissent une nouvelle inclinaison. Le recours à la technique qui autorise le relevé systématique et automatique des traces digitales et leur accumulation dans des réseaux en voie d'intégration sont la marque de la stratégie de l'état d'urgence en voie de constitution.

---

[82] IPTS – INSTITUTE FOR PROSPECTIVE TECHNOLOGICAL STUDIES, *op. cit.*, p.4.
[83] Op. cit., p 6.

CONCLUSION

Nombreuses et variées, les techniques biométriques offrent un éventail de réponses aux défis de l'authentification et de l'identification. Cependant, aucune n'apporte de solution universelle compte tenu des coûts ou des contraintes de mises en œuvre. Les systèmes ne sont pas intrinsèquement fiables à cent pour cent et peuvent, dans certaines conditions, être abusés par des utilisateurs malintentionnés. De plus, les bases de données centralisées constituent des objectifs de choix pour des cyber-attaques. En dépit de ces défauts, les Etats mettent en place des systèmes de contrôle de la population qui s'appuient sur la biométrie, ces évolutions sont souvent justifiées par la lutte antiterroriste. Le terrorisme n'est pourtant pas la raison objective du développement des techniques de contrôle biométrique, le besoin de sécurité qu'il crée dans les sociétés occidentales induit des choix politiques lourds de conséquences.

En effet, au nom d'une « simple menace », qui n'a pas d'ailleurs pas l'immédiateté d'un quelconque danger, des mesures techniques peuvent remettre en cause fondamentalement les libertés individuelles. D'aucun pourront essayer de démontrer que le téléphone portable ou la carte bleue permettent déjà de suivre les déplacements des Français. Mais personne n'est obligé de posséder ce genre de produit, en tout état de cause on peut choisir le moment et le lieu de leur utilisation. Ce n'est pas le cas des puces RFID qui associeront de manière irréversible l'individu et son document biométrique sans qu'il n'en ait conscience à chacun de ses déplacements.

Les changements du rapport des Etats avec les frontières n'ont pas qu'un intérêt sociologique. Ils démontrent la difficulté des institutions à s'adapter à la mobilité des individus et la tendance récurrente à répondre aux besoins de sécurité de la population par des mesures intrusives, disproportionnées par rapport aux objectifs à atteindre.

Il ne s'agit aucunement de refuser les progrès technologiques, mais les circonstances dans lesquelles sont développés et mis en place ces systèmes doit conduire tout citoyen à s'interroger. D'autant plus que les institutions européennes jouent ici un rôle particulièrement important. Alors qu'elles sont censées être le dernier rempart contre les excès des Etats nations (on pensera à la troisième partie du défunt projet de constitution), elles sont utilisées comme alibi pas des gouvernements qui peinent à justifier leurs décisions. Il s'agit d'un glissement continuel du contrat social vers un état d'urgence permanent. Le niveau actuel du plan Vigipirate suffit à illustrer cette affirmation : quel gouvernement aura le courage de rétablir une véritable échelle de valeur ?

La problématique liée à l'emploi des technologies biométriques renvoie plus généralement à la philosophie de la lutte anti-terroriste. Jusqu'où, sous prétexte de combattre terrorisme, doit-on aller dans l'altération des fondements de nos sociétés ? Ne risque-t-on pas de susciter dans les populations la réaction souhaitée par les terroristes, c'est-à-dire une rupture du contrat social du fait de la radicalisation des organes de contrôle ?

BIBLIOGRAPHIE

- BITE. 4th BITE scientific meeting. *The European Industrial Context, 4th November 2005*. [en ligne]. Disponible sur http://.www.biteproject.org (Consulté le 02/01/06).

- BBC NEWS, *Concern over biometric passports, 30 March 2004.* [en ligne]. Disponible sur < http://news.bbc.co.uk/1/hi/technology/3582461.stm > (consulté le 17/01/07).

- CABAL, Christian (*rapporteur*). *Rapport n°938 sur les méthodes scientifiques d'identification des personnes à partir de données biométriques et les techniques de mise en oeuvre,* Office parlementaire d'évaluation des choix scientifiques et technologiques. [en ligne]. Disponible sur < http://www.assemblee-nationale.fr/12/rap-off/i0938.asp> (Consulté le 28/12/2006).

