

RIEN À CACHER, RIEN À CRAINDRE ?

David Lyon, l'Université Queen's

Conférence pour la Ligue des Droits et Libertés, Montréal, le 30 janvier 2010.

La surveillance comme un mode de vie

Tout le monde sait que les gens sont sous contrôle quand ils se rendent à un aéroport. Vous vous attendez à voir vérifiées vos coordonnées au comptoir des compagnies aériennes ou par le système de billetterie électronique; comme vous savez aussi que vous devez passer par la sécurité. Là, votre carte d'embarquement est vérifiée et votre bagage à main passe par la machine de la numérisation tout en traversant la voûte électronique, et ainsi, peut-être obtenez-vous le feu vert comme par baguette magique. Si vous êtes à Londres Heathrow ou sur certains sites équipés de façon similaire, un contrôle biométrique est surajouté à l'appareillage de surveillance : vous devez alors fixer un objectif d'appareil photographique durant une ou deux secondes. Et si votre destination se trouve dans un autre pays, les douanes et les services d'immigration exigeront davantage de données. Personne ne sera surpris d'apprendre que vous êtes également surveillés par caméras vidéo, même si vous avez été trop préoccupés par le besoin de repérer les emplacements où d'autres recherches s'effectuent.

Au Canada, les écrans vidéo peuvent être consultés par les opérateurs à l'aéroport, mais les images des principaux aéroports internationaux sont également disponibles au siège de la rue Bank de l'*Administration canadienne de la sûreté du transport aérien*, à Ottawa. Ainsi, alors que vous faites face à la sécurité, à Vancouver par exemple, un agent, à 3 500 kilomètres de distance, peut observer la scène. Non seulement cela, mais ils peuvent effectuer un zoom pour lire votre carte d'embarquement ou vérifier leur écran pour voir la radiographie par rayons X d'éventuels objets suspects dans votre sac. Aux États-Unis, les tests réussis du corps entier sous images ont mené l'*Administration de la Sécurité du Transport* à décider, en 2009, que cette méthode doit être introduite progressivement de préférence à celle du balayage à détection des objets métalliques. Les images radiographiques du corps dévêtu sont transmises et vues, nous en sommes convaincus, par des opérateurs, à un emplacement éloigné, incapables de relier l'image avec la personne radiographiée. Le même délicat équipement est également utilisé au Canada (il sera installé en 2010) bien qu'outre atlantique, le Parlement européen ait rejeté le scanner corporel, en 2008.

Comme je l'ai dit au début de mon propos, nous nous attendons à une forme de contrôle à l'aéroport, mais certaines personnes pourraient, et seraient, peut-être, surprises de découvrir combien elles sont observées même ailleurs. Notre présentation permettra de montrer qu'il existe de nombreuses variantes de surveillance de notre monde. Vous n'aurez pas besoin d'aller à un aéroport pour vous sentir observé ou sous contrôle. La surveillance est omniprésente. Elle fait preuve d'ubiquité. Tout n'est pas visible, mais presque. En fait, toute surveillance n'implique pas un regard direct et constant. On nous observe à travers nos relevés bancaires, nos appels de téléphone portable, les cartes de bus, de travail, de fidélité aux grandes surfaces, les passeports, les cartes de crédit, des services de santé et le numéro d'assurance sociale; sur *Google*, *Facebook* et *Twitter*. Seulement peu de ces moyens sont visibles. Mais on peut examiner beaucoup de données personnelles. Certains systèmes comme les caméras de surveillance des aéroports, sont d'une grande fidélité visuelle, tout comme les scanners corporels sont précis dans la mise à nu des passagers. Plutôt que de s'appesantir sur les légendes des bienfaits de la surveillance de haute technologie, nous allons prendre du recul et donner une vue d'ensemble du phénomène de contrôle par les temps qui courent. Après avoir défini la notion de « surveillance » à travers l'examen de quelques exemples, je vais essayer de répondre à trois questions:

Premièrement : pourquoi la surveillance prend-elle une dimension centrale dans la vie quotidienne aujourd'hui? Nous explorerons le monde des organisations pour le découvrir. Nos informations sont évaluées pour de nombreuses raisons et les organisations sont avides de ces données personnelles.

Deuxièmement : pourquoi ne prenons-nous pas pour acquis le fait que nous sommes surveillés 24 heures sur 24, 7 jours sur 7? La surveillance est une réalité de la vie contemporaine et nous donnons l'impression d'être à l'aise avec ça.

Troisièmement : pourquoi les gens commencent-ils à s'occuper de la surveillance de leur propre entourage ? En effet, le contrôle des autres n'est plus le domaine exclusif des grandes organisations.

Les gens ordinaires dans la vie quotidienne se livrent aussi à la surveillance, quelquefois de façons rudimentaire, sans connaissances techniques particulières, parfois avec l'utilisation étonnante d'un équipement de haute technologie. Une fois les gens rassurés, est-ce que la devise « si vous n'avez rien à cacher, vous n'avez rien à craindre » est encore vraie, comme une assurance absolue?

