

Un rapport sur la société de la surveillance

Rapport préparé par le *Surveillance Studies Network* à l'intention du
Commissaire à l'information

Document de discussion publique

Septembre 2006

Rédaction :

David Murakami Wood et Kirstie Ball

Matériel de recherche :

Louise Amoore
Kirstie Ball
Steve Graham
Nicola Green
David Lyon
David Murakami Wood
Clive Norris
Jason Pridmore
Charles Raab
Ann Rudinow Saeftnan

Londres 2016 : Tout est sous contrôle¹

Comme tous les autres participants à la manifestation antiguerre qui se déroule au cœur de Londres, Ben Jones, 18 ans, fait l'objet d'une surveillance constante. De petits UAV (avions sans pilote) tournent au-dessus de leurs têtes². Ces avions espions ont fait leurs débuts lors des Jeux Olympiques de 2012 et le « succès » de ce que les publicités décrivent comme un « regard amical venu du ciel » suffit à justifier leur utilisation continue aux yeux du maire de la ville³. Les gens ne les remarquent pratiquement plus. De minuscules caméras intégrées dans les lampadaires et les murs au niveau des yeux et en hauteur permettent une utilisation plus efficace des systèmes de reconnaissance faciale désormais universels.⁴ Les logiciels de morphage qui combinent les images provenant de différentes caméras pour produire une image tridimensionnelle sont également en cours d'essai, et ce en dépit des protestations des militants et des avocats pour qui ces images manquent de précision et ne sont pas « réelles ». Grâce à des réseaux sans fil virtuellement omniprésents, les caméras sont dépourvues de boîtiers encombrants et de câbles. Ces réseaux sont en outre reliés à un éclairage public intelligent, qui procure des conditions d'éclairage « idéales » pour la reconnaissance faciale, ainsi qu'à des projecteurs automatiques et des caméras supplémentaires, qui se déclenchent en cas de mouvement « inhabituel ». Bon nombre de bâtiments officiels, qui étaient entourés de barricades en béton depuis 2001, sont à nouveau visibles, mais sont désormais protégés par toutes sortes de capteurs reliés à des barricades automatiques impénétrables qui s'enfoncent dans le sol lorsqu'elles ne sont pas utilisées.

Alors qu'ils se dirigent vers le métro, Ben et son ami Aaron pénètrent accidentellement dans la zone d'exclusion de Westminster. Ils sont arrêtés par des agents de sécurité privés, employés par le Westminster Business Improvement District (BID)⁵, et supervisés à distance par des opérateurs de la police via des ordinateurs de poche⁶ et des micro-caméras montées sur les casques, qui scannent les deux garçons⁷. Ben fournit l'habituel échantillon d'ADN qui est analysé instantanément et tend sa carte d'identité à micropuce. A la lecture des données qui s'affichent sur l'écran, le policier plaisante : n'est-il pas ironique qu'un militant anticapitaliste ait récemment passé ses vacances aux Etats-Unis⁸ ? Ben grimace poliment. Les cartes d'identité ne sont toujours pas obligatoires, et Aaron qui vient d'une famille ultra-chrétienne, refuse d'en avoir une. Sa mère y voit là « la marque de la bête ». Aaron, lui, voudrait simplement qu'on le laisse tranquille. Car cela complique son existence : sans carte d'identité, Aaron sait qu'il ne pourra jamais travailler pour le gouvernement ni toucher des allocations ou même un prêt étudiant. Et il lui est interdit de voyager en avion ou sur les grandes lignes de train, même en Grande-Bretagne. Il commence à se demander si tout ça en vaut la peine ! Les choses sont en outre sur le point de se compliquer pour lui : en raison de la couleur de sa peau (il est noir) et en l'absence de carte d'identité, Aaron affiche un profil de risque élevé pour la police. Le QG de la police ordonne au personnel de sécurité de l'amener au poste afin qu'il puisse y être interrogé⁹...

Ce scénario fictif, censé se dérouler en 2016, n'est pourtant pas si éloigné de la réalité actuelle !

En 2004, Richard Thomas, le commissaire à l'information chargé par le parlement de surveiller l'usage de nos données personnelles, avertissait que nous étions « en passe de glisser vers une société de la surveillance, tels des somnambules¹⁰ ».

Le fait est que nous vivons déjà dans une telle société :

- Les caméras vidéo nous observent en permanence : dans les immeubles et les rues commerçantes, sur la route et dans les quartiers résidentiels. Les systèmes automatiques sont aujourd'hui capables de reconnaître les plaques minéralogiques (et de plus en plus souvent les visages).
- L'usage de bracelets électroniques permet de surveiller les mouvements des personnes en liberté provisoire. Toute personne arrêtée par la police doit fournir un échantillon d'ADN, qui est ensuite conservé qu'elle soit ou non reconnue coupable. Des efforts sont également entrepris pour identifier de plus en plus tôt les « tendances criminelles ».
- Nous sommes constamment invités à nous identifier, qu'il s'agisse de recevoir des allocations sociales, des soins de santé, etc. Le gouvernement envisage aujourd'hui d'adopter un nouveau système de cartes d'identité biométriques dont certains paramètres (empreintes digitales et image de l'iris), seraient reliés à une gigantesque base de données personnelles.
- A chaque fois que nous nous rendons à l'étranger, notre identité, notre destination et nos bagages font l'objet d'un contrôle et d'une surveillance accrue et les informations recueillies sont stockées. Nos passeports sont eux aussi en train de changer d'aspect et sont désormais équipés de micropuces ; tout comme pour les cartes d'identité, il est aujourd'hui question de passeports biométriques.
- Bon nombre d'écoles utilisent des cartes à puce intelligentes et des systèmes biométriques pour surveiller les déplacements des enfants, leur alimentation ou les livres qu'ils empruntent à la bibliothèque.
- Nos dépenses quotidiennes sont analysées par des logiciels, et les données collectées sont ensuite vendues à toutes sortes d'entreprises. La célérité des centres de service et la palette des offres – prêts, assurances ou emprunts – dépendent en grande partie de notre pouvoir d'achat, de notre lieu de résidence et de notre identité.
- Nos appels téléphoniques, nos courriels et l'usage que nous faisons d'Internet risquent en permanence d'être interceptés et analysés par les services de renseignement britanniques et américains selon qu'ils contiennent certains mots ou expressions clés.
- Nos performances et notre productivité au travail sont de plus en plus étroitement surveillées et les organisations qui nous emploient s'intéressent de plus en plus à notre vie privée¹¹.

La société de la surveillance est devenue réalité sans que nous n'y prenions garde.

Elle est la somme totale d'un vaste ensemble de nouvelles technologies, de décisions de police et de développements sociaux. Certains de ces aspects sont essentiels pour fournir les services dont nous avons besoin, notamment en termes de santé, de prestations sociales et d'éducation. D'autres sont plus douteux. D'autres encore sont totalement injustifiés, intrusifs et oppressifs. L'opinion du public peut être partagée, mais très peu de gens sont en fait conscients de l'existence de cette société de la surveillance, et celle-ci relève pour eux plus de la science-fiction que de la vie quotidienne. Ce qui explique la quasi-absence de débats publics autour de ce sujet. L'industrie de la surveillance représente un chiffre d'affaires pharamineux et sa croissance est aujourd'hui bien supérieure à celle des autres secteurs d'activité (surtout depuis les attentats du 11 septembre 2001)¹². La valeur de ce secteur dans le monde est estimée à près de 1 trillion de dollars US, et couvre un vaste éventail de biens et de services, allant du matériel militaire aux caméras de télévision en circuit fermé et aux

cartes à puces. La société de la surveillance est devenue lentement, subtilement et imperceptiblement une réalité, à la manière de petits sentiers qui à force de se rejoindre de façon imprévue se seraient peu à peu transformés en route, route dont il convient aujourd'hui de discuter et de débattre d'urgence.

Nous prenons soin de vous

Geeta est âgée de 69 ans et vit seule dans son appartement. Outre des détecteurs de mouvement d'urgence dans toutes les pièces, sa salle de bains est équipée d'un appareil de surveillance de la fréquence cardiaque, ses toilettes sont dotées d'un système de mesure du taux de glycémie et sa cuisine comporte différents capteurs chargés de détecter les fuites de gaz, les incendies et les fuites d'eau. Elle dispose d'un bouton d'alarme relié au centre d'appels municipal, qui la rappellerait et vérifierait instantanément son état de santé si le bouton venait à être actionné. Ses proches sont confortés par la présence de ces capteurs et de ces caméras dans son appartement et savent qu'elle est en sécurité : ils lui rendent donc moins souvent visite que par le passé, et Geeta se sent quelque peu isolée. Elle apprécie cependant les scanners RFID (identification par radiofréquences) qui équipent son réfrigérateur et ses placards : à chaque fois que le niveaux de ses provisions diminuent, l'ordinateur de gestion ménagère passe une commande en ligne automatique auprès du supermarché local. Geeta qui a opté pour un contrat de livraison à domicile n'a même pas besoin de sortir de chez elle. Elle bénéficie également de check-up médicaux réguliers. Mais le NHS (ou National Health Service, l'équivalent de la sécurité sociale française) compare constamment à son insu les résultats de ses analyses à ceux d'autres femmes du même âge provenant des autres régions régionales de la santé du pays.¹³ Le NHS peut ainsi mieux déterminer les facteurs de risque et prédire par exemple avec beaucoup plus de précision les risques de crise cardiaque. Résultat : Geeta, qui affiche un risque de cardiopathie élevé, se voit offrir des conseils nutritionnels. Mais la situation se complique : le NHS refuse continuellement de vastes sommes d'argent que les compagnies d'assurance lui font miroiter en échange de l'accès à des informations de santé selon le principe du « besoin de savoir ». Face à un manque de ressources chronique, ces offres sont de plus en plus tentantes, mais les administrateurs du NHS redoutent un scandale, tel que celui qu'a connu l'Islande, où toutes les bases de données ADN ont été vendues à des entreprises privées à des fins de recherche et de profit privé.¹⁴

Inconvénients de la société de la surveillance

La surveillance ne relève pas d'un malin complot ourdi par une puissance diabolique : elle repose en grande partie sur de bonnes intentions ou du moins sur des intentions neutres comme un désir de sécurité, de bien-être, d'efficacité, de vitesse et de coordination. Certains systèmes de surveillance visent intentionnellement à limiter et à contrôler nos comportements ou mouvements, souvent à notre insu et sans notre consentement. D'autres ont cet effet sans vraiment le rechercher. Ce qui ne signifie pas que tous ces systèmes soient acceptables : il est crucial de bien comprendre les effets de la surveillance ainsi que ses conséquences sur notre vie personnelle et la société en générale.

