Les technologies de l'identification.
Une note de recherche

Équipe de recherche sur le terrorisme et l'antiterrorisme (ERTA)
Revue internationale de criminologie et de police technique et scientifique
N° 1, 2005, 69-82.

Résumé
Le texte vise a donner une vue d'ensemble des différentes technologies utilisées pour identifier les individus dans différents contextes quotidiens, entre autres le contrôle de l'accès à des installations ou la surveillance de personnes soupçonnées d'activités illicites. Les technologies y sont catégorisées d'après leur objectif et leur contexte pratique d'application. On constate que certaines d'entre elles, comme la lecture d'empreintes digitales, sont utilisées dans des contextes radicalement différents comme l'accès à des services sur internet ou le contrôle d'identité judiciaire, tout en s'adaptant au cadre juridique et culturel propre à chaque contexte. Cette adaptabilité pourrait facilement produire leur omniprésence. D'autres technologies visent l'intégration de toutes les formes d'identification afin de rendre la société transparente au regard des organes officiels de contrôle.

Summary
This short paper provides a brief overview of the many new technologies developed to facilitate the identification of persons and organizes them according to their objectives and the practical context or their application. Identification technologies are deployed in many different contexts, for instance to control access to secure premises or to keep track of individuals suspected of illicit activities. Some of these technologies can be found in very different settings: for instance, fingerprint analysis is used to recognize customers of online services and for forensic identification. In these cases the technology is adapted to the different legal and cultural standards which prevail in each setting, and this capacity for adaptation has predictable impacts on the spreading of the technologies. Other technologies involve the integration of many or all identification systems in order to produce a more transparent society to facilitate the work of official control agencies.

Introduction
On peut tenter d'introduire un certain ordre dans l'explosion récente des technologies de l'identification humaine en les classifiant selon le type d'objectifs qu'ils poursuivent. Certaines technologies peuvent viser plusieurs objectifs à la fois et, dans cette mesure, notre catégorisation constitue une épure qui ne tient pas compte des cas hybrides. Toutefois, le contexte pratique où ces technologies d'identification ont été développées tend en premier lieu à déterminer la forme de

ces technologies. Il tend surtout à fixer les limites de leur acceptabilité au regard des droits de la personne et des lois existantes. Ces limites varient considérablement d'un contexte à l'autre.

La typologie présentée ci-dessous comprend six grandes catégories de technologies selon leur contexte d'application privilégié (on expliquera par la suite les acronymes utilisés dans ce tableau).

Contexte	Objectifs	Exemples
1. Contrôle d'accès	Sécurité des lieux, gestion du personnel	cartes-clés, biométrie, implants
2. fins commerciales	Maximisation du revenu	cartes fidélité, étiquettes RFID
3. Judiciaire	Preuve, contrôle de la récidive	Empreintes digitales, ADN
4. Contrôle du comportement	Monitoring des délinquants dangereux, protection des personnes à risque	Bracelet électronique
5. Surveillance de proximité	Sécurité des personnes, contrôle des déplacements, dissuasion	Reconnaissance du visage, carte d'identité, passeports
6. Surveillance à distance	classification des individus identifiés selon leur risque sécuritaire	exploration de données, méta-banques de données

Ce genre de typologie nous semble plus instructif que celles qui sont fondées sur la nature des technologies employées. Ces dernières classifications sont tributaires de changements technologiques constants et, en confondant leurs objectifs, on méconnaît la différence entre les critères de légalité qui s'appliquent à chaque contexte. Ces derniers ont pourtant un impact important sur le développement ou l'utilisation des nouvelles technologies.

1 Identification et contrôle d'accès

La plus ancienne technologie de contrôle d'accès relève bien sûr de la serrurerie. Celle-ci a plusieurs défauts qui conduisent aujourd'hui à son remplacement progressif. Les hôtels, par exemple, utilisent des clés magnétiques ou optiques qui peuvent être neutralisées et remplacées en un instant si elles sont perdues ou emportées par un hôte distrait. La clé magnétique peut aussi être individualisée, devenant ainsi une technologie d'identification de son usager. Dans une entreprise où chaque employé détient une carte personnalisée, il devient dès lors facile de savoir qui a ouvert quelle porte à quel moment, et de conserver cette information dans des banques de données pour consultation éventuelle, ou pour en extraire des *patterns* de comportement. Fonctionnellement, ceci est équivalent à l'assignation d'un code personnel à chaque individu disposant d'un accès dans un lieu. L'avantage est que le code imprimé sur une carte peut être beaucoup plus long que celui que son titulaire doit tenter de mémoriser, et qu'il offre ainsi davantage de combinaisons possibles.