- CNIL. *Délibération n°2005-279 du 22 novembre 2005 - Thème(s) : Déplacement, Sécurité, Biométrie, Titres d'identité*. [en ligne]. Disponible sur < http://www.cnil.fr/index.php?id=1992 > (Consulté le 28/12/2006).

- CNIL. *Délibération n° 83-058 du 29 novembre 1983 portant adoption d'une recommandation concernant la consultation du Répertoire national d'identification des personnes physiques et l'utilisation du numéro d'inscription au répertoire*. [en ligne]. Disponible sur < http://www.cnil.fr/index.php?id=1380&print=1 > (Consulté le 17/01/07).

- Commission de l'éthique de la science et de la technologie. *L'utilisation des données biométriques à des fins de sécurité : questionnement sur les enjeux éthiques*. [en ligne]. Document adopté à la 17e réunion de la Commission de l'éthique de la science et de la technologie le 7 décembre 2004, Québec. Disponible sur < http://www.ethique.gouv.qc.ca/fr/ftp/Biometrie-reflexion.pdf > (consulté le 12/01/2007).

- CONSEIL DE L'EUROPE. *Convention de sauvegarde des Droits de l'Homme et des Libertés fondamentales, amendée par le Protocole n° 11*. Rome, 4.XI.1950. [en ligne]. Disponible sur < http://conventions.coe.int/Treaty/fr/Treaties/Html/005.htm >. (Consulté le 12/01/07).

- CONSEIL DE L'EUROPE. *Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, 1981, no. 108.* [en ligne]. < http://conventions.coe.int/Treaty/FR/Treaties/Html/108.htm > (Consulté le 28/12/2006).

- CONSEIL EUROPEEN. *Règlement n° 2252/2004 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 membre.* [en ligne]. Disponible sur < http://eur-lex.europa.eu/LexUriServ/site/fr/oj/2004/l_385/l_38520041229fr00010006.pdf > (Consulté le 12/01/2007).

- CONSEIL EUROPEEN. *Directive on the obligation of carriers to communicate passenger data, Brussels, 23 March 2004, 7595/04*. [en ligne]. Disponible sur < http://www.statewatch.org/news/2004/mar/eu-pnr-Directive.pdf > (consulté le 12/01/07).

- CRETTIEZ, Xavier et PIAZZA, Pierre (Coll.). Du papier à la biométrie, identifier les individus. Sciences Po. Paris. 2006. 331 p.

- DAVID, Charles-Philippe. *La guerre et la paix : approches contemporaines de la sécurité et de la stratégie*, Paris, Presses de science po.

- FARRIER, Charles. House of commons, Home Affairs Committee Publications session 2003-2004. *Government proposals for identity card scheme*. [en ligne]. Disponible sur < http://www.parliament.the-stationery-office.com /pa/cm/cmhaff.htm> (consulté le 28/12/2005).

- FIDIS. *Déclaration de Budapest sur les documents de voyage à lecture automatique (MRTD-Machine ReadableTravelDocuments*. [en ligne]. Disponible sur < http://www.fidis.net/fileadmin/fidis/press/budapest_declaration_on_MRTD.fr.pdf > (Consulté le 28/12/2006).

- Forum (Le) des droits sur l'Internet. *Contribution de Bernard Didier sur les aspects biométrie.* [en ligne]. Disponible sur http://www.foruminternet.org/forums/read.php?f=16&i=3106&t=3106 (consulté le 27/01/07).

- Forum des droits sur l'Internet. *Rapport sur la carte d'identité électronique*. [en ligne]. juin 2005. Disponible sur <http://www.foruminternet.org/telechargement/documents/rapp-cnie-20050616.pdf > (Consulté le 17/02/07).

- FOUCAULT, Michel. *Sécurité, Territoire, Population. Cours au Collège de France. 1977-1978*. Paris ; Seuil/Gallimard, 2004, p. 112.