Nous sommes de plus en plus préoccupés par les risques et les dangers, au lieu de poursuivre des objectifs sociaux plus positifs. Un nombre croissant de situations quotidiennes sont aujourd'hui perçues en termes de « risque », et les mesures qui relevaient autrefois d'une sécurité exceptionnelle sont désormais la norme. Il est cependant rare que nous réfléchissions aux conséquences involontaires d'une telle approche et aux inégalités qu'elle entraîne en termes d'accès

et d'opportunités : non seulement les distinctions de classe, de race, de sexe, d'implantation géographique et de citoyenneté en sont aggravées, mais elles sont aussi devenues une composante intrinsèque des décisions quotidiennes.

Les processus et les pratiques de surveillance contribuent aussi à la création d'un monde, dont nous savons qu'il ne nous fait pas vraiment confiance. La surveillance engendre la suspicion.¹⁵ Les employeurs qui équipent leurs stations de travail d'un enregistreur de frappes au clavier ou leurs véhicules de service de dispositifs de suivi déclarent ne pas faire confiance à leurs employés. L'employé du service des prestations sociales qui recherche les preuves de cumul d'allocations ou interroge les voisins pour savoir si l'assuré fraude affiche son manque de confiance à l'égard de ce dernier. Et les parents qui utilisent des webcams et des systèmes GPS pour surveiller les activités de leurs enfants avouent en fait qu'ils ne leur font pas confiance non plus.

La question fondamentale de cette société de la surveillance est de savoir si nous sommes tellement hypnotisés par le « besoin » de trouver des solutions high-tech aux problèmes de la délinquance, du terrorisme, de la fraude, etc... que nous en oublions de nous demander si ces solutions sont seulement adéquates et s'il existe d'autres réponses non technologiques ou moins envahissantes.

Ce bref document et le rapport complet qui l'accompagne entendent poser pour la première fois ces questions en vue d'inspirer un débat public très nécessaire. Il est possible que nous voulions vivre dans une société surveillée, mais il nous appartient alors de le décider en toute connaissance de cause, et non à la manière de somnambules. Les pages suivantes dressent un portrait détaillé de cette société de la surveillance et de ses conséquences.

Qu'entend-on par « société de la surveillance »

La société de la surveillance est une société dont l'organisation et la structure reposent sur l'utilisation de techniques de surveillance. Ces moyens technologiques lui permettent d'enregistrer les données relatives à nos déplacements et nos activités personnels pour le compte des organisations et des gouvernements qui la structurent. Les informations ainsi recueillies sont alors triées, passées au crible et classées, avant de servir de base à des décisions qui affectent le cours de nos vies. Ces décisions touchent au droit et à l'accès aux prestations sociales, au travail, aux produits, aux services et à la justice pénale ainsi qu'à la santé, au bien-être et à nos mouvements dans les lieux publics et privés.

On trouvera dans les pages suivantes la description de certaines des caractéristiques clés de cette société de la surveillance : la technologie, le flux de données, la convergence, le tri social, le verrouillage technologique et l'échec des technologies.

Technologie

Il est important de garder en mémoire que la surveillance a toujours joué un rôle important à travers l'Histoire et que certains des régimes les plus autoritaires, tels que celui de l'ancienne Allemagne de l'Est, reposaient entièrement sur des moyens aussi peu sophistiqués que des dossiers sur papier et la délation.¹⁶ L'avènement de technologies évoluées a cependant modifié le concept de surveillance. Les nouvelles technologies de surveillance sont plus compactes et plus puissantes, et permettent de recueillir et de stocker une foule d'autres informations, reliées entre elles et instantanément disponibles. Ce document ne saurait couvrir toutes les technologies de surveillance existantes ni tous les domaines d'application de ces technologies. Il entend plutôt souligner les changements essentiels qui sont intervenus dans cinq secteurs particuliers : les bases de données, les télécommunications, les télévisions à circuit fermé, la biométrie et les technologies de repérage et de suivi.

Les bases de données

Les bases de données informatiques sont le fondement même de toutes les nouvelles technologies de surveillance. Elles permettent de recueillir, tabuler et référencer de vastes volumes de données de manière considérablement plus rapide et plus précise que les anciens dossiers sur papier. Les services publics et les entreprises privées s'appuient aujourd'hui sur de gigantesques bases de données personnelles relatives aux citoyens lambda. La comparaison des différents jeux de données permet d'identifier les personnes et les modèles d'activités suspectes. Ces données peuvent être également « exploitées », c'est-à-dire analysées de manière approfondie par le biais de technologies sophistiquées afin de révéler les modèles nécessitant des recherches plus poussées.

Toute transaction laisse une « trace » de coordonnées personnelles, qui renvoie à une personne, un type de personnes ou encore un lieu.¹⁷ Ces transactions englobent pêle-mêle l'utilisation des cartes de crédit, des cartes bancaires, des téléphones portables et d'Internet ainsi que tout achat, recherche ou appel téléphonique. Les programmes de cartes de fidélité, les enquêtes de consommation, les groupes de discussion, les concours promotionnels, les demandes d'informations de produits, les contacts avec les centres d'appels, les « cookies » informatiques, les forums de feedback et les transactions de crédit sont autant de sources de données supplémentaires. A ces informations se superposent souvent des données provenant de sources publiques, telles que les statistiques nationales, les organisations à but non lucratif ou les sociétés de collecte de données spécialisées, qui permettent d'établir des « profils » d'individus ou de communautés. Certaines technologies plus sophistiquées, telles que le « Knowledge Discovery in Databases » (KDD) une méthodologie de création de nouveaux savoirs à partir de bases de données bibliographiques, permettent d'identifier les modèles cachés et de prévoir les transactions futures de façon toujours plus personnelle : c'est ce qui permet à *Amazon.com* notamment de proposer à ses clients des livres ou des DVD susceptibles de les intéresser.¹⁸

Les bases de données constituent un élément essentiel de l'évolution que connaissent aujourd'hui les services publics, et on citera à ce titre le très controversé programme IT *Connecting for Health* du NHS britannique, le plus important projet de ce type en Europe.¹⁹ Ce système connectera les dossiers électroniques des patients et les informations disponibles sur le terrain pour créer une base de données numériques nationale regroupant tous les dossiers médicaux personnels. Quelque deux millions de personnes sont arrêtées chaque année par la police anglaise et galloise. Les empreintes digitales et les échantillons d'ADN sont aujourd'hui prélevés sur la quasi-totalité des personnes arrêtées et conservés dans les bases de données de la police, indépendamment de la culpabilité ou de l'innocence des personnes concernées. Il existe actuellement près de six millions de jeux d'empreintes digitales au sein de cette base de données,²⁰ tandis que la National DNA Database, fondée en 1995, répertorie désormais l'ADN de 3,45 millions de personnes, soit 5,2 % de la population tout entière. Il est intéressant de souligner que 40 % des noirs de sexe masculin figurent aujourd'hui dans cette base de données contre 9 % de blancs et 13 % d'asiatiques du même sexe.²¹ Parmi les autres bases de données de la police, citons le système ANPR de reconnaissance automatique des plaques minéralogiques, le registre des infractions violentes et sexuelles (ViSOR) et un projet de base de données nationale d'images faciales (FIND). Ces systèmes devraient être bientôt reliés au système informatique national de la police (PNC)²² qui sera non seulement accessible depuis tous les postes de police, mais également, grâce au développement du système Airwave de communications numériques de la police, par tout policier dans la rue, par le biais d'un ordinateur de poche.²³

Les frontières nationales sont en passe de se transformer en « frontières intelligentes », où de vastes bases de données vérifient en coulisses les informations relatives aux personnes et à leurs déplacements. Les technologies de profilage sont également utilisées pour établir des listes de surveillance des passagers dangereux ou identifier les groupes potentiellement à risque. D'aucuns suggèrent même ouvertement de hisser le profilage racial au rang de politique officielle²⁴.

La surveillance aux frontières

Pour la famille Jones, de retour de vacances en Floride en 2016, les formalités aux frontières ont considérablement changé. Tout comme dans les pays de l'UE et du G10, les services d'immigration et de contrôle des frontières de la Grande-Bretagne et des Etats-Unis ont été confiés à un seul et même groupe privé transnational, BorderGuard²⁵. Les craintes continues d'une immigration illégale et la rhétorique des gouvernements sur la « guerre contre le terrorisme » ont amené ces mêmes pays à se doter d'un système de « frontières intelligentes ». Le contrôle des passeports s'effectue désormais par le biais d'une série de caméras et de scanners chargés de photographier le visage, l'iris et les empreintes digitales des voyageurs et de les comparer à ceux des passeports biométriques normalisés (ou dans le cas de l'Angleterre, de la carte d'identité), adoptés par les pays du G10 et de l'UE²⁶. Les données contenues sur la micropuce RFID incluent des données touchant à la citoyenneté, au statut d'immigration, aux visas et au casier judiciaire, aux côtés d'informations de santé. Ces données sont instantanément comparées aux bases de données nationales et internationales, ainsi qu'à diverses informations extraites de transactions commerciales que BorderGuard se procure auprès d'entreprises spécialisées²⁷. Le passage à la frontière s'effectue sans difficulté pour la majorité de la famille, à l'exception de Geeta, la grand-mère. Le Pakistan n'a pas encore adopté la version complète du programme de frontières intelligentes, et Geeta n'a jamais acheté de passeport biométrique. Elle est par conséquent contrainte de faire la queue pendant plusieurs heures et de subir des fouilles ainsi qu'un interrogatoire supplémentaires. Malgré son identité britannique, les traits asiatiques de Yasmin, la mère, déclenchent l'alerte à son passage à la frontière et elle doit répondre à toutes sortes de questions supplémentaires. A la douane, tous les membres de la famille sont soumis à un scan corporel complet et à une fouille corporelle virtuelle ...²⁸

Télécommunications

Le terme de « télécommunications » ne renvoie pas uniquement au système téléphonique traditionnel, rattaché à une ligne fixe (voix et télécopie, mais aussi aux téléphones portables (y compris la voix, le texte, les images, les sons et les informations géodépendantes) et aux moyens de communication informatiques, tels qu'Internet (ADSL, etc.). A l'époque des réseaux de téléphone analogiques nationalisés, les téléphones devaient être « mis sur écoute » (généralement par la police ou les services de sécurité) pour pouvoir exercer une surveillance. Trois choses ont changé : les technologies de téléphonie (téléphones portables, fibre optique, sans fil, etc.), la combinaison des technologies de télécommunications et de stockage/traitement des informations (Courriel, sites Web, etc.), et la transition vers des opérateurs privés. L'évolution actuelle tend à une convergence accrue des technologies et à toujours plus d'« interopérabilité », en vue de permettre aux différentes technologies de fonctionner ensemble.