La carte elle-même a beaucoup évolué et elle est passée d'un simple support magnétique ou optique à une puce informatique. Celle-ci, au lieu de se réduire à n'être que le véhicule d'un code, peut échanger de l'information avec le système gérant les accès et faire l'objet d'une nouvelle programmation à intervalles imprévisibles, ce qui déjoue les copies. On peut également l'équiper d'un émetteur miniature actif ou passif (ce qui en fait un *transpondeur,* qui ne

requiert donc pas de source d'énergie). Ces cartes/clés n'exigent plus que l'utilisateur les glisse dans une fente ou les présente à un récepteur afin qu'elles soient lues. Des senseurs encastrés dans les murs, plafonds ou portes peuvent lire à distance leur contenu, et leur détenteurs n'ont plus à les sortir de leurs poches. Ceci règle aussi le problème des déplacements multiples (plusieurs personnes passant la même porte déverrouillée par l'une d'elles) et permet de multiplier les points de contrôle.

Ces transpondeurs fonctionnent à des fréquences standardisées internationalement et peuvent être placés sur un grand nombre de supports, rendant caduque la carte proprement dite. On a alors affaire à une technologie désignée sous le vocable d'identification par fréquence radio (RFID, *Radio Frequency Identification*), fonctionnant avec des transpondeurs souvent ultra miniaturisés (certains correspondent à l'épaisseur de trois cheveux et ne coûtent que quelques cents). Ainsi, une pièce de vêtement, une montre ou une bague peuvent servir de système de contrôle d'accès. Le professeur Kevin Warwick, de l'Université de Reading, avait fait la manchette des journaux en 1998 en se faisant implanter un émetteur directement sous la peau d'une épaule. Le système lui permettait de déverrouiller des portes, mettre sous tension l'éclairage et d'autres appareils à son arrivée, etc. Depuis 2003, 160 employés du Procureur général de Mexico portent un implant de ce type sous leur peau, qui leur sert de clé pour se déplacer à l'intérieur des bureaux de l'institution.

Une faille importante de cette technologie est qu'elle exige la coopération et la bonne volonté des détenteurs du matériel — ils ne doivent pas prêter leur transpondeur personnalisé ou l'oublier quelque part (ce qui n'est pas le cas des implants mais ceux-ci restent rares pour l'instant). Les techniques biométriques visent en partie à combler cette faille.

On désigne généralement sous l'appellation de « biométrie » tous les procédés d'identification fondés sur la mesure du corps, dont le premier prototype fut inventé par Alphonse Bertillon à la fin du 19^{e} siècle. Bertillon avait découvert que la mesure combinée de certaines parties du corps humain est unique à chaque individu. À l'origine, le « bertillonnage » servait à déjouer les récidivistes, qui pouvaient blanchir leur dossier criminel en changeant simplement de nom à chaque arrestation. Il fut remplacé par les empreintes digitales lorsqu'on réussit à trouver un moyen de classer celles-ci de façon à pouvoir les consulter systématiquement. Dans ces deux cas, il s'agit de « biométrie » au sens où c'est une caractéristique physique du corps ou d'une de ses parties qui sert à identifier l'individu.

Aujourd'hui les techniques biométriques sont multiples. Les plus répandues sont les empreintes digitales, la mesure des proportions de la main par un lecteur optique, la cartographie des vaisseaux sanguins de la rétine ou des replis de l'iris, l'analyse de la voix et la reconnaissance automatique du visage. En principe chacune de ces techniques permettrait une identification infaillible presque instantanée, mais en pratique des erreurs sont fréquentes, même pour ce qui est des traditionnelles empreintes digitales. De plus, selon la revue en ligne *Computertechnik* (anglais et allemand) plusieurs de ces systèmes sont relativement faciles à déjouer — ce qui n'enlève toutefois rien à leur popularité.

Cet aspect des technologies sécuritaires est crucial : leur adoption procède d'une logique qui accorde un privilège démesuré à l'efficacité en théorie sur l'efficacité en pratique parce que le concept de technologie est indissociable de ceux d'amélioration et de développement progressifs (Leman-Langlois, 2003). En principe, l'efficacité théorique et l'efficacité pratique finiraient inéluctablement par coïncider, ce mouvement de superposition de la théorie et de la pratique constituant la définition même de la technologie.

Si certains systèmes d'identification biométrique sont très coûteux et sont destinés à des applications industrielles, militaires ou à leur adoption par de grandes institutions, d'autres visent au contraire le public en général. Certains lecteurs d'empreintes digitales sont destinés à sécuriser l'accès à des ordinateurs personnels et coûtent moins de 50 (par exemple, les produits Digitalpersona). Non seulement la plupart peuvent-ils être déjoués, mais, comme tout moyen de défense insuffisamment validé, ils peuvent être récupérés à l'avantage de l'attaquant. En effet, on peut d'abord contourner l'obstacle de défense en activant la dernière empreinte laissée sur le lecteur avec un petit sac de plastique rempli d'eau (*Computertechnik*). Chose plus préoccupante encore : un *hacker* mal intentionné pourrait facilement obtenir les empreintes digitales des utilisateurs de tels appareils. Quoi qu'il en soit, notons surtout que la « démocratisation » de ces technologies est un aspect absolument déterminant pour l'étude de leur développement et de leur adoption à grande échelle : si le citoyen adopte ce système chez lui, le choc de le rencontrer ailleurs finira par s'émousser, ce qui favorisera la *normalisation* de ces moyens de contrôle et leur acceptation commune. La Audi A8 reconnaît les empreintes de son propriétaire ; Nokia produit un téléphone portable qui fait la même chose ; Microsoft permet à ceux qui préfèrent ne pas s'encombrer d'une multitude de mots de passe pour utiliser des services internet de simplement utiliser leurs empreintes digitales pour s'identifier. En fait le lecteur séparé n'est déjà plus nécessaire, la technologie pouvant être intégrée à la souris ou au clavier — ainsi, l'identification aura lieu sans que l'utilisateur en ait conscience, sans qu'il ait à poser un geste spécifique comme appliquer son doigt sur un lecteur.