- Groupe de travail «ARTICLE 29» sur la protection des données. *Avis 5/2006 sur l'arrêt de la Cour de justice du 30 mai 2006 dans les affaires jointes C-317/04 et C-318/04 relatives au transfert de données PNR aux Etats-Unis.* [en ligne]. Disponible sur < http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp122_fr.pdf> *(*Consulté le 17/02/07).

- GUERRIER, Philippe, *LexisNexis craint un vol massif de données confidentielles.* [en ligne]. Disponible sur < http://www.vnunet.fr/fr/vnunet/news/2005/04/12/lexisnexis-craint-vol-massif-donnees-confidentielles > (Consulté le 28/12/2006).

- INSTITUTE FOR PROSPECTIVE TECHNOLOGICAL STUDIES (IPTS), *Sécurité et respect de la vie privée du citoyen à l'ère du numérique après le 11 septembre : Vision prospective, [en ligne],* Juillet 2003. disponible sur <http://cybersecurity.jrc.es/docs/LIBE%20STUDY/LIBE-IPTS%20study%20%20executive%20summary%20French%20version.pdf>. (Consulté le 12/01/2007),

- JACKSON, William. *NIST identifies good and bad points of biometrics*. [en ligne]. Disponible sur < http://www.gcn.com/print/21_25/19773-1.html > (Consulté le 28/12/2006).

- KOLOWSKY, Rey. Real *challenges for virtual borders: The Implementation of US-VISIT*. [en ligne]. Migration Policy Institute, juin 2005. Disponible sur < http://www.migrationpolicy.org/pubs/Koslowski_Report.pdf > (consulté le 23/01/2007).

- LAQUEUR, Walter. *The New Terrorism: Fanaticism and the Arms of Mass Destruction*, Oxford, Oxford University Press, 1999, 320 p.

- LECERF, Jean-René. *Identité intelligente et respect des libertés.* [en ligne]. Rapport d'information du Sénat n° 439 (2004-2005). Disponible sur <http://www.senat.fr/rap/r04-439/r04-439.html> (consulté le 21/01/07).

- LIVRE BLEU. *Grands programmes structurants*. juillet 2004. [en ligne]. Disponible sur < http://www.gixel.fr/Portal_Upload/Files/ASSISES%202004/LB300604.pdf > (consulté le 17/02/07).

- MAC CUE, Andy. *UK faces massive ID card challenges*, 01/12/2003. [en ligne]. Disponible sur < http://management.silicon.com/government/0,39024677,39117139,00.htm > (Consulté le 28/12/2006).

- MANONNI, Pierre. *Les logiques du terrorisme*, Paris, In Press, 2004. 230 p.

- MASCRE, Frédéric. *La biométrie comme méthode d'authentification : enjeux et risques*. [en ligne].Disponible sur <http://www.droit-informatique.com/index.htm> (consulté le 21/01/07).

- Office parlementaire d'évaluation des choix scientifiques et technologiques, *Les méthodes scientifiques d'identification des personnes à partir de données biométriques et les techniques de mise en œuvre*, Rapport présenté au Sénat par Christian CABAL, député, Assemblée nationale, juin 2003. [en ligne]. Disponible sur http://www.senat.fr/commission/offices/office030616.html#toc3. (Consulté le 18/01/06).

- Organisation de l'aviation civile internationale. [en ligne]. Informations diverses et règlements disponibles et < http://www.icao.int/index_f.html> (consulté le 13/02/07).

- Parlement européen et Conseil européen. *Règlement sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen de deuxième génération (SIS II)*. [en ligne]. Disponible sur < http://eur-lex.europa.eu/LexUriServ/site/fr/com/2005/com2005_0236fr01.pdf > (Consulté le 19/02/01).

- Parlement européen et Conseil européen. *Règlement concernant le système d'information sur les visas (VIS) et l'échange de données entre les États membres sur les visas de court séjour*. [en ligne]. Disponible sur <http://europa.eu.int/eur-lex/lex/LexUriServ/site/fr/com/2004/com2004_0835fr01.pdf > (Consulté le 18/02/07).

- Parlement européen et Conseil européen. *Directive 95/46/CE du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.* [en ligne]. Journal officiel n° L 281 du 23/11/1995 p. 0031 – 0050. Disponible sur < http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:FR:HTML> (Consulté le 12/01/07).