Le fonctionnement de ces technologies exige l'échange de signaux ou de données entre différents dispositifs, et c'est là qu'intervient la surveillance. Il est par exemple possible de localiser les téléphones portables, tandis que les fournisseurs d'accès Internet (FAI) peuvent cataloguer les sites visités en ligne. Cette connexion accrue des technologies de télécommunication engendre un plus grand volume d'informations. La loi veut aujourd'hui que ces informations soient conservées à des fins d'analyse : en février 2006, l'UE et le Home Office (ministère de l'intérieur britannique) ont proposé que ces données puissent être conservées pendant un maximum de deux ans et mises à la disposition de la police durant cette période.

Chaque pays filtre également, et régulièrement, les communications téléphoniques et autres télex, courriels et télécopies pour des raisons d'« intérêt national » (sécurité et intérêts économiques). A titre d'exemple, le système « ECHELON », le réseau de surveillance global de la NSA (American National Security Agency), possède un vaste centre à Menwith Hill dans le comté anglais du North Yorkshire : ce centre filtre automatiquement et régulièrement l'ensemble du trafic de télécommunications du Royaume-Uni à la recherche de mots et d'expressions clés et fait de plus en plus souvent appel à des algorithmes de reconnaissance verbale et sémantique toujours plus sophistiqués²⁹.

Une surveillance virtuelle

Une fois relâché par la police, Ben rentre chez lui, mais son ordinateur de poche³⁰ est désormais surveillé par le biais du système Galileo³¹. Il est également placé sur une liste de surveillance des communications, et son FAI reçoit un ordre RIP 2 (loi de 2009) lui indiquant que l'ensemble du trafic Internet et des courriels de Ben doivent être sauvegardés et transmis à la police³². Dans la mesure où la plupart des appels téléphoniques sont aujourd'hui effectués via Internet (et où les anciennes lignes fixes sont en voie de disparition), cette mesure concerne toutes les communications de Ben. Cette surveillance a cependant une conséquence imprévue : Toby, le jeune frère de Ben, qui utilise également occasionnellement les comptes de Ben (essentiellement parce que le « craquage » des ordinateurs³³ est l'une de ses grandes passions) est également concerné par cette surveillance. Toby passe la majeure partie de son temps en ligne sur des sites MMOG (Massively Multiplayer Online Games), des mondes virtuels qui possèdent leurs propres règles et leurs propres économies³⁴. La société de la surveillance s'est cependant déjà infiltrée dans ces univers. Ces mondes de données et d'avatars en ligne font l'objet d'une surveillance accrue, notamment de la part des entreprises soucieuses de mieux comprendre les nouvelles opportunités offertes à des marchés émergents bien réels. Il existe une nouvelle catégorie de « joueurs d'entreprise » dont la seule fonction est d'étudier les habitudes des autres joueurs via leurs avatars et de commercialiser viralemment des produits virtuels et réels à l'intérieur comme à l'extérieur de ces mondes³⁵. La police expérimente également avec des logiciels conçus pour surveiller ces univers virtuels et identifier les avatars qui affichent certains types de comportement, susceptibles d'indiquer de réelles tendances criminelles chez les joueurs³⁶. Cette approche est fortement contestée par les joueurs, qui affirment que l'évasion dans des mondes virtuels n'a rien à voir avec la vie réelle.

Vidéosurveillance

Bien que leur invention remonte aux années 60, l'essor des caméras de télévision en circuit fermé (CCTV) au Royaume-Uni date de la fin des années 80 ; l'idée était à l'époque d'enrayer le déclin des centres commerciaux urbains et d'apaiser les craintes face au terrorisme, à la criminalité et au vandalisme. Il existerait aujourd'hui près de 4,2 millions de caméras de CCTV en Grande-Bretagne, soit une pour quatorze habitants,³⁷ et chaque personne peut être filmée plus de 300 fois par jour³⁸. L'investissement consenti dans l'infrastructure CCTV au cours des dix dernières années est estimé à 500 millions de livres sterling,³⁹ alors même qu'une étude du Home Office a conclu que « les programmes de CCTV évalués n'ont qu'un effet global marginal sur les taux de délinquance ».⁴⁰

La numérisation s'est traduite par une utilisation accrue des systèmes de CCTV automatisés. Les plaques minéralogiques des véhicules sont aujourd'hui utilisées pour identifier leurs propriétaires. Le nombre de caméras de surveillance de la vitesse est passé d'un peu plus de 300 000 en 1996 à plus de deux millions en 2004, et quelque 113 millions de livres sterling d'amendes sont recueillies chaque année.⁴¹ Cette surveillance étatique accrue a mauvaise presse,⁴² et ce bien que les caméras

de surveillance de la vitesse, à la différence des caméras de CCTV, contribuent réellement à diminuer le nombre d'accidents de la route graves ou mortels.⁴³

La surveillance accrue des automobilistes devrait s'intensifier rapidement. En mars 2005, l'Association des officiers de police (Association of Chief Police Officers) a réclamé la mise en place d'un réseau national de lecteurs de plaques minéralogiques, « intégrant les caméras de la police, de la Highways Agency (Ponts et Chaussées britanniques) ainsi que des autres organismes partenaires et du secteur commercial »⁴⁴, y compris les caméras qui équipent déjà les centres villes et les rues commerçantes⁴⁵, le tout relié à un centre national de données ANPR (Reconnaissance automatique des plaques minéralogiques). Un tel système pourrait ainsi traiter quelque 35 millions de plaques minéralogiques par jour (50 millions d'ici 2008) et stocker ces résultats pendant deux ans.

Conduite accompagnée

Gareth s'apprête à quitter la cité et les grilles en fer forgé s'ouvrent automatiquement : une caméra enregistre l'heure de départ exacte, le numéro d'immatriculation du véhicule et les identités du conducteur et des passagers. Le système ANPR est opérationnel sur les routes britanniques depuis 2008 et les caméras sont à ce point omniprésentes qu'il ne sert à rien d'essayer de deviner leur emplacement à l'aide de scanners ou de cartes. De toute façon, l'ordinateur de poche que Gareth branche sur sa voiture est directement relié au système de navigation par satellite Galileo ainsi qu'aux caméras de surveillance de la circulation de l'Etat, et lui indique l'itinéraire le plus court. L'itinéraire recommandé est également le moins onéreux dans la mesure où le kilométrage effectué par Gareth est automatiquement facturé sur son compte bancaire via le système ANPR⁴⁶.

Biométrie

La quasi-totalité des nouveaux systèmes de cartes d'identité ont recours à la biométrie : les empreintes digitales, les scans de l'iris, de la topographie faciale et des mains font partie intégrante des différents systèmes de passeport et de cartes d'identité. La biométrie est souvent présentée comme une méthode infaillible, conçue pour améliorer la précision et combattre la fraude. Alors que les codes personnels et les mots de passe peuvent s'oublier ou se perdre, le corps représente un lien direct et constant entre les archives et la personne. La biométrie a fortement progressé aux Etats-Unis depuis les attentats du 11 septembre 2001 et l'Amérique insiste sur la normalisation des passeports biométriques.

Les systèmes d'accès biométriques (par le biais de scans de la voix et des mains notamment) sont aujourd'hui monnaie courante dans de nombreux bureaux ou sites de sociétés privées, ainsi que dans certains aéroports, tels que celui de Schiphol aux Pays Bas, où l'on utilise le système de scan de l'iris Privium. Mais la biométrie est également en train de gagner nos rues. Certaines villes de Grande-Bretagne – dont Newham (Londres), Birmingham, Tameside et Manchester pour ne citer qu'elles - expérimentent des logiciels de « reconnaissance faciale » automatiques. La reconnaissance faciale et les autres systèmes CCTV biométriques ne sont certes pas encore au point à l'extérieur ou dans les rues très passantes où les gens marchent vite, mais des investissements considérables sont actuellement consentis pour les améliorer.

Votre santé nous intéresse

Nous sommes en 2016 et Gareth travaille en tant que gérant d'un centre d'appels. Tout comme en 2006, les employés sont surveillés en permanence et un ordinateur enregistre la nature et la durée de chaque activité. La surveillance en matière de recrutement et de prestations sociales s'est cependant intensifiée. Les employés doivent aujourd'hui se prêter à toute une gamme de tests biométriques et psychométriques et d'études sur leur style de vie. Pour Gareth, il est important que le profil des employés corresponde à celui des clients afin d'assurer un meilleur service clientèle.⁴⁷ Il vérifie également que les employés ne s'adonnent pas à des sports dangereux, tels que le rugby ou le VTT, afin de ne pas courir le risque de longues périodes d'absence en cas d'accident. Les tests biométriques, basés autour d'échantillons buccaux et d'urine, sont rapidement analysés par l'infirmière de la société à l'aide d'un kit bon marché. L'employeur peut ainsi évaluer si un employé potentiel pose un risque de productivité en raison de problèmes de santé ou de toxicomanie. Le système permet également à l'organisation de proposer un ensemble de prestations sociales flexible, selon l'état de santé de l'employé. Certains candidats plus enthousiastes ont commencé à offrir volontairement des informations de santé, et la société rejette à présent fréquemment les CV qui ne contiennent pas ce type de données. Soucieuses de la santé de leurs employés, de nombreuses entreprises sont aujourd'hui proactives. Les employés utilisent leurs cartes d'accès à puce RFID pour bénéficier de réductions auprès de centres de mise en forme locaux. La fréquentation de ces centres figure sur leur registre d'emploi électronique et ceux qui ne s'y rendent pas régulièrement sont parfois interrogés sur leur style de vie dans le cadre des évaluations annuelles. Des tests psychométriques périodiques indiquent également à la direction si l'attitude des employés est compatible avec la culture et les valeurs de la société.

Positionnement, suivi et repérage

Les systèmes de surveillance sont de plus en plus omniprésents, qu'il s'agisse du GIS (Système d'information géographique) du GPS (Système de positionnement mondial), des puces RFID, des cartes d'identité intelligentes, des transpondeurs ou des signaux radio émis par les téléphones ou les ordinateurs portables.