Le contexte pratique du contrôle d'accès impose peu de limites socioculturelles, éthiques ou légales aux technologies d'identification. Le concept même d'accès implique un privilège et non un droit, et comporte naturellement des conditions. De plus, lorsqu'il s'agit d'un contexte de travail, les exigences d'identification peuvent être inclues dans un contrat d'embauche. Dans ce cas, un employé qui refuserait de s'y plier serait tout simplement congédié, ou se verrait refuser promotions et hausses de salaire.

2 Identification à fins commerciales

Dans ce contexte tout autre, l'objectif est la maximisation des profits. L'identification du client se fait pour augmenter sa consommation des biens et services offerts par l'entreprise. Par exemple, on tente de neutraliser son désir de comparer les prix des produits offerts, on l'invite à visiter des lieux (lieux physiques

ou site internet), on lui soumet de nouvelles suggestions d'achats ou, enfin, on l'incite à remplir ses besoins plus efficacement ou plus agressivement.

Ceci est particulièrement évident dans les transactions effectuées sur internet. Premièrement, il existe une multitude de façons de personnaliser la publicité envoyée à l'écran de chaque utilisateur, de manière à se rapprocher le plus possible de ses intérêts personnels. En effet la publicité ordinaire, telle qu'on en voit à la télévision par exemple[1], est très peu efficace sur internet parce que son utilisateur en est beaucoup moins captif et peut simplement choisir de changer aussitôt de page ou de faire disparaître l'encadré publicitaire simplement en faisant défiler le contenu de la page. Contrairement à la télévision dans son format actuel, l'Internet offre des moyens puissants d'individualisation des messages publicitaires à travers l'identification des utilisateurs. Parmi les moyens les plus élémentaires, qui se rapprochent de l'identification sans en être vraiment, on trouve par exemple la publicité présente sur un moteur de recherche comme Google, qui est sélectionnée d'après les termes de recherche introduits par l'utilisateur. C'est le niveau le plus primaire d'identification. Depuis quelques mois Google offre un service de courriel en apparence « gratuit », au sens où son utilisateur ne débourse rien. Ce service présente toutefois à l'écran des messages publicitaires sur mesure en analysant le contenu des courriels des abonnés : par exemple, si vous échangez au sujet de vos vacances, on vous servira des publicités de lignes aériennes. Tout ceci, bien sûr, est conservé dans votre profil d'utilisateur — incluant le fait que vous ayez cliqué sur la publicité présentée ou non.

L'identification commerciale procède par séduction — elle convainc l'utilisateur de s'identifier lui-même et de s'engager à continuer de s'identifier dans le futur en échange d'un avantage quelconque. Dans le cas d'un logiciel multimédia, comme RealPlayer, c'est le logiciel lui-même qui est offert gratuitement. En échange, l'utilisateur permet à l'entreprise de construire un profil de ses goûts musicaux. Dans le cas des cartes « fidélité » le client accepte de revenir au même endroit pour faire ses achats en échange d'un rabais qui lui sera consenti. En utilisant sa carte, le consommateur s'identifie et aide l'entreprise à bâtir son profil de consommation. Les stations-service offrent à leurs clients des appareils qui leur permettent de faire le plein et de partir « sans payer » — l'appareil est un transpondeur qui les identifie automatiquement et place leur achat sur leur compte personnel. L'entreprise fait également un profil de sa consommation d'essence (quantité, fréquence, lieux où il s'est arrêté) qui servira à des fins commerciales et publicitaires. Le même genre de technologie est également utilisé par les ponts et les routes à péage.

La technologie RFID envahit déjà l'espace commercial, où on l'utilise pour fins d'inventaire, surtout en entrepôt mais bientôt en magasin. Les produits en étalage pourront « parler » à leurs étagères intelligentes, signaler leur présence ou leur mouvement dans tout le magasin. Le client, en se déplaçant dans les rayons, informera l'ordinateur central de ses choix, de la quantité, rapidité et séquence de

[1] Déjà dans ce contexte, les périodes de publicité sont achetées en fonction du public ciblé par le produit et du profil de l'auditoire de l'émission pendant laquelle on diffuse le message publicitaire. C'est ce qu'on pourrait appeler une identification de masse.

ses achats ; il passera ensuite à la caisse sans s'arrêter, ses achats étant enregistrés automatiquement et classés dans son profil personnel. La prochaine étape technologique, toute proche de nous, consistera à reconnaître ce même client à sa prochaine venue, parce que ses vêtements porteront toujours leur étiquette RFID individualisée.