- PERERA, Rick. *Biometric cards debated* (21/12/2002). [en ligne]. Disponible sur < http://www.pcworld.com/article/id,80392-page,1-c,encryption/article.html > (Consulté le 28/12/2006).

- PUEL, Hélène. *Des milliers de Français victimes du vol de leur numéro de carte* bancaire. [en ligne]. Disponible sur <http://www.01net.com/article/282062.html. > (Consulté le 28/12/2006).

- OCDE, Direction de la science, de la technologie et de l'industrie, comité de la politique de l'information, de l'informatique et des communications, *technologies fondées sur la biométrie (DSTI/ICCP/REG(2003)2/FINAL)*. 15 juin 2005. [en ligne]. Disponible sur < http://appli1.oecd.org/olis/2003doc.nsf/43bb6130e5e86e5fc12569fa005d004c/d15c6d3ea769bc64c1256e84004c42fc/$FILE/JT00186151.PDF > (Consulté le 28/12/2006).

- TICHIT, Ludovic. *Le vol d'identités toujours aussi critique aux Etat Unis*24/05/2006. Disponible sur < http://solutions.journaldunet.com/0605/060524-vol-basededonnees.shtml > (consulté le 28/12/2006).

- UK PASSEPORT SERVICE. *Biometrics Enrolment Trial Report May 2005*. 301 p. [en ligne]. Disponible sur http://www.passport.gov.uk/downloads/UKPSBiometrics_Enrolment_Trial_Report.pdf > (Consulté le 28/12/2006).

- WEIN, Lawrence M., testimony at the hearing on "*Disrupting Terrorist Travel: Safeguarding America's Borders through Information Sharing*," *[en ligne]*, US House of Representatives Select Committee on Homeland Security, September 30, 2004. Disponible sur < http://cisac.stanford.edu/publications/disrupting_terrorist_travel_safeguarding_americas_borders_through_information_sharing/ > Consulté le 23/01/2007).

- Wolf, Philippe. *De l'authentification biométrique*. [en ligne].Sécurité Informatique, Octobre 2003 < http://www.cnrs.fr/Infosecu/num46.pdf > (consulté le 27/01/2007).

Annexe 1 : Convention de sauvegarde des Droits de l'Homme et des Libertés fondamentales

telle qu'amendée par le Protocole n° 11
Rome, 4.XI.1950 (EXTRAITS)

Les gouvernements signataires, membres du Conseil de l'Europe,

….

Sont convenus de ce qui suit:

Article 1 – Obligation de respecter les droits de l'homme

Les Hautes Parties contractantes reconnaissent à toute personne relevant de leur juridiction les droits et libertés définis au titre I de la présente Convention:

Titre I – Droits et libertés

…..

Article 8 – Droit au respect de la vie privée et familiale [1]

1. Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance.
2. Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui…..

Annexe 2 : Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel

Strasbourg, 28.I.1981 (EXTRAITS)

Chapitre I – Dispositions générales

Article 1er – Objet et but

Le but de la présente Convention est de garantir, sur le territoire de chaque Partie, à toute personne physique, quelles que soient sa nationalité ou sa résidence, le respect de ses droits et de ses libertés fondamentales, et notamment de son droit à la vie privée, à l'égard du traitement automatisé des données à caractère personnel la concernant («protection des données»).

Article 2 – Définitions

Aux fins de la présente Convention:

a. «données à caractère personnel» signifie: toute information concernant une personne physique identifiée ou identifiable («personne concernée»);
b. «fichier automatisé» signifie: tout ensemble d'informations faisant l'objet d'un traitement automatisé;
c. «traitement automatisé» s'entend des opérations suivantes effectuées en totalité ou en partie à l'aide de procédés automatisés: enregistrement des données, application à ces données d'opérations logiques et/ou arithmétiques, leur modification, effacement, extraction ou diffusion;
d. «maître du fichier» signifie: la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui est compétent selon la loi nationale, pour décider quelle sera la finalité du fichier automatisé, quelles catégories de données à caractère personnel doivent être enregistrées et quelles opérations leur seront appliquées.