Les systèmes GPS et RFID sont de plus en plus souvent utilisés dans le cadre de l'application des lois et de la gestion du personnel. La surveillance électronique est ainsi une condition sine qua non de toute mise en liberté provisoire, et en 2004/5 quelque 631 adultes et 5751 adolescents, certains à peine âgés de 12 ans, ont été munis de bracelets électroniques afin d'attendre leur procès chez eux plutôt qu'en détention provisoire.⁴⁸ Les délinquants libérés font de plus en plus souvent l'objet d'une surveillance électronique, en échange d'une sortie de prison anticipée avec couvre-feu et détention à domicile,⁴⁹ ou d'une libération conditionnelle.⁵⁰

Il y a encore peu, la technologie RFID ne concernait que les grands conteneurs d'expédition, les biens de consommation et divers types de cartes à puce intelligentes. Une nouvelle étape importante a cependant été récemment franchie, mais est passée en grande partie inaperçue : la greffe de puces RFID sur des êtres vivants. Les puces contenant les informations sur vaccinations et propriétaires ont progressivement remplacé les exigences de mise en quarantaine des animaux de compagnie au sein de l'UE depuis le 28 février 2000. Baptisé PETS, ce programme a depuis été étendu hors de l'Europe⁵¹. La première utilisation des puces RFID chez l'être humain a eu lieu aux Etats-Unis : quelque 70 personnes âgées souffrant de maladies dégénératives se sont ainsi vues implanter une puce afin de permettre à leurs accompagnants de les localiser rapidement⁵². Certains chercheurs et inconditionnels de la technologie se greffent également des micropuces depuis

plusieurs années⁵³, et une chaîne de night-clubs espagnols offre à ses clients la possibilité de se faire implanter une puce contenant le détail de leurs privilèges et du contenu de leur compte: ceux-ci n'ont alors plus qu'à se faire scanner le bras par le personnel du bar pour effectuer leurs paiements ou éviter les files d'attente.⁵⁴ Ce système a franchi un nouveau pas en février 2006, lorsqu'une société de sécurité de l'Ohio, aux Etats-Unis, a greffé une micropuce RFID sur deux de ses employés afin de leur permettre d'accéder aux locaux appartenant à la société⁵⁵. Certains sites Web technologiques débattent aujourd'hui sérieusement de la nécessité de faire greffer une puce sur chacun d'entre nous.

Pour l'avenir, les entreprises considèrent les puces RFID et le système GPS comme de simples méthodes de marketing personnalisé en temps réel, destinées à des clients particuliers, et qui permettent par exemple de leur offrir, via leur portables, des remises dans les magasins de telles ou telles villes. Le développement continu de l'application en temps réel des données de localisation sur le profil des consommateurs fournira aux entreprises une strate de données supplémentaire qui leur permettra de cibler des clients donnés lors de campagnes de marketing et le cas échéant, de favoriser leur surveillance par les organismes chargés de l'application des lois et les gouvernements.

Le nouveau « brandscape »

Nous sommes en 2016 et les Jones se rendent au centre commercial de leur quartier : les caméras CCTV et les gardes de sécurité sont toujours là, mais quelque chose a changé. Outre le contrôle de la délinquance, la modélisation spatiale du « brandscape »⁵⁶ et l'adaptation des messages publicitaires en fonction des différentes catégories de consommateurs constituent désormais une priorité stratégique. Le centre commercial a accès à une vaste base de données partagée, obtenue à partir des données des cartes de fidélité, qui lui permettent de générer des informations sur les clients. Le système repose sur l'utilisation de puces RFID dans les vêtements, de scanners omniprésents et de bases de données. Les scanners des portes des magasins enregistrent les identifiants uniques des puces RFID intégrées dans les vêtements des consommateurs. Des panneaux publicitaires intelligents, placés au niveau des yeux, affichent une gamme de produits destinés à chaque client en temps réel. Sara est ainsi ravie d'assister au téléchargement du nouveau morceau de son groupe préféré, tandis que Toby note les informations relatives aux modifications de son monde de jeux en ligne favori. Des messages de marketing peuvent être également envoyés aux ordinateurs de poche des consommateurs lorsqu'ils sont aux abords de certains magasins.

Les clients à forte valeur ajoutée sont désormais invités à s'inscrire à un nouveau programme sans espèces. Ce système permet aux clients à plus fort potentiel d'achat⁵⁷ de se faire greffer une puce sous la peau⁵⁸. Le coût de l'implant est de 200 livres sterling, mais cet investissement est rapidement amorti (et plus qu'amorti) par les nombreuses remises offertes par les magasins⁵⁹. Le consommateur peut alors recharger le crédit de sa puce et payer dans les différents magasins en se faisant scanner le bras, au lieu d'utiliser une carte de crédit, de débit ou de fidélité. Les consommateurs « greffés » ont également accès sur place à un salon VIP, un spa et un centre de massage. Pour les partisans de ce système « sans espèces », les consommateurs sont ainsi moins exposés aux risques d'agressions et aux pickpockets, et ne risquent plus une utilisation frauduleuse de leur carte de crédit. Des rumeurs circulent pourtant : certains consommateurs auraient été agressés sur le parking et les puces leurs auraient été découpées du bras, mais les opérateurs prétendent qu'il s'agit là d'un « mythe urbain ». Gareth, le père, qui pensait un instant s'inscrire à ce programme, hésite aujourd'hui après avoir vu un reportage télévisé affirmant que les puces pouvaient être la cible de virus informatiques. Il est d'autant plus inquiet que les soupçons de fraude peuvent avoir des

conséquences des plus sérieuses. En raison de l'utilisation d'algorithmes prédictifs beaucoup plus sophistiqués, basés sur les profils individuels des clients, le simple fait de recevoir un appel de sa banque équivaut à une quasi-culpabilité : les cartes sont automatiquement désactivées et le client doit fournir à la banque la preuve indépendante de son identité et de son domicile.

Flux de données

Les données recueillies par les technologies de surveillance circulent entre les réseaux informatiques. Bon nombre d'entre-nous peuvent certes accepter de fournir des informations dans un cas précis, mais que se passe-t-il si ces données sont transférées ailleurs ? Le public et les organismes de partage des données ne savent cependant généralement pas grand chose de la destination finale de ces données.

Détournement d'usage

La surveillance semble obéir à une logique bien particulière qu'il convient cependant de remettre en question, d'examiner et de vérifier, notamment lorsque les données circulent d'un site à l'autre et que les informations fournies dans un cadre donné sont réutilisées ailleurs à d'autres fins. Citons à titre d'exemple les cartes de transport Oyster à Londres, qui sont de plus en plus utilisées par les services de police dans le cadre de leurs enquêtes.⁶⁰ Les techniques d'exploitation des données, développées pour le profilage des consommateurs, sont non seulement utilisées par les services de sécurité et de renseignement pour dresser le profil des terroristes potentiels, mais les données à partir desquelles ces profils sont établis, sont souvent les mêmes. Les technologies de diagnostic médical sont aujourd'hui de plus en plus souvent détournées vers d'autres usages plus généraux, ce qui peut nuire à leurs qualités prédictives de diagnostic et désavantager les patients mal diagnostiqués. Les technologies de surveillance au travail permettent parfois d'obtenir plus d'informations que prévu, et la direction est alors tentée d'étendre ces pratiques de surveillance sans consulter les employés, affectant du même coup les décisions de salaire ou de promotion.

Convergence

Dans la mesure où de plus en plus de systèmes sont aujourd'hui conçus dans une optique de flux de données et d'interopérabilité intégrée, on constate une convergence accrue des technologies de surveillance. Il est ainsi possible que nous assistions à l'émergence totalement imprévue et déréglementée de nouveaux produits. Citons à titre d'exemple les cartes d'identité conçues pour différents usages : passages des frontières, lutte contre la fraude et accès aux informations gouvernementales, voire même commerciales (location de vidéos) et semi-commerciales (bibliothèques). Les personnes contrôlant ces bases de données identitaires disposeraient ainsi d'un immense pouvoir sur des fichiers contenant des informations essentielles, susceptibles d'affecter toute une vie.

Vers une surveillance omniprésente

Les technologies ne sont jamais aussi importantes que lorsqu'elles sont omniprésentes, acceptées de tous et en grande partie invisibles. Nous sommes tous de plus en plus souvent amenés à traverser quotidiennement des « points de passage », où les systèmes électroniques et physiques se conjuguent pour offrir une combinaison de technologies à base de CCTV, de biométrie, de bases de données et de suivi. La surveillance gagne partout et constamment du terrain et est désormais omniprésente.

Tri social

Le « tri social » est un aspect endémique de la société de la surveillance. L'Etat et le secteur privé analysent et catégorisent de vastes bases de données personnelles afin de définir les marchés cibles et les populations à risque⁶¹. Une fois classé, il est difficile de sortir de ce moule. Depuis les attentats du 11 septembre 2001, il est certes possible qu'un tel tri ait contribué à augmenter la sécurité des compagnies aériennes (nous ne le saurons jamais), mais il a certainement entraîné un profilage grossier de certains groupes, dont les musulmans, profilage qui a débouché sur des inconvénients, des privations et parfois même des cas de torture.

Le tri social définit de plus en plus la société de la surveillance. Il offre différentes opportunités à différents groupes et revient souvent – de façon subtile et parfois involontaire – à organiser nos sociétés et à adopter des politiques sans véritable débat démocratique. Les systèmes invisibles de péage urbain et de transport public intelligent maintenant acceptés ont certes leur utilité, mais ils divisent la ville en groupes, entre ceux qui peuvent circuler relativement librement et ceux qui éprouvent des difficultés à se déplacer. Ces systèmes peuvent être parallèlement utilisés à des fins de lutte contre la criminalité et de sécurité nationale. Personne n'a voté directement pour de tels systèmes. Leur émergence s'inscrit dans le cadre de campagnes d'efficacité accrue des services publics et sous la pression des grandes entreprises technologiques, avec pour toile de fond le thème croissant du « risque » au sein de nos sociétés et l'idée que nous ne devons pas ménager nos efforts pour prévenir les dangers.