Le monde du commerce comprend quelques restrictions de plus que celui du travail dans l'utilisation des techniques d'identification, surtout à cause des associations de consommateurs. Ces dernières pourraient estimer que certaines pratiques sont abusives et violent la vie privée des clients. Néanmoins, comme nous l'avons souligné, l'entreprise peut facilement « séduire » le client en lui offrant un avantage quelconque en échange, par exemple, de porter en permanence les puces d'identification radio. Notons qu'à partir du moment où une masse critique d'individus consentent à être identifiés, ceux qui restent sont identifiés *de facto* comme clients difficiles.

3 Identification judiciaire

L'identification judiciaire utilise depuis longtemps les empreintes digitales pour prouver certains faits relatifs à des infractions criminelles, dont la présence de l'accusé en un lieu, le fait qu'il ait touché un objet ou une personne, etc. La science des empreintes digitales a beaucoup progressé et permet maintenant, dans certaines conditions, de relever des empreintes même quand le malfaiteur portait des gants. Mais les plus grands progrès se font à deux niveaux. Le premier est celui de la conservation et de l'analyse des résultats — autre conséquence des avancées rapides de l'informatique. La quantité des empreintes comparées et la rapidité avec laquelle les résultats sont connus se sont multipliées depuis les 10 dernières années. Le second niveau est légal : dernièrement, plusieurs pays ont amendé les lois qui régissent la cueillette et la conservation d'empreintes digitales, ce qui fait que de plus en plus de citoyens peuvent être identifiés de la sorte.

La plus grande percée récente en matière d'identification judiciaire est sans aucun doute l'analyse de l'ADN. En permettant à la fois d'innocenter des détenus condamnés pour des crimes affreux et de trouver les coupables de crimes anciens restés sans solution, l'ADN a été souvent présenté dans les médias comme la baguette magique qui abolirait la possibilité même d'une erreur judiciaire, assurant des verdicts scientifiquement vérifiables et, par voie de conséquence, des sentences objectivement justifiées.

Nonobstant l'enthousiasme médiatique, notons que l'identification par ADN prend de plus en plus d'ampleur et que presque tous les pays occidentaux ont des bases de données contenant des milliers, sinon des millions de signatures génétiques. En France le ministère de l'Intérieur vise à meubler son Fichier national automatisé des empreintes génétiques (FNAEG), qui ne contient que très peu d'information (moins de 10 000 fichiers), et a utilisé l'ADN de personnes déjà détenues pour ce faire (Statewatch, 2004). La Banque nationale de données génétiques (BNDG) du Canada contient 65 000 profils, qui seront conservés pour une durée indéterminée. La palme revient toutefois au Royaume-Uni, qui détient

le profil génétique de près de trois millions de ses citoyens, et vient tout juste d'élargir une fois de plus les conditions dans lesquels un échantillon peut être légalement recueilli et conservé par la police, permettant le prélèvement à l'arrestation et la conservation même si le suspect est relâché sans procédures.

On donnera un exemple du zèle britannique. Les transports en commun du Royaume-Uni sont soumis à une mauvaise épreuve : les conducteurs de bus et autres membres du personnel du transport de surface se font (physiquement) cracher dessus, cette pratique étant avec justice perçue comme ignoble par les Britanniques. Dorénavant, les employés du transport en commun seront munis d'un instrument « avaleur de crachats » (*gob gobbler)* qui recueillera des échantillons de glaviots. On procédera ensuite à une analyse de la signature ADN contenue dans ces échantillons ; celle-ci sera comparée aux signatures de la banque de données et les contrevenants seront en théorie appréhendés.

En l'absence de suspect précis, l'identification par l'ADN n'est limitée que par le nombre d'échantillons dans la banque de données — le système parfait contiendrait *tous* les profils individuels d'une population. C'est exactement ce qui est recommandé par l'inventeur du système britannique, le professeur Alec Jeffreys de l'Université de Leicester (R-U ; New Scientist, 2002). Dès 1987, le principe de ce qu'on pourrait appeler le « filet génétique » fut mis en pratique au Royaume-Uni, avec la collecte d'échantillons de plus de 5 000 citoyens mâles de trois villages avoisinant la résidence de deux adolescentes qui avaient été violées et tuées. La police allemande a également eu recours à ce genre de filet dans le passé, et la chose devient de plus en plus courante aux États-Unis. La police de Toronto a utilisé des filets dans au moins trois affaires récentes, demandant aux citoyens du voisinage des victimes de consentir à donner un échantillon d'ADN. Légalement, dans la plupart des cas le citoyen doit donner son consentement à la prise d'un échantillon, mais le refus de coopérer le place automatiquement sur la liste des suspects (cette situation se compare au refus de se soumettre à un test d'alcool). En général, ces filets génétiques sont très peu productifs (Police Professionalism Initiative, 2004) — peu d'affaires sont effectivement résolues de cette façon — mais les échantillons s'accumulent et ainsi de plus en plus de citoyens ont un fichier génétique à leur nom dans les ordinateurs de la police.