Article 3 – Champ d'application

1. Les Parties s'engagent à appliquer la présente Convention aux fichiers et aux traitements automatisés de données à caractère personnel dans les secteurs public et privé.

Article 5 – Qualité des données

Les données à caractère personnel faisant l'objet d'un traitement automatisé sont:

a. obtenues et traitées loyalement et licitement;
b. enregistrées pour des finalités déterminées et légitimes et ne sont pas utilisées de manière incompatible avec ces finalités;
c. adéquates, pertinentes et non excessives par rapport aux finalités pour lesquelles elles sont enregistrées;
d. exactes et si nécessaire mises à jour;
e. conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire aux finalités pour lesquelles elles sont enregistrées.

Article 6 – Catégories particulières de données

Les données à caractère personnel révélant l'origine raciale, les opinions politiques, les convictions religieuses ou autres convictions, ainsi que les données à caractère personnel relatives à la santé ou à la vie sexuelle, ne peuvent être traitées automatiquement à moins que le droit interne ne prévoie des garanties appropriées. Il en est de même des données à caractère personnel concernant des condamnations pénales.

Article 7 – Sécurité des données

Des mesures de sécurité appropriées sont prises pour la protection des données à caractère personnel enregistrées dans des fichiers automatisés contre la destruction accidentelle ou non autorisée, ou la perte accidentelle, ainsi que contre l'accès, la modification ou la diffusion non autorisés.

Article 8 – Garanties complémentaires pour la personne concernée

Toute personne doit pouvoir:

a. connaître l'existence d'un fichier automatisé de données à caractère personnel, ses finalités principales, ainsi que l'identité et la résidence habituelle ou le principal établissement du maître du fichier;
b. obtenir à des intervalles raisonnables et sans délais ou frais excessifs la confirmation de l'existence ou non dans le fichier automatisé, de données à caractère personnel la concernant ainsi que la communication de ces données sous une forme intelligible;
c. obtenir, le cas échéant, la rectification de ces données ou leur effacement lorsqu'elles ont été traitées en violation des dispositions du droit interne donnant effet aux principes de base énoncés dans les articles 5 et 6 de la présente Convention;
d. disposer d'un recours s'il n'est pas donné suite à une demande de confirmation ou, le cas échéant, de communication, de rectification ou d'effacement, visée aux paragraphes b et c du présent article.

Article 9 – Exceptions et restrictions

…

1. Il est possible de déroger aux dispositions des articles 5, 6 et 8 de la présente Convention lorsqu'une telle dérogation, prévue par la loi de la Partie, constitue une mesure nécessaire dans une société démocratique:

a. à la protection de la sécurité de l'Etat, à la sûreté publique, aux intérêts monétaires de l'Etat ou à la répression des infractions pénales;

b. à la protection de la personne concernée et des droits et libertés d'autrui….

Annexes 3 : Directive 95/46/CE du parlement européen et du conseil (extraits)

Du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données

LE PARLEMENT EUROPÉEN ET LE CONSEIL DE L'UNION EUROPÉENNE, ONT ARRÊTÉ LA PRÉSENTE DIRECTIVE:

CHAPITRE PREMIER DISPOSITIONS GÉNÉRALES

Article premier

Objet de la directive

1. Les États membres assurent, conformément à la présente directive, la protection des libertés et droits fondamentaux des personnes physiques, notamment de leur vie privée, à l'égard du traitement des données à caractère personnel.

2. Les États membres ne peuvent restreindre ni interdire la libre circulation des données à caractère personnel entre États membres pour des raisons relatives à la protection assurée en vertu du paragraphe 1…..

Article 2

Définitions

Aux fins de la présente directive, on entend par:

a) «données à caractère personnel»: toute information concernant une personne physique identifiée ou identifiable (personne concernée); est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale;

…..