Surveillance des enfants

En 2016, le repérage et le suivi sont devenus des composantes absolument essentielles de l'éducation.⁶² A la suite d'une série d'affaires médiatisées dans lesquelles des élèves se sont perdus ou ont été blessés ou tués, de nombreuses écoles, et en particulier les écoles primaires et même les maternelles, ont exprimé le désir de pouvoir localiser les élèves en permanence, afin d'éviter d'éventuelles poursuites en justice.⁶³ Les écoles primaires ont commencé à introduire des dépistages de drogue, en réponse à la politique gouvernementale visant à identifier à un stade précoce les enfants à problèmes, à lutter contre l'absentéisme et à améliorer la concentration en classe – autant d'arguments importants face aux « league tables » omniprésentes.⁶⁴ L'école de Toby Jones a adopté un système de carte sans espèces qui permet aux familles de surveiller l'alimentation de leurs enfants. Trois ans plus tard, la chaîne de supermarchés NSC a racheté la société de gestion de ces cartes pour accéder à un marché de la jeunesse lucratif et favoriser la promotion de marques via la fourniture de matériel éducatif. Les parents sont invités à présenter la carte de l'enfant à la caisse du supermarché, permettant ainsi l'identification de l'école, de l'élève et des parents. NSC fournit alors du matériel scolaire supplémentaire en fonction du volume d'achat des parents. Certains fournisseurs importants de NSC⁶⁵ ont commencé à installer des distributeurs dans les écoles. L'école de Toby a poursuivi ce programme et à chaque arrivage de nouveaux équipements, la marque « NSC » est mise en valeur. Les autorités scolaires locales surveillent les aliments consommés dans l'école de Toby et s'en inspirent pour mener diverses campagnes d'« alimentation saine ». La carte est devenue de plus en plus intégrée : outre les données relatives aux repas des enfants, elle a progressivement incorporé des données sur leur assiduité, leurs résultats, leurs activités périscolaires, les dépistages de drogue et l'accès à Internet ; la carte était même utilisée comme partie intégrante des cours d'instruction civique. Bien que la surveillance accrue dans les écoles se soit traduite par des avantages mesurables pour les établissements et les élèves, les enfants acceptent petit à petit comme chose normale ces systèmes de surveillance de plus en plus intrusive, le suivi à distance de leur localisation et de leurs déplacements et de leur alimentation ...

Verrouillage technologique

Une réponse technologique peut également être apportée au problème de la surveillance : l'usage de certaines technologies dites de protection de la vie privée (PET), qui permettent de limiter ou de modérer la surveillance, doit être encouragé le cas échéant. Cela étant, la solution aux problèmes techniques ou en matière de protection de la vie privée ne peut se limiter au progrès technologique. Plus les Etats, les organisations, les personnes et la société dans son ensemble deviennent dépendants des technologies de surveillance, plus il se produit un phénomène de « verrouillage » qui empêche la prise en compte d'autres options susceptibles d'atteindre les mêmes objectifs, et plus le fossé s'élargit en termes de compréhension, ce qui accroît notre dépendance vis-à-vis des experts non soumis au contrôle démocratique. Par exemple, l'introduction de la carte d'identité se traduira inévitablement par une plus grande dépendance du gouvernement britannique vis-à-vis des experts techniques et commerciaux.

Il convient d'être prudent face aux propositions visant à apporter une solution purement technique aux soi-disant problèmes techniques. Comme nous allons le voir, la réalité de la société de la surveillance est beaucoup trop complexe pour se limiter à des réponses aussi superficielles. On peut également se demander si les autorités disposent des outils nécessaires pour mettre en place une réglementation significative des technologies et des pratiques de surveillance dont la complexité ne cesse de s'accroître. Peut-on forcer un génie à rentrer dans sa bouteille ?

Echecs technologiques

Bien entendu, les technologies ne tiennent jamais entièrement leurs promesses. Les ambitions technologiques du programme biométrique USVISIT, par exemple, ont été revues à la baisse pour des raisons logistiques, la lecture des empreintes digitales ayant remplacé l'identification par lecture de l'iris initialement envisagée⁶⁶. De même, des problèmes ont été rencontrés lors de la mise en œuvre des éléments biométriques du programme e-Borders (frontières électroniques) au Royaume-Uni⁶⁷. Les performances des systèmes de reconnaissance faciale continuent d'être insuffisantes en situation réelle. Le service britannique des casiers judiciaires (Criminal Records Bureau) a révélé qu'environ 2700 personnes avaient été faussement identifiées comme détentrices d'un casier judiciaire, et qu'en conséquence, un certain nombre d'entre elles s'étaient vues refuser un emploi⁶⁸. En ce qui concerne le système de cartes d'identité envisagé au Royaume-Uni, on estime qu'une personne sur six pourrait ne pas être en mesure d'utiliser sa carte en raison des problèmes techniques liés à la saisie de ses données dans le système.⁶⁹

De telles erreurs sont susceptibles de limiter l'accès à certains lieux ou services, mais dans d'autres domaines, par exemple en ce qui concerne la surveillance médicale, elles peuvent mettre des vies en danger, et elles sont beaucoup plus courantes qu'on ne le pense. Les conséquences de ces échecs ou insuffisances technologiques peuvent ainsi être pires, en termes d'opportunités futures, que celles offertes par un système performant.

Quelles conséquences la société de la surveillance entraîne-t-elle ?

Si la société de la surveillance s'accompagne d'avantages et de droits, elle entraîne également des conséquences négatives dont certaines peuvent être graves et potentiellement irréversibles. Tout débat public consacré à la surveillance doit considérer les questions suivantes : quels sont ses effets sur la vie privée, la déontologie et les droits de l'Homme ? Quel est son impact sur l'inclusion et l'exclusion sociale ? Quels changements apporte-t-elle en termes de choix, de pouvoir et d'autonomisation ? Dans quelle mesure est-il possible d'exiger que les sociétés exploitant de tels

systemes prennent leurs responsabilités ? Et quelle est la transparence des processus de surveillance?

Vie privée, déontologie, droits de l'Homme

La plupart des discussions actuelles concernant la surveillance gravitent autour du thème de la vie privée. Depuis les années 70, de nombreuses lois en matière de protection des données et de la vie privée ont été introduites en Europe et ailleurs. Cela étant, il s'est avéré difficile de persuader les autorités de l'existence d'une dimension *sociale* plus profonde de la vie privée,⁷⁰ et encore moins de la nécessité de confronter les autres problèmes non liés à la vie privée qui découlent de la société de la surveillance. Dans la plupart des cas, les gens ne sont même pas conscients de l'existence du problème, et ont encore moins la capacité de l'identifier, de savoir à qui faire part de leurs doléances et de quelle façon ils peuvent obtenir réparation.

La protection de la vie privée est essentielle, mais la société de la surveillance pose également d'autres problèmes d'ordre déontologique et associés aux droits de l'Homme. Il est anormal d'attendre du citoyen ordinaire qu'il se protège lui-même. Les trois aspects fondamentaux sont les suivants :

Exclusion sociale, discrimination

Comme nous l'indiquons dans le rapport complet, la surveillance varie en fonction du lieu, de la classe sociale, du groupe ethnique et du sexe. La surveillance, l'invasion et la protection de la vie privée varient selon les groupes, au profit de certains et au détriment d'autres. La surveillance s'est développée parallèlement aux changements intervenus dans les secteurs de la santé et de la sécurité sociale, et dans de nombreux cas, ces services publics ont été réduits à de simples opérations de gestion des risques qui demandent une connaissance totale de la situation. Les données personnelles sont donc essentielles pour déterminer l'attribution des ressources.⁷¹ Et dans la mesure où les réseaux de surveillance permettent une plus grande intégration, il est beaucoup plus facile pour les compagnies d'assurance de travailler en collaboration avec la police, ou pour les supermarchés d'unir leurs forces avec les sociétés de collecte de données. En conséquence, les points névralgiques de la police se situent fréquemment dans des quartiers à forte concentration ethnique, et les hypermarchés s'implantent dans des quartiers haut de gamme ou périphériques qui sont plus facilement accessibles en voiture.

Solutions sociales totales ?

En 2016, les zones résidentielles sont plus clairement divisées entre les quartiers privés à accès contrôlé, tels que celui où vit la famille Jones, patrouillés et surveillés par des sociétés de gardiennage bien équipées, et les anciennes cités HLM comme la cité Dobcroft. Pour les Jones, les caméras et systèmes d'identification installés dans leur quartier permettent de minimiser leurs frais d'assurance⁷². Dans la cité Dobcroft, le travail de Yasmin au sein d'une équipe d'assistance sociale plurilatérale est désormais sous-traité à un consortium privé baptisé, de façon plutôt optimiste, Solutions Sociales Totales. SST est chargé de surveiller et de faire appliquer les programmes relatifs au comportement personnel PBS (Personal Behaviour Schemes⁷³) auxquels chaque habitant de la cité Dobcroft « souscrit » depuis sa naissance⁷⁴ (certains sont même identifiés avant⁷⁵). La plupart des personnes qui font l'objet d'une surveillance PBS plus intense, comme celles en période de probation⁷⁶, portent un implant RFID actif automatiquement détecté par des capteurs installés à leur domicile et aux entrées de la cité⁷⁷. La pose de ces implants est soi-disant volontaire, mais comme c'est le cas pour les programmes lancés dans les magasins et les écoles, son acceptation apporte des récompenses, notamment la cessation anticipée de la période de probation. A l'heure actuelle, un « couvre-feu généralisé » est également imposé dans la cité Dobcroft (un évènement qui survient périodiquement) après que des jeunes ont été soi-disant identifiés comme auteurs de troubles par une résidente du village de retraite Sunnyview. La vieille dame avait signalé des activités suspectes filmées par les caméras de vidéosurveillance locales, et retransmises sur les chaînes de télévision numérique locales qui proposent

également un trombinoscope des personnes ayant enfreint leur programme PBS⁷⁸. Une interdiction d'entrer ou de quitter la cité entre 18 h et 6 h frappe actuellement les moins de 18 ans.

Choix, pouvoir et autonomisation

Avons-nous notre mot à dire face à cette société de la surveillance ? Le citoyen ordinaire peut influencer (et influence) les débats, notamment en insistant pour que la réglementation soit respectée, en remettant le système en cause ou en refusant que ses données soient utilisées à des fins pour lesquelles il ne dispose que d'informations partielles ou qui lui semblent suspectes.