On ne mentionnera que par souci d'exhaustivité le « *profilage criminel* », qui doit sa popularité surtout aux romans de l'auteur Thomas Harris, qui a créé le personnage sulfureux d'Hannibal Lecter, à la fois tueur en série et consultant pour les « profileurs » du FBI. Grâce aux adaptations cinématographiques de ces romans, les personnages de Thomas Harris ont capturé l'imagination des masses et suscitent des vocations enthousiastes parmi les jeunes. Le profilage criminel est, de l'aveu même des experts du FBI, une pratique où la réalité de l'enquête policière et l'inspiration qu'elle reçoit de la fiction policière sont indissociables (Douglas et Olshaker, 1995[2] ; Ainsworth, 2002.). Le profilage n'est pas, comme tel, une technique d'identification. Il vise moins à l'identifier un individu mais qu'à

[2] John Douglas est un nagent du FBI qui est co-auteur de manuels sur l'enquête policière, alors que Mark Olshaker est l'auteur de nombreux romans policiers. Ils ont uni leurs efforts pour écrire un ouvrage sur le profilage criminel.

réduire le bassin des suspects, que les policiers doivent explorer pour procéder à l'identification d'un tueur en série (on cherchera, par exemple, un individu du sexe masculin, de peau blanche et dont l'âge se situerait entre vingt en trente ans). Beaucoup de policiers font du profilage comme Monsieur Jourdain faisait de la prose, l'indice du sexe masculin étant, par exemple, une donnée automatique, puisque que les tueurs en série sont des hommes, à très peu d'exceptions près.

À notre époque sécuritaire, la collecte d'information facilitant l'identification de contrevenants réels, d'individus suspects ou constituant des dangers potentiels ne choque plus l'opinion. L'ère est aux grands moyens pour contrôler le crime et le terrorisme (Garland, 2001). C'est un secteur économique où les investissements tant publics que privés sont en croissance.

4 Identification et contrôle du comportement

Le parc d'attractions Legoland, au Danemark, offre aux parents de placer un bracelet électronique au poignet de leurs enfants afin de pouvoir les retracer au mètre près sur la propriété. À l'extérieur des parcs d'attractions, les parents peuvent équiper leurs enfants de médailles (conçues à l'origine pour les animaux de compagnie) qui permettent de les retrouver par localisation satellite. Les ados seront sans doute sensible à l'utilisation du téléphone portable à localisation GPS (*Global Positioning System* ; par exemple, *GPS Anywhere*) pour contrôler leurs mouvements. Cette technologie permet aux parents de savoir en tout temps où se trouve leur progéniture (ou du moins, le téléphone correspondant) en entrant un mot de passe sur un site internet. Cette technologie est également vendue aux entreprises pour enregistrer et surveiller les déplacements de leurs employés.

Une autre industrie en essor ces dernières années est celle de la surveillance électronique de personnes sous contrôle pénal : personnes assignées à résidence, interdites de séjour ou d'approche de certains lieux, en peine de sursis, en libération conditionnelle ou en attente de procès. L'automatisation complète de ces systèmes, combinée à l'utilisation du système GPS, permet un niveau de surveillance personnalisée sans précédent. Les autorités peuvent non seulement s'assurer que le justiciable est présent à un endroit désigné au moment voulu, comme c'était le cas des premiers balbutiements de cette technologie. Désormais, des ordinateurs peuvent garder une description complète des déplacements d'un l'individu en surveillance; ils peuvent également signaler en temps réel s'il prend une voiture, un autobus ou s'il marche à pied (selon sa vitesse et la correspondance de son trajet à celui des transports en commun) et signaler, enfin, s'il fait régulièrement des détours pour passer près d'une école ou de l'appartement de son ex-femme, combien de fois il visite son avocat et combien de temps il passe avec lui, et ainsi de suite. Au regard de la technologie disponible, rien n'empêche l'utilisation du bracelet de surveillance pour prendre le pouls de celui ou celle qui le porte, pour enregistrer les réactions électriquement mesurables de sa peau (procédé typique du détecteur de mensonges) ou d'enregistrer les sons environnants.

Dans tous ces cas la surveillance individuelle est appliquée à des personnes en manque d'autonomie (enfants, malades, personnes âgées), des employés ou

des justiciables, des personnes qui sont légalement subordonnées (par contrat ou par la loi) à d'autres. La légitimité de tels contrôles est donc relativement facile à défendre et devrait trouver plusieurs preneurs.

5 Surveillance de proximité : Identification et surveillance géographique

La plupart des pays du monde utilisent une forme ou une autre de carte d'identité (souvent appelée « carte » même s'il s'agit d'un livret de type passeport), à des fins multiples — services sociaux, imposition, identification légale, etc. Toutefois, pour constituer une mesure réellement efficace, une carte servant au contrôle et à la surveillance doit être obligatoire et les forces de l'ordre doivent avoir le pouvoir de l'exiger à tout moment. La France, la Belgique, l'Allemagne, l'Espagne et d'autres pays ont établi depuis longtemps ou récemment des programmes de carte nationale, mais la possession et le port de la carte restent ne sont pas obligatoires dans un grand nombre de pays[3]. Le Canada, les États-Unis, l'Australie et autres pays de droit coutumier anglo-saxon n'ont pour l'instant aucune forme de carte d'identité nationale. Le citoyen canadien, par exemple, doit produire son « numéro d'assurance sociale » à diverses fins, mais cette production n'est obligatoire que pour fins d'emploi et d'imposition. Il n'y a aucun autre contexte où il soit tenu de s'identifier.