Article 6

1. Les États membres prévoient que les données à caractère personnel doivent être:

a) traitées loyalement et licitement;

b) collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités. Un traitement ultérieur à des fins historiques, statistiques ou scientifiques n'est pas réputé incompatible pour autant que les États membres prévoient des garanties appropriées;

c) adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement;

d) exactes et, si nécessaire, mises à jour; toutes les mesures raisonnables doivent être prises pour que les données inexactes ou incomplètes, au regard des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement, soient effacées ou rectifiées;

e) conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement. Les États membres prévoient des garanties appropriées pour les données à caractère personnel qui sont conservées au-delà de la période précitée, à des fins historiques, statistiques ou scientifiques.

2. Il incombe au responsable du traitement d'assurer le respect du paragraphe 1.

Article 7

Les États membres prévoient que le traitement de données à caractère personnel ne peut être effectué que si:
a) la personne concernée a indubitablement donné son consentement
ou
b) il est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci
ou
c) il est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis
ou
d) il est nécessaire à la sauvegarde de l'intérêt vital de la personne concernée
ou
e) il est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique, dont est investi le responsable du traitement ou le tiers auquel les données sont communiquées
ou
f) il est nécessaire à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le ou les tiers auxquels les données sont communiquées, à condition que ne prévalent pas l'intérêt ou les droits et libertés fondamentaux de la personne concernée, qui appellent une protection au titre de l'article 1er paragraphe 1.
Article 8
Traitements portant sur des catégories particulières de données
1. Les États membres interdisent le traitement des données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que le traitement des données relatives à la santé et à la vie sexuelle.
2. Le paragraphe 1 ne s'applique pas lorsque:
a) la personne concernée a donné son consentement explicite à un tel traitement, sauf dans le cas où la législation de l'État membre prévoit que l'interdiction visée au paragraphe 1 ne peut être levée par le consentement de la personne concernée
ou
b) le traitement est nécessaire aux fins de respecter les obligations et les droits spécifiques du responsable du traitement en matière de droit du travail, dans la mesure où il est autorisé par une législation nationale prévoyant des garanties adéquates
ou
c) le traitement est nécessaire à la défense des intérêts vitaux de la personne concernée ou d'une autre personne dans le cas où la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement
ou
d) le traitement est effectué dans le cadre de leurs activités légitimes et avec des garanties appropriées par une fondation, une association ou tout autre organisme à but non lucratif et à finalité politique, philosophique, religieuse ou syndicale, à condition que le traitement se rapporte aux seuls membres de cet organisme ou aux personnes entretenant avec lui des contacts réguliers liés à sa finalité et que les données ne soient pas communiquées à des tiers sans le consentement des personnes concernées
ou

e) le traitement porte sur des données manifestement rendues publiques par la personne concernée ou est nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice.
3. Le paragraphe 1 ne s'applique pas lorsque le traitement des données est nécessaire aux fins de la médecine préventive, des diagnostics médicaux, de l'administration de soins ou de traitements ou de la gestion de services de santé et que le traitement de ces données est effectué par un praticien de la santé soumis par le droit national ou par des réglementations arrêtées par les autorités nationales compétentes au secret professionnel, ou par une autre personne également soumise à une obligation de secret équivalente.
4. Sous réserve de garanties appropriées, les États membres peuvent prévoir, pour un motif d'intérêt public important, des dérogations autres que celles prévues au paragraphe 2, soit par leur législation nationale, soit sur décision de l'autorité de contrôle.
5. Le traitement de données relatives aux infractions, aux condamnations pénales ou aux mesures de sûreté ne peut être effectué que sous le contrôle de l'autorité publique ou si des garanties appropriées et spécifiques sont prévues par le droit national, sous réserve des dérogations qui peuvent être accordées par l'État membre sur la base de dispositions nationales prévoyant des garanties appropriées et spécifiques. Toutefois, un recueil exhaustif des condamnations pénales ne peut être tenu que sous le contrôle de l'autorité publique.
…..
Article 13
Exceptions et limitations
1. Les États membres peuvent prendre des mesures législatives visant à limiter la portée des obligations et des droits prévus à l'article 6 paragraphe 1, à l'article 10, à l'article 11 paragraphe 1 et aux articles 12 et 21, lorsqu'une telle limitation constitue une mesure nécessaire pour sauvegarder:
a) la sûreté de l'État;
b) la défense;
c) la sécurité publique;
d) la prévention, la recherche, la détection et la poursuite d'infractions pénales ou de manquements à la déontologie dans le cas des professions réglementées;
e) un intérêt économique ou financier important d'un État membre ou de l'Union européenne, y compris dans les domaines monétaire, budgétaire et fiscal;
f) une mission de contrôle, d'inspection ou de réglementation relevant, même à titre occasionnel, de l'exercice de l'autorité publique, dans les cas visés aux points c), d) et e);
g) la protection de la personne concernée ou des droits et libertés d'autrui.
2. Sous réserve de garanties légales appropriées, excluant notamment que les données puissent être utilisées aux fins de mesures ou de décisions se rapportant à des personnes précises, les États membres peuvent, dans le cas où il n'existe manifestement aucun risque d'atteinte à la vie privée de la personne concernée, limiter par une mesure législative les droits prévus à l'article 12 lorsque les données sont traitées exclusivement aux fins de la recherche scientifique ou sont stockées sous la forme de données à caractère personnel pendant une durée n'excédant pas celle nécessaire à la seule finalité d'établissement de statistiques.
….
Article 29