Mais jusqu'à quel point les citoyens ou les groupes peuvent-ils choisir d'être exposés à cette surveillance et limiter les données personnelles qui sont collectées et utilisées ? Souvent trop compliqués sur le plan technique pour le citoyen ordinaire, les systèmes de surveillance ont tendance à disparaître au sein des structures et systèmes quotidiens de la société : travail, loisirs, maison, école, transports, communications et services publics. Il semble plus difficile de peser réellement sur le débat. Par exemple, ce n'est que lorsqu'un scandale concernant un vol d'identité éclate que les consommateurs prennent conscience de l'ampleur des opérations de profilage individuel effectuées par les grandes entreprises,⁷⁹ et là encore, le débat a tendance à se concentrer sur les questions de sécurité – comment empêcher d'autres cas de fraude similaires – plutôt que sur la limitation de l'emprise des sociétés privées et des organismes publics sur les données. En matière de contrôle de l'impact de la surveillance, le citoyen est fortement désavantagé.

Transparence, responsabilité

Les capacités de surveillance des infrastructures commerciales, publiques et de transport sont en plein essor, mais les citoyens et les groupes ont des difficultés à découvrir ce qui advient de leurs données personnelles, qui les manipule, à quel moment et dans quel but. Pourtant, peu à peu, ces données personnelles sont utilisées pour façonner leurs opportunités futures et orienter leurs choix. Les organisations doivent assumer leurs responsabilités, en particulier lorsque des opérations de surveillance intense, dont les conséquences sont potentiellement négatives, se déroulent au quotidien. Il faut passer de l'autoprotection de la vie privée à la responsabilisation des manipulateurs de données, celle-ci venant s'ajouter au travail des instances réglementaires officielles chargées d'appliquer les mesures de contrôle et d'encourager la minimisation de la surveillance.

Les défis en termes de réglementation

Est-il possible de réglementer la surveillance, d'en maîtriser les effets négatifs, et de la rendre compatible avec le type de société et de démocratie que nous souhaitons ?⁸⁰ Une évaluation de l'impact des nouveaux projets sur la vie privée et la surveillance contribuerait au débat et à la sensibilisation du public, et ajouterait une dimension importante aux systèmes de réglementation. Il existe un grand nombre de lois et de codes de déontologie relatifs à la protection de la vie privée. Certaines technologies offrent également une certaine protection. Il existe des organismes de réglementation chargés de faire appliquer la loi, de répondre aux doléances du public, et d'influencer la politique des gouvernements et les orientations des entreprises. Certains groupes de pression, ainsi que les médias, nous préviennent des dangers liés à la surveillance. Mais on peut s'interroger sur la valeur et l'efficacité de ces mécanismes de réglementation ; ils demandent à être réexaminés et améliorés. Quoi qu'il en soit, la protection de la vie privée n'est qu'un des aspects du problème. Il est essentiel qu'un plus grand nombre de personnes prenne conscience des questions liées à la surveillance, et exprime son opinion sur ce qu'il convient de faire pour que celle-ci serve au mieux les intérêts du public. Mais la réglementation ne peut se limiter à un pays, voire à un groupe de pays comme l'Union européenne. En matière de surveillance, les flux d'informations sont véritablement d'ordre mondial ; il en est de même des mouvements et des activités qui font l'objet

de cette surveillance. Pour faire face à ces défis, la réglementation doit être intégrée et harmonisée davantage au niveau mondial.

La galerie des glaces

Bien que la surveillance soit omniprésente en 2016, les gens, en particulier ceux qui sont suffisamment cultivés ou riches pour l'apprécier ou pour se l'offrir, en sont de plus en plus conscients et savent de mieux en mieux la gérer. Gareth Jones souscrit à un service de gestion des informations personnelles chargé de contrôler en ligne ses « données fantômes », de corriger automatiquement les informations inexactes détenues sur les bases de données publiques et commerciales, et de l'informer des problèmes potentiels. Son ordinateur de poche, très coûteux, bloque également les messages publicitaires à caractère commercial. Malheureusement, tout le monde n'est pas en mesure de modifier et d'accéder à ses données personnelles de la même façon. Les personnes moins rompues aux techniques de gestion des informations personnelles, ou moins en mesure de s'offrir les services d'autres personnes pour assurer cette gestion à leur place, sont fortement désavantagées. Certains groupes de pression ont obtenu qu'il soit plus facile d'accéder et de modifier les informations personnelles détenues par l'Etat et les entreprises privées travaillant au service de l'Etat, mais cet accès fait désormais partie des nombreux services nécessitant la possession d'une carte d'identité. La question de savoir qui sait quoi, qui possède les données et qui a le droit de les modifier fait l'objet d'une polémique croissante entre les citoyens et l'Etat. Mais en 2016, les gens sont plus habitués à observer et à être observés. Un grand nombre d'entre eux procèdent à une auto-surveillance permanente, une sorte de consignation électronique de leur existence en temps réel, qui consiste à enregistrer, stocker ou placer directement en ligne⁸¹ tout ce qu'ils font au quotidien. Certaines milices de citoyens, qui considèrent que l'Etat fait preuve de laxisme en matière de lutte contre le terrorisme, la criminalité et l'immigration illégale⁸², effectuent également des opérations de surveillance, et la prolifération des sites Internet non-officiels consacrés aux « suspects » entraîne une multitude de problèmes et d'erreurs d'identification⁸³. Les protestataires, les artistes et les surréalistes résistent et se jouent de cette surveillance omniprésente de diverses manières, y compris en désactivant les dispositifs de surveillance publics⁸⁴, à l'aide de technologies dites de « sousveillance » qui permettent de contrer ces dispositifs⁸⁵. Certains militants anticapitalistes, comme Aaron et Ben, passent leurs samedis après-midi à coller des plaques d'aluminium hautement adhésives et à placer de minuscules émetteurs de micro-ondes alimentés par pile à l'entrée des magasins pour perturber les signaux sans fil.⁸⁶ En outre, la consignation électronique de l'existence n'est pas infaillible, l'amélioration constante des logiciels de gestion des données et de production vidéo permettant de plus en plus d'ajuster, voire de créer sa propre vie à des fins ludiques, subversives ou frauduleuses. En 2016, il existe un nombre croissant de données fantômes entièrement virtuelles, qui ne correspondent à aucune réalité, qui donnent l'impression d'exister et qui, elles-mêmes, font l'objet d'une gestion des informations et d'une surveillance en ligne effectuées par des systèmes automatisés qui travaillent en silence et dans l'ombre, et qui hantent une galerie des glaces sans fin...

Références

Nota : toutes les pages Internet étaient accessibles au 1er septembre 2006.

- ¹ Ces divers aperçus d'un avenir éventuel sont issus de la section C du rapport complet, qui comprend également une « Semaine typique dans la vie » d'une famille moyenne en 2006.
- ² Les avions sans pilote sont utilisés par l'armée américaine depuis de nombreuses années : l'exemple le plus connu actuellement est le drone de reconnaissance « Predator » utilisé en Irak ; cf. : « Predator RQ-1 / MQ-1 / MQ-9 Unmanned Aerial Vehicle (UAV), USA », *airforce-technology.com*, 2006, <http://www.airforce-technology.com/projects/predator/>. De nombreuses utilisations ont été suggérées au Royaume-Uni, cf. : Jha, A., « On the horizon ... pilotless planes as fishermen's and firefighters' friends », *The Guardian*, 30 août 2006, <http://www.guardian.co.uk/science/story/0,,1860825,00.html>. A Los Angeles, la police a déjà testé un petit avion espion télécommandé baptisé « SkySeer » : Bowes, P., « High hopes for drone in LA skies », *BBC News*, 6 juin 2006, <http://news.bbc.co.uk/1/hi/world/americas/5051142.stm>.
- ³ Les grands événements sportifs ont souvent été utilisés pour tester et introduire de nouvelles technologies de surveillance. Par exemple, en ce qui concerne les caméras de surveillance en circuit fermé lors de la Coupe du Monde au Japon en 2002, consulter : Abe, K., (2004) « Everyday policing in Japan: surveillance, media, government and public opinion », *International Sociology*, 19, 215–231 ; en ce qui concerne les caméras de surveillance CCTV lors des Jeux Olympiques d'Athènes, consulter : Samatas, M. (2004) *Surveillance in Greece*, Athènes : Pella.
- ⁴ Consulter les rapports d'expert en matière de crime, de justice et d'infrastructure (Crime and Justice and Infrastructure Expert Reports). L'angle de vision des caméras constitue l'un des principaux problèmes concernant la reconnaissance faciale ; consulter, p. ex. : Introna, L. and Wood, D. (2004) « Picturing algorithmic surveillance: the politics of facial recognition systems », *Surveillance & Society*, 2(2/3) : 177–198.
- ⁵ La gouvernance urbaine est progressivement confiée à des partenariats public privé, des organisations de gestion des centres-villes (<http://www.atcm.org/>) et des BID. Selon le gouvernement, les BID sont une source « d'investissement au sein de l'environnement commercial local grâce à leur offre de services à valeur ajoutée » : <http://www.ukbids.org/>. En 2016, l'un des principaux problèmes d'ordre réglementaire concerne le partage des informations entre l'Etat et les sociétés de surveillance privées qui interviennent au nom ou à la place de l'Etat, notamment dans la mesure où l'ordinateur central de la Police Nationale (Police National Computer, ou PNC) relie désormais un très grand nombre de bases de données, et où les services de police et de probation, l'administration pénitentiaire et les services sociaux sont étroitement liés.
- ⁶ De nombreux services de police procèdent déjà à des essais dans ce domaine (consulter p. ex. : « Pocket computers put police 'in the picture' », *West Yorkshire Police*, 28 mars 2006, <http://www.westyorkshire.police.uk/section-item.asp?sid=12&iid=2226>), et le projet « Airwave » (cf. rapport d'expert en matière criminelle et judiciaire) est conçu pour prendre ces systèmes en compte.
- ⁷ Ici encore, les systèmes de caméras fixées au casque et reliées en direct à une salle de contrôle ont déjà été introduits dans plusieurs régions ; consulter p. ex. : « Police use anti-yob head cameras », *BBC News*, 23 mars 2006, http://news.bbc.co.uk/1/hi/wales/north_east/4836598.stm.
- ⁸ En 2016, la police et ses partenaires privés ont accès à pratiquement toutes les bases de données reliées par le PNC..
- ⁹ En 2016, ces méthodes policières suscitent encore la polémique au sein des médias et du monde politique. Mais les services de police affirment que la carte d'identité offre un moyen pratique de vérifier la bonne foi des usagers, et qu'ils ne peuvent prendre le risque de présumer de l'innocence des personnes qui ne la possèdent pas.
- ¹⁰ Ford, R., « Beware rise of Big Brother state, warns data watchdog », *The Times*, 16 août 2004, http://www.timesonline.co.uk/article/0,,2-1218615_1,00.html
- ¹¹ Le degré de surveillance dans la vie quotidienne est documenté dans la section C du rapport complet.
- ¹² Source : *SecurityStockWatch.com 100 Index*, août 2006 : <http://www.securitystockwatch.com/>
- ¹³ Consulter, par exemple : « The future of screening », *BBC News*, 14 décembre 2002, <http://news.bbc.co.uk/1/hi/health/2570787.stm>.
- ¹⁴ McKie, R., « Icelandic DNA project hit by privacy storm », *The Observer*, 16 mai 2004, <http://observer.guardian.co.uk/international/story/0,6903,1217842,00.html>. Rose, H. (2001) *The Commodification of Bioinformation: The Icelandic Health Sector Database*, Londres : The Wellcome Trust.
- ¹⁵ Ce sujet est débattu dans Lyon, D. *Surveillance after September 11*, Cambridge, Royaume-Uni : Polity Press, 45–48, 142ff.
- ¹⁶ Garton Ash, T. (1997) *The File: A Personal History*, New York : Vintage.