Le Canada, le Royaume-Uni et les États-Unis débattent aujourd'hui des avantages et désavantages d'adopter une carte d'identité nationale obligatoire. Au Canada, la carte d'identité récemment proposée par le gouvernement fédéral devrait de plus porter de l'information biométrique (empreintes digitales ou autre). Le ministère britannique de l'Intérieur (*Home Secretary*) se propose d'instaurer une telle carte d'identité avant 2010 ; cette carte lierait son propriétaire à son profil dans une banque nationale de données génétiques, comme il faut s'y attendre en ce pays. L'obtention et le port d'une telle carte seraient initialement volontaire mais pourrait devenir obligatoire dans les années suivantes. La Chine dispose déjà d'un tel programme, visant à contrôler les allées et venues des citoyens d'une province et d'une ville à l'autre.

Il ne faudrait pas oublier la forme classique d'identification légale qu'est le passeport, dont l'usage obligatoire s'est rétréci. Plusieurs de ces contextes ont en effet disparu, comme par exemple lors du passage des frontières à l'intérieur de la Communauté européenne, où le passeport n'est plus exigé. En fait, le passeport est en train d'y être fonctionnellement remplacé par les cartes d'identité nationales et par la conservation et l'analyse des données personnelles des voyageurs aériens. Dans une large mesure c'est seulement la modalité de contrôle des voyageurs qui change et devient moins perceptible. Cela dit, le passeport n'est pas près de disparaître, et son contenu sera modifié par la technologie de l'identification. Le passeport du futur contiendra sans doute plusieurs types de données biométriques et, probablement, génétiques.

[3] Ce texte fait état de façon générale de développements dans les pays anglo-saxons. Pour un travail en profondeur sur l'histoire de la carte nationale d'identité en France, par exemple, on consultera le récent ouvrage de Pierre Piazza (2004).

Quand l'objectif de l'identification est de contrôler et de surveiller un espace, on ne peut tenir compte du consentement ou non de ceux qui y sont présents. En effet, un système de surveillance dépendant de l'adhésion volontaire de ceux qui y sont soumis ne peut par définition remplir ses fonctions, car on peut vraisemblablement supposer que le délinquant potentiel ou le citoyen recherché par la police seront les premiers à se soustraire au contrôle. La mise en application d'un tel système implique donc l'obligation de ne pouvoir s'y soustraire et le recours à des mesures coercitives pour contraindre les récalcitrants. Ces mesures coercitives pourraient être d'un type « soft » et obtenir qu'on s'y conforme pour profiter d'avantages collatéraux, à l'instar des pratiques du secteur privé. Cette coercition douce pourrait consister dans la privation de services gouvernementaux pour ceux qui ne détiennent pas la carte leur permettant d'en bénéficier. Insistons à cet égard sur le fait que plusieurs projets de cartes nationales présentent comme un avantage de ce modèle la « simplification » des relations du citoyen avec son gouvernement. La carte d'identité servirait ainsi pour les services sociaux, la santé, les déplacements aériens, et pourrait par exemple remplacer le permis de conduire; ceux qui choisiraient librement de ne pas se la procurer devraient également se passer des bénéfices correspondants. Ce raisonnement peut être étendu aux pays qui disposent déjà d'une carte d'identité nationale, comme la France : les informations que la carte en vigueur contient déjà pourraient être enrichies de façon abusive sous le prétexte que cet enrichissement facilite l'accès aux services gouvernementaux et leur « rationalisation ».

Toutefois, la question du consentement (effectif ou extorqué) est peut-être déjà caduque, grâce encore à la technologie moderne. Il se trouve que la surveillance peut aisément être exercée à travers des procédures de reconnaissance d'identité sans que ceux qui y sont soumis s'en aperçoivent et sans qu'elle ne requière d'action consentante de leur part. C'est le cas des systèmes d'identification à distance, principalement par reconnaissance du visage (des systèmes de reconnaissance de la démarche sont également en développement). À l'heure actuelle, la reconnaissance du visage fonctionne à condition que le propriétaire du visage coopère : ne pas bouger, faire face à la caméra et ainsi de suite. Cette situation ne durera pas : un nombre considérable d'entreprises, d'universités et d'agences gouvernementales (surtout militaires) s'affairent à perfectionner ces technologies, partout dans le monde (Leman-Langlois, 2003). De nombreux systèmes permettant de reconnaître des individus dans des foules ont déjà été testés, vendus et utilisés, surtout au Royaume-Uni et aux États-Unis. Que leur efficacité ait jusqu'ici laissé à désirer ne devrait pas occulter le fait que l'argumentaire justifiant leur adoption est déjà bien reçu : seuls ceux qui ont quelque chose à se reprocher s'opposent à la perte de leur anonymat.