Groupe de protection des personnes à l'égard du traitement des données à caractère personnel

1. Il est institué un groupe de protection des personnes à l'égard du traitement des données à caractère personnel, ci-après dénommé «groupe».

Le groupe a un caractère consultatif et indépendant.

2. Le groupe se compose d'un représentant de l'autorité ou des autorités de contrôle désignées par chaque État membre, d'un représentant de l'autorité ou des autorités créées pour les institutions et organismes communautaires et d'un représentant de la Commission.

Chaque membre du groupe est désigné par l'institution, l'autorité ou les autorités qu'il représente. Lorsqu'un État membre a désigné plusieurs autorités de contrôle, celles-ci procèdent à la nomination d'un représentant commun. Il en va de même pour les autorités créées pour les institutions et organismes communautaires….

TABLES DES MATIERES

INTRODUCTION **2**

1 DES TECHNOLOGIES IMMATURES AUX APPLICATIONS MULTIPLES **6**

1.1 La biométrie : entre mythe et réalités **6**
1.1.1 Généralités sur la biométrie 7
1.1.2 Des technologies complexes non encore abouties ? 11

1.2 La biométrie dans la lutte contre les diverses formes de criminalité **14**
1.2.1 Un secteur en plein expansion aux applications multiples 16
1.2.2 Du fichier national automatisé des empreintes génétiques (FNAEG) et le projet INES 17

2 UN CADRE LEGAL EN CONSTRUCTION **23**

2.1 Une Union européenne frappée de schizophrénie ? **23**
2.1.1 Un cadre légal garant des droits fondamentaux 24
2.1.2 Les conséquences de l'impératif de coopération 26

2.2 Biométrie et terrorisme : des enjeux mondiaux **31**
2.2.1 Etats-Unis : l'imposition de normes ? 31
2.2.2 Un secteur économique stratégique en pleine expansion 34

3 LA MISE EN PLACE DE LA BIOMETRIE : UN PIEGE POUR LA DEMOCRATIE ? **37**

3.1 Quel est le prix à payer pour des systèmes biométriques efficaces ? **37**
3.1.1 Peut-on établir un lien d'efficacité objectif entre la biométrie et la lutte antiterroriste ? 38
3.1.2 Quel prix à payer pour des systèmes biométriques offrant une véritable plus-value ? 40

3.2 La géopolitique est-elle modifiée par le recours a biométrie dans la lutte antiterroriste ? **44**
3.2.1 Le terrorisme est-il l'alibi utilisé pour résoudre le défi de la mobilité ? 44
3.2.2 Vers une transformation radicale de la notion de frontière et un état d'urgence permanent ? 48

CONCLUSION **51**

BIBLIOGRAPHIE **54**
Annexe 1 : Convention de sauvegarde des Droits de l'Homme et des Libertés fondamentales 58
Annexe 2 : Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel 59
Annexes 3 : Directive 95/46/CE du parlement européen et du conseil (extraits) 62