¹⁷ Par exemple, bien que les transactions effectuées en numéraire ne puissent ordinairement être attribuées à tel ou tel consommateur, elles sont souvent analysées par rapport à des transactions antérieures similaires et à des types de consommateurs qui ont effectué les mêmes achats.

¹⁸ Cf. Fink, J. et Kosba. A. (2000) « A review and analysis of commercial user modeling servers for personalization on the world wide web », *User Modeling and User-Adapted Interaction*, 10, 209–249

¹⁹ Rapport Wanless (2002) *Securing Our Future Health: Taking a Long-Term View: Final Report*, Londres : HM Treasury.

²⁰ PITO (2005) *Police Information Technology Organisation, Annual Report 2004 – 2005*, HC 261, Londres : The Stationery Office.

²¹ Randerson, J., « DNA of 37% of black men held by police », *The Guardian*, 5 janvier 2006, <http://www.guardian.co.uk/frontpage/story/0,,1678168,00.html> .

²² PITO (2006) *Facial Images National Database (FIND)*, <http://www.pito.org.uk/products/FIND.php> .

²³ ACPO (Association of Chief Police Officers) (2002) *Infinet: A National Strategy for Mobile Information*, Association of Chief Police Officers.

²⁴ Il est indiscutable que le profilage racial existe déjà de façon informelle et ce, depuis longtemps. Son adoption officielle a également été suggérée par la police britannique, cf. : « No racial profiling by anti-terror police, says minister » *Times Online*, 2 août 2005, <http://www.timesonline.co.uk/article/0,,22989-1717624,00.html> . Pour de plus amples informations, consulter : « Racial Profiling: Old and New », *ACLU*, <http://www.aclu.org/racialjustice/racialprofiling/index.html> ..

²⁵ Consulter le rapport d'expert relatif aux frontières (Borders Expert Report).

²⁶ L'Organisation de l'aviation civile internationale a approuvé les normes relatives aux documents de voyage lisibles à la machine (Machine Readable Travel Documents, ou MRTD) en 2004, sous l'impulsion de l'actuelle Initiative du G8 pour la facilité et la sécurité des voyages internationaux (Secure and Facilitated International Travel Initiative, ou SAFTI) : « G8 meeting at Sea Island in Georgia, USA - sets new security objectives for travel », *Statewatch*, 2004, <http://www.statewatch.org/news/2004/jun/09g8-bio-docs.htm> . Ceci en dépit des inquiétudes concernant la facilité de cloner les puces RFID : Johnson, B., « Hackers crack new biometric passports », *The Guardian*, 7 août 2006,

<http://politics.guardian.co.uk/homeaffairs/story/0,,1838754,00.html> . Le fait que la carte d'identité britannique puisse facilement fusionner avec le passeport biométrique a déjà été signalé : Lettice, J., « UK biometric ID card morphs into £30 'passport lite' », *The Register*, 8 juillet 2005, http://www.theregister.co.uk/2005/07/08/id_card_as_passport/ .

²⁷ Consulter le rapport d'expert en matière de consommation (Consumer Expert Report). En 2016, les questions de propriété intellectuelle des données de voyage continuent de constituer un sujet de contentieux entre les Etats et les sociétés externalisées de sécurité aux frontières. Les autorités britanniques maintiennent leur « droit » de vendre les données relatives à l'identité, conformément à la proposition émise en 2006 : Elliot, F., « ID plans: powers set to widen », *The Independent*, 6 août 2006, <http://news.independent.co.uk/uk/politics/article1216000.ece> . Le seul dont la voix continue d'être ignorée, c'est le citoyen.

²⁸ Ce type de scanner intégral, qui existe sous diverses formes, est déjà testé à titre expérimental. Par exemple, le système à faibles rayons X Secure 1000 de Rapiscan (<http://www.rapiscansystems.com/sec1000.html>) testé à l'aéroport de Heathrow (cf. : Lettice, J. « 'See through clothes' scanner gets outing at Heathrow », *The Register*, 8 novembre 2004, http://www.theregister.co.uk/2004/11/08/heathrow_scanner_pilot/), ou le scanner à onde millimétrique mis au point par QinetiQ, et testé par Eurotunnel (http://www.qinetiq.com/home/newsroom/news_releases_homepage/2004/3rd_quarter/Next_generation_security_screening.html).

²⁹ Campbell, D. (1999) *Development of Surveillance Technology and Risk of Abuse of Economic Information (An appraisal of technologies of political control) Volume 2/5: the state of the art in Communications Intelligence (COMINT) of automated processing for intelligence purposes of intercepted broadband multi-language leased or common carrier systems, and its applicability to COMINT targeting and selection, including speech recognition (AKA Interception Capabilities 2000)*, Luxembourg : Parlement européen, Direction générale de la Recherche, Direction A, Programme STOA.

³⁰ En 2016, la plupart des gens possèdent ce type d'appareil qui offre un accès Internet sans fil en itinérance, des services téléphoniques, un système de navigation GPS etc. La fonction de navigation permet également le suivi de l'appareil (et par conséquent de l'utilisateur).

³¹ Le système Galileo est l'alternative civile européenne au système GPS de l'armée américaine. Le premier satellite a été lancé en 2004 et certains services seront opérationnels d'ici 2008, cf. : « Galileo, Système

européen de navigation par satellite » CEC Direction générale de l'énergie et des transports, http://ec.europa.eu/dgs/energy_transport/galileo/intro/future_en.htm .

³² La loi britannique relative à la réglementation des pouvoirs d'investigation (Regulation of Investigatory Powers Act, ou RIP) n'autorise actuellement qu'une rétention limitée des informations, mais on peut imaginer que d'ici 2016, les services de police et de sécurité auront fait pression pour que les « vides juridiques » soient comblés, probablement suite à quelque affaire de terrorisme ou de pédophilie ayant défrayé la chronique.

³³ Le terme 'cracking' signifie « violer l'intégrité d'un système informatique », *The New Hacker's Dictionary*, http://www.outpost9.com/reference/jargon/jargon_toc.html

³⁴ D'après certaines estimations, les jeux en ligne dits « massivement multijoueurs » rassemblent quelque 13 millions d'abonnés, les plus populaires étant *World Of Warcraft*, <http://www.worldofwarcraft.com/index.xml> et la série coréenne *Lineage I* (<http://www.lineage.com/>) et *II* (<http://www.lineage2.com/>). Certains jeux virtuels sont plus proches du monde réel, comme p. ex. *Second Life* : <http://secondlife.com> . Ces jeux sont de plus en plus « immersifs », et l'économie qu'ils génèrent côtoie de plus en plus le monde réel, certains objets virtuels étant même vendus sur les sites d'enchères comme *ebay* (<http://www.ebay.com>). Le site *MMOGCHART.COM* (<http://www.mmogchart.com/>) fournit un certain nombre de données statistiques.

³⁵ Certains exemples de « surveillance virtuelle » ont déjà été signalés ; consulter, p. ex. : « Confessions of a Virtual Intelligence Analyst », *Terranova*, 15 mars 2006,

http://terranova.blogs.com/terra_nova/2006/03/confessions_of_.html . Les analystes spécialisés en marketing ont déjà identifié certains marchés virtuels émergents significatifs, les entreprises commencent à cibler le monde des jeux (cf. , p. ex. : Burns, E., « Marketing Opportunities Emerge in Online Gaming Venues », *ClickZ*, 1er août 2006, <http://www.clickz.com/showPage.html?page=3623035>), et les premiers « panneaux d'affichage virtuels » ont déjà été lancés, voir : Shields, M., « Massive Unveils Toyota Ad Units Within Anarchy », *Mediaweek*, 19 juillet 2006, http://www.mediaweek.com/mw/news/interactive/article_display.jsp?vnu_content_id=1002876380 .

³⁶ Ceci fait suite à un certain nombre d'incidents survenus pendant plusieurs années en relation avec les jeux en ligne massivement multijoueurs, les MMOG, et le monde criminel ; voir, p. ex. : « Chinese gamer sentenced to life », *BBC News*, 8 juin 2005, <http://news.bbc.co.uk/1/hi/technology/4072704.stm> .

³⁷ McCahill, M. et Norris, C. (2003), « Estimating the Extent, Sophistication and Legality of CCTV in London », M. Gill (éd.) *CCTV*, Leicester : Perpetuity Press.

³⁸ Norris, C et Armstrong, G. (1999) *The Maximum Surveillance Society: The Rise of Closed Circuit Television*, Oxford : Berg, 42.

³⁹ Norris, C. (2006) « Closed Circuit Television: a review of its development and its implications for privacy », document préparé pour la réunion trimestrielle du *Department of Home Land Security Data Privacy and Integrity Advisory Committee*, 7 juin, San Francisco, Californie.

⁴⁰ Gill, M. et A. Spriggs (2005). *Assessing the Impact of CCTV*. Londres : Home Office Research, Development and Statistics Directorate, 43, 60–61.

⁴¹ Wilkins, G. et Additcott, C. (1998) *Motoring Offences England and Wales 1996*, Home Office Statistical Bulletin, Londres : Home Office ; Ransford, F., Perry, D. Murray, L. (2005) *Motoring Offences and Breath Test Statistics: England and Wales 2003*, Home Office Statistical Bulletin, Londres : Home Office

⁴² McCahill et Norris, 2003, *op cit.*.