L'enjeu le plus controversé au regard des problématiques de l'identification - la reconnaissance automatique des individus *sur la voie publique* - est à portée de main d'une capture politique autoritaire. En effet, le public accepte facilement qu'un agent de sécurité surveille ses allées et venues dans un parking souterrain pour assurer sa sécurité et faire obstacle à un agresseur potentiel. Il y a peu de raison de limiter cette logique aux lieux privés, si le danger déferle dans les espaces publics et que la technologie préventive est d'emblée disponible.

6 S*urveillance à distance : Intégration et exploration des données (*data mining*)*

On pourrait tenter de concevoir l'exploration en profondeur des données comme un essai de rendre le monde parfaitement transparent, mais uniquement pour des machines programmées à n'exercer que des fonctions de stockage et d'inspection de données. Le fait que seul un œil mécanique percerait les cloisons de la vie privée constituerait une réponse à la plupart des objections ordinaires contre l'intrusion d'un tiers dans l'intimité des citoyens, puisqu'en pratique la vie privée continue de n'être connue de *personne* (voir Brodeur et Leman-Langlois, 2004). Cette affirmation n'est paradoxale qu'en apparence. Les fonctionnaires de l'impôt ont déjà accès à des informations que nous considérons presque tous comme très sensibles sans qu'on s'en inquiète véritablement, car l'État garantit que ces informations ne seront utilisées que pour les fins étroites qui leur sont assignées, à savoir le contrôle de la perception des impôts. Cette garantie serait généralisée dans le cas de l'exploration en profondeur des données : la machine à l'œil à tout, mais elle ne peut produire un signalement pour des intervenants en sécurité qu'en suivant un protocole précis, dont le contenu aurait préalablement fait l'objet d'un débat public ou parlementaire.

L'exploration de données ne vise pas au premier chef à établir l'identité d'un individu, mais à le classer selon son niveau de risque sécuritaire. Elle passe par la construction de biographies informatisées, formées à partir des traces informatiques laissées par les activités des citoyens et de tous ceux qui résident, ne serait-ce que pour une période transit, sur un territoire national. Elle active donc une description aussi exhaustive que possible, qui est appariée à un nom : quand un individu doit décliner son identité, sa biographie devient potentiellement disponible, dans l'instant. Sans toutefois que le fonctionnaire devant lequel une personne s'identifie ait besoin d'avoir accès au contenu de sa biographie, le système d'exploration en profondeur pourra déclencher une alarme selon des standards programmés à l'avance. Certains de ces standards sont conventionnellement admis depuis longtemps, comme la recherche d'un suspect ou d'un condamné en fuite. À ceci s'ajoute toutefois d'autres éléments déclencheurs d'alarme entièrement nouveaux, issus des plus récents développements de l'informatique. Ils tiennent dans l'identification de patterns ou de séquences d'actions dont l'étude a révélé qu'ils révélaient un risque statistique. Par exemple, le pattern suivant : une personne a acheté une arme, le billet d'avion qu'elle tente de se procurer est un aller simple, elle veut payer son passage en argent comptant, une autre personne avec laquelle elle est en contact fréquent a été portée sur une liste de suspects terroristes et ainsi de suite.

Le fondement de tout programme d'exploration de données est la masse des données elles-mêmes : plus elles sont étendues, plus l'exploration est efficace. En mai 2000, le ministère fédéral canadien du Développement et des Ressources humaines démantelait, à la suite d'un tollé de protestations, son *Fichier longitudinal sur la main-d'œuvre*. Celui-ci contenait 2 000 items d'information sur 34 millions de canadiens vivants et décédés (c'est-à-dire qu'aucune information n'était jamais retirée de la banque, même à la mort du sujet ; voir Commissaire à la protection

de la vie privée du Canada, 2000). Cette forme primitive de découpage de la vie privée, qui rappelle *1984* de George Orwell, est probablement en voie de disparition car la révélation de l'existence de ce type de banque de données suscite un scandale. L'exploration en profondeur de données qui procède en couplant l'inspection mécanique avec une action enclenchée par un signalement fondé ne prêterait pas, d'après ceux qui la préconisent, un flanc aussi large à des critiques normatives de tous ordres.

Au début 2002 on révélait dans la presse que le ministère de la Défense des États-Unis était à mettre sur pied un programme massif d'exploration de données appelé *Total Information Awareness* (TIA ; voir Brodeur et Leman-Langlois, 2004). En principe, une méta-banque de données allait former le cœur du programme et elle devait contenir des informations de sources très variées, dont *toutes* celles décrites précédemment dans cette note de recherche, incluant même les profils de consommation des individus. La méfiance initiale que suscitait ce projet se cristallisa sur sous-programme où on se proposait d'utiliser les « lois du marché » boursier pour prédire des événements politiques dans le monde, en invitant les participants à investir leur argent dans un marché à terme d'événements tels que l'assassinat de personnalités ou l'effondrement de régimes. C'est à la suite de ce scandale que les parlementaires étatsuniens firent rayer tous les programmes liés au TIA bien qu'on l'eût habilement renommé *Terrorism Information Awareness* du budget de la défense. Il faut toutefois y insister, la spéculation boursière sur des crises humanitaires potentielles souleva beaucoup plus d'indignation que les technologies sophistiquées d'identification développées sous le programme TIA.

Un autre projet, nommé CAPPSII (*Computer Assisted Passenger Prescreening System*) et visant plus spécifiquement la sécurité aérienne, a aussi été aboli aux États-Unis, en partie parce que les compagnies aériennes hésitaient à y participer, et parce que le *General Accounting Office* du Congrès avait estimé, en février 2004, qu'il violait sept des huit principaux standards définissant la vie privée (GAO, 2004). CAPPSII classait les passagers selon leur risque sécuritaire et le besoin de les contrôler de plus près avant leur embarcation. La classification était le résultat d'une analyse de plusieurs banques de données fédérales et privées. CAPPSII est déjà remplacé par « Secure Flight », le dernier né de la *Transportation Safety Administration*, limité pour l'instant à comparer des listes de passagers à des listes de personnes à risque maintenues par le FBI.

Malgré la disparition de tels projets, les technologies impliquées restent bien réelles et continuent d'être développées ailleurs. L'équivalent européen de CAPPSII, le programme d'identification des passagers, comparera les noms des voyageurs à plusieurs listes compilées par la police et conservera les données de leurs allées et venues pour un certain temps, après quoi, en principe, elles seront détruites — sauf si une organisation policière européenne et peut-être aussi le FBI désire les obtenir et justifie le besoin de les conserver.

Il faut prévoir qu'une argumentation au profit de la mise en réseau des moyens technologiques d'identification au sein d'une méta-banque de données (une banque de banques) se fera bientôt entendre d'une façon de plus en plus fréquente. L'intégration des technologies d'identification et des informations qu'elles recueillent en décuplerait l'efficacité et l'on fera valoir qu'il serait

irresponsable de se priver d'un tel outil dans la lutte contre le terrorisme international (tout comme le célèbre avocat états-unien Alan Dershowitz[4] (2002) prône déjà qu'on a tort de se priver du recours à la torture). La problématique de cette interconnexion sera présentée sous un angle technologique : les bases de données et les systèmes d'analyse sont souvent incompatibles et leur « interopérabilité » dépendra de prouesses informatiques coûteuses qui éclipseront dans l'esprit des « décideurs » les questions éthiques, juridiques et sociopolitiques, surtout si d'autres attaques terroristes d'envergure devaient se produire.

Sources :

Ainsworth, Peter B. (2002), *Offender Profiling and Crime Analysis*, Cullompton (UK), Willan Publishing.

Alien Technology, www.alientechnology.com.

Banque nationale de données génétiques (BNDG), www.nddb-bndg.org/francais/main_f.htm.

Brodeur, Jean-Paul et Stéphane Leman-Langlois (2004, sous presse), « La surveillance totale », *Cahiers de l'IHESI*.

Commissaire à la protection de la vie privée du Canada (2000), *Rapport annuel 1999-2000*, Ottawa, Ministre des Travaux publics et Services gouvernementaux Canada, www.privcom.gc.ca/information/ar/02_04_08_f.asp.

Computertechnik, http://www.heise.de/ct/english/02/11/114.

Dershowitz, Alan (2002), *Why Terrorism Works. Understanding the Threat and Responding to the Challenge*, New Haven, Yale University Press.

Digitalpersona, www.digitalpersona.com.

Douglas, John and Mark Olshaker (1995), *Mind Hunter. Inside the FBI's ,*New York, Scribner.

Garland, David (2001) *The Culture of Control*, Chicago, University of Chicago Press.

General Acounting Office (GAO, É-U), *Aviation Security : Computer-Assisted Passenger Prescreening System Faces Significant Implementation Challenges*, www.gao.gov/new.items/d04385.pdf.

GPS Anywhere, www.gpsanywhere.com.tw.

Leman-Langlois, Stéphane (2003), « The Myopic Panopticon: the Social Consequences of Policing Through the Lens », *Policing and Society*, 13 (1), 43-58.

New Scientist (2002), « DNA Database "Should Include Every Citizen" », 12.09.02, www.newscientist.com/news/news.jsp?id=ns99992792.

Panasonic Biometrics, www.panasonic.com/business/security/biometrics_access.asp.

[4] Cet ouvrage qui préconise l'usage des la torture aux États-Unis a été endossé avec enthousiasme par M. Elie Wiesel, prix Nobel de la paix, dont les propos sont reproduits pour faire la publicité du livre.

Piazza, Pierre (2004), *Histoire de la carte nationale d'identité*, Paris, Odile Jacob.
Police Professionalism Initiative (2004), *Police Dna "Sweeps" Extremely Unproductive : A National Survey of Police DNA "Sweeps.* Omaha (Nebraska), Department of Criminal Justice of the University of Nebraska. www.acluva.org/publications/dnasweepstudy.pdf
RFID Journal : www.rfidjournal.com.
Statewatch (2004), « Prisoners' DNA Samples Entered Into Database », 14 (1), 4.
Warwick, Kevin, *Project Cyborg*, www.rdg.ac.uk/KevinWarwick/html/project_cyborg_1_0.html.