⁴³ PA Consulting (2004) *Denying Criminals the Use of the Road*, PA Consulting (2004) *Denying Criminals the Use of the Road*, http://police.homeoffice.gov.uk/news-and-publications/publication/operational-policing/ANPR_10.000_Arrests.pdf?view=Binary .

⁴⁴ *ibid.* : 6.

⁴⁵ *ibid.* : 18.

⁴⁶ Il existe de nombreux projets potentiels. Consulter, p. ex. : Independent Transport Commission (2006) *Paying to Drive*, http://trgl.civil.soton.ac.uk/itc/p2d_main.pdf .

⁴⁷ L'inconvénient d'un tel système réside dans le fait que l'organisation n'embauchera qu'un certain type d'employés, limitant ainsi la diversité de sa main d'œuvre – Consulter le rapport d'expert en matière de surveillance sur le lieu de travail (Workplace Surveillance Expert Report).

⁴⁸ NPS (2006a) - National Probation Service - *Electronic Monitoring*: 6.

<http://www.probation.homeoffice.gov.uk/output/Page137.asp#Current%20Programmes> .

⁴⁹ Le projet HDC prévoit la libération anticipée (entre 2 semaines et 4 mois et demi avant terme) des prisonniers dont la peine est comprise entre 3 mois et 4 ans, avec obligation de « couvre-feu » contrôlée par surveillance électronique. En 2004/5, 19.096 prisonniers ont bénéficié de cette mesure (NPS, *op. cit.*:6).

⁵⁰ NPS, *op cit.*

- ⁵¹ Pour de plus amples informations, consulter le site Internet PETS du Ministère britannique de l'environnement, de l'alimentation et des affaires rurales (Department of Environment, Food and Rural Affairs, ou DEFRA) : <http://www.defra.gov.uk/animalh/quarantine/pets/index.htm> .
- ⁵² La société impliquée est Verichip Corporation : <http://www.verichipcorp.com/> ..
- ⁵³ Amal Graafstra est l'un des fervents partisans de l'auto-implantation. Son site Internet offre des informations, des images et des vidéos : <http://amal.net/rfid.html> .
- ⁵⁴ Graham-Rowe, D., « Clubbers chose chip implants to jump queues », *New Scientist*, 21 mai 2004, <http://www.newscientist.com/article.ns?id=dn5022> .
- ⁵⁵ Waters, R., « US group implants electronic tags in workers », *Financial Times*, 12 février 2006, <http://www.ft.com/cms/s/ec414700-9bf4-11da-8baa-0000779e2340.html> .
- ⁵⁶ Le UK Design Council définit le terme « brandscape » de la façon suivante : « La portée expérientielle totale et le pouvoir de sollicitation d'une marque. Un terme qui rassemble tous ceux qui entrent en contact et qui ont des rapports avec la marque, y compris les clients, fournisseurs, employés, concurrents, revendeurs, distributeurs, partenaires etc. » : http://www.design-council.org.uk/webdav/harmonise?Page/@id=6046&Session/@id=D_rPjLjJbFNakH0E0GQvIo&Document%5B@id%3D5232%5D/Chapter/@id=7 .
- ⁵⁷ Ceux-ci sont déterminés après vérification de leur solvabilité et de leur profil client. Être un client privilégié signifie être susceptible de dépenser davantage. L'implant devient un symbole de statut social.
- ⁵⁸ Cf. Baja Beach (nd.) « Zona VIP » <http://www.bajabeach.es/> .
- ⁵⁹ Ceci permettra d'enregistrer, dans la base de données, les choix futurs de ces consommateurs.
- ⁶⁰ Cf. « Oyster data use rises in crime clampdown », *The Guardian*, 13 mars 2006, <http://politics.guardian.co.uk/foi/story/0,,1730771,00.html> .
- ⁶¹ Consulter la célèbre étude d'Oscar Gandy : *The Panoptic Sort: A Political Economy of Personal Information*, Boulder, CO : Westview, 1993.
- ⁶² Ce système existe déjà à l'état embryonnaire aux Etats-Unis. Voir, p. ex. : Leff, L. « Students ordered to wear tracking tags », *Associated Press*, 9 février 2005, <http://www.msnbc.msn.com/id/6942751/> .
- ⁶³ Voir, p. ex. : « Neglect ruling in girl pond death », *BBC News*, 23 mars 2006, http://news.bbc.co.uk/1/hi/england/coventry_warwickshire/4837614.stm .
- ⁶⁴ Au Royaume-Uni, les établissements scolaires sont classés en fonction des résultats aux examens de leurs élèves.
- ⁶⁵ Par exemple Nestlé, Unilever, Pepsico, etc.
- ⁶⁶ Le programme USVISIT (United States Visitor and Immigrant Status Indicator Technology) est en place à tous les points d'entrée terrestres, aériens et maritimes depuis 2004.
- ⁶⁷ Cf. : Amoore, L. (2006) « Biometric Borders: Governing Mobilities in the War on Terror », *Political Geography* 25(2) : 336-351.
- ⁶⁸ « Criminal records mix-up uncovered », *BBC News*, 21 mai 2006, <http://news.bbc.co.uk/1/hi/uk/5001624.stm> .
- ⁶⁹ Cf. : Grayling, A.C. (2005) *In Freedom's Name: The Case against Identity Cards*, Londres : Liberty.
- ⁷⁰ Consulter l'excellent ouvrage consacré à la socialité de la vie privée : Regan, P. (1995) *Legislating Privacy*, Chapel Hill : University of North Carolina Press.
- ⁷¹ Cf. : Ericson, R. et Haggerty, K. (1997) *Policing the Risk Society*, Toronto : University of Toronto Press.
- ⁷² L'association des assureurs britanniques (Association of British Insurers, ou ABI) a demandé la mise en place d'un tel système dans un important rapport consacré au logement : ABI(n.d.) *Securing the Nation: The Case for Safer Homes*, Londres : ABI, 12. <http://www.abi.org.uk/BookShop/ResearchReports/Securing%20the%20Nation%20July%202006.pdf>
- ⁷³ On imagine ici que les ordonnances sur les comportements anti-sociaux (Anti-Social Behaviour Order), les programmes de surveillance intensive (Intensive Supervision) et autres mesures analogues (cf. rapport d'expert en matière criminelle et judiciaire) ont été réunis au sein de programmes généraux baptisés « Personal Behaviour Schemes » ou PBS (surveillance des comportements individuels) destinés aux personnes correspondant à certains profils de risque en matière de délinquance. Dans la mesure où les résidents de la cité Dobcroft remplissent au moins un des critères puisqu'ils habitent dans une cité où la criminalité est latente, ils font tous l'objet de programmes PBS.
- ⁷⁴ L'intérêt croissant pour une intervention précoce s'étend déjà jusqu'à la naissance ; voir, par ex. : Woolf, M., « 'Failures' targeted at birth », *The Independent*, 16 juillet 2006, <http://news.independent.co.uk/uk/politics/article1180225.ece> .
- ⁷⁵ La soi-disant « biocriminologie », ou l'étude des aspects génétiques liés aux comportements criminels, rencontre un intérêt croissant à l'heure actuelle ; voir, par ex. : Rose, D. (2006) « Lives of crime », *Prospect* 125(Août), http://www.prospect-magazine.co.uk/article_details.php?id=7604 . Pour une critique antérieure

de cette approche, consulter : Rose, N. (2000) « The biology of culpability: pathological identity and crime control in a biological culture », *Theoretical Criminology*, 4 (1), 5–34.

⁷⁶ En 2016, l'incarcération n'est qu'un des divers échelons du programme PBS. L'assistance sociale, la probation et l'incarcération font désormais partie d'un système homogène géré, dans la plupart des cas, par le secteur privé.

⁷⁷ Clôturée en 2010, soi-disant pour renforcer la sécurité des résidents, la cité Dobcroft ne dispose que de quatre entrées et sorties surveillées par des agents de proximité, des caméras et des scanners RFID.

⁷⁸ Un système expérimental similaire a été introduit à Shoreditch (Londres) en 2006. Il a été immédiatement baptisé « ASBO TV » ; voir, par ex. : Swinford, S., « Asbo TV helps residents watch out », *Times Online*, 8 janvier 2006, <http://www.timesonline.co.uk/article/0,,2087-1974974,00.html> .

⁷⁹ Consulter l'éditorial du *New York Times* : « The data-fleecing of America », 21 juin 2005.

⁸⁰ Cf. Bennett, C. et Raab, C. (2006) *The Governance of Privacy: Policy Instruments in Global Perspective*, 2e édition, Cambridge, MA : MIT Press

⁸¹ La pratique du « life logging » (consignation électronique de l'existence) dérive du blogage sur Internet. De nombreuses technologies ont déjà été développées dans ce domaine ; voir, p. ex. : Ward, M. « Log your life via your phone », *BBC News*, 10 mars 2004, <http://news.bbc.co.uk/1/hi/technology/3497596.stm> .

⁸² Consulter le rapport d'expert relatif aux frontières, et l'exemple de la milice des Minutemen aux Etats-Unis : <http://www.minutemanproject.com/> .

⁸³ Ce type d'incident s'est déjà produit lors du mouvement de psychose concernant les pédophiles, une pédiatre ayant été chassée de son domicile en 2000 ; cf., p. ex. : Allison, R., « Doctor driven out of home by vigilantes », *The Guardian*, 30 août 2000, <http://www.guardian.co.uk/child/story/0,7369,361031,00.html> . Nous imaginons simplement qu'en 2016, les technologies faciliteront la diffusion plus rapide et plus large de telles erreurs.

⁸⁴ De nombreux manuels consacrés à ces méthodes de résistance existent déjà ; voir, p. ex. : « Guide to Closed Circuit Television (CCTV) destruction », *Schnews*, <http://www.schnews.org.uk/diyguide/guidetoclosedcircuittelevisioncctvdestruction.htm> .

⁸⁵ Cf. Mann, S., Nolan, J. et Wellman, B. (2004) « Sousveillance: inventing and using wearable computing devices for data collection in surveillance environments », *Surveillance & Society*, 1(3), 331–355.

⁸⁶ La technique RFID (identification par radiofréquence) fonctionne en visibilité directe. Les micro-ondes, les tôles, les briques, et même la sève des arbres peuvent créer des interférences ; cf., p. ex. : « RFID Technology », *RFID Centre*, <http://www.rfidc.com/docs/rfid.htm> .