Le monde tel qu'observé aujourd'hui

Ce n'est pas arrivé soudainement, comme par une nuit un peu plus sombre. Durant les cent dernières années, les sociétés de surveillance se sont développées, mais lentement et progressivement au début, ensuite à un pas accéléré. On ne peut occulter

le fait que les sociétés de surveillance d'aujourd'hui sont quelque chose de nouveau, d'inédit et d'inquiétant à la fois. Évidemment, les gens se sont toujours observés; chose somme toute naturelle. Dans le village ancien chacun savait ce qui se passe dans la vie des autres. Mais la surveillance d'aujourd'hui, bien que semblable par quelques aspects à celle d'autrefois, est sous-tendue par une nouvelle dynamique. En partie, elle répond à une logique économique : les données personnelles n'ont jamais eu autant de valeur. Une logique organisationnelle joue aussi sur deux tableaux en déplaçant la gestion du risque à la précaution, voire à la prévention. A cela, il faut ajouter, bien sûr, une logique technologique : nous avons les moyens pour amasser et traiter les données personnelles qui n'étaient jamais disponibles auparavant pour la vieille dame derrière ses rideaux. Derrière tout ceci s'installe une forme de dépendance culturelle à l'observation et à la visibilité; *on veut le voir, pour être certain!*

Comment devrions-nous définir la surveillance aujourd'hui ? La définition de la notion nous aiderait largement à éviter des rêves fondés essentiellement sur la haute technologie (ou ses craintes), ou de privilégier les définitions opératoires relatives à la sécurité nationale qui se concentrent sur « le terrorisme ». La surveillance peut être pensée autrement, comme n'importe quelle attention soutenue, ordinaire et systématique aux détails personnels dans un but de gestion, de contrôle, de soin, d'influence ou de protection. En effet, il y a beaucoup de buts auxquels la surveillance est dévolue, mais ceux qui nous concernent, ici, impliquent tous des données personnelles. Quelques objectifs, à grande échelle, incluent la prévention du terrorisme, la réduction de la violence urbaine ou la limitation de la diffusion d'un virus de la grippe. Bien sûr, quand nous commençons à affiner cette définition, nous pouvons noter que la surveillance non-humaine est aussi significative, ou que les détails personnels peuvent être dépersonnalisés par leur séparation des données de l'identification individuelle. Mais la surveillance non-humaine, indirecte, comme le système de surveillance électronique à puces accrochées aux vêtements, peut aider à localiser des personnes. Et même combinées les données peuvent aider au profilage des gens qui reviennent dans l'image ou sur la table de contrôle.

Par contre, pour être tout à fait clair depuis le début, la surveillance n'est pas juste sinistre. Les buts qu'elle sert peuvent être positifs. J'ai été hospitalisé récemment et, après la chirurgie, il était important que les signes essentiels de mes organes vitaux puissent être observés à des fins de contrôle post chirurgical. J'ai remarqué un jour où l'infirmière est entrée dans ma salle que plutôt que de me demander comment je me sentais, elle m'a simplement dit qu'elle avait le plaisir de voir que les indications de l'électrocardiogramme montraient le bon fonctionnement de mon cœur. « Mais vous ne l'avez pas vérifié encore, ai-je répondu. Bien sûr que si, rétorqua-t-elle, il y a un branchement à distance sur l'écran de la station des infirmières. Nous vous observons sans interruption». Cette sorte de pratique adopte la même approche que celle de

l'entreprise vigilante, ordinaire, systématique quant à l'utilisation des détails personnels, maintenant adaptés aux fins des services de santé. Comme dans l'exemple précédent, les détails sont aussi intimes et passés au peigne fin. Désormais, la surveillance n'est pas nécessairement sinistre ou effrayante; elle est même fondamentalement rassurante ou sans particularité. Pas bonne ou mauvaise ou neutre, à cet égard. Pourquoi pas « neutre »?

La surveillance signifie «observer», du verbe français polysémique « surveiller » : contrôler le déroulement d'une action, veiller sur quelque chose, sur quelqu'un avec vigilance, surveiller par exemple les enfants dans la cour de l'école, se surveiller soi-même dans certaines circonstances. C'est à peine neutre. Dans sa version anglophone la plus usuelle, de signification plus étroite, disons : le contrôle de police d'un suspect, ce qui inclut toutes les sortes d'observation, l'examen minutieux ou le regard fixe constant. Et comme nous l'avons noté, le regard fixe peut être virtuel dans le sens que des données numériques peuvent être rassemblées pour que les gens et les populations puissent être mieux vus, observés, soumis à la loupe du système de surveillance. Ainsi « l'œil fixe du gouvernement » concentré sur ses citoyens peut être aidé par des informations statistiques amassées par le recensement ou par un ministère de l'emploi ou de la santé. L'état nous surveille avec des moyens spécifiques qui aident à maintenir les gens dans le respect des normes étatiques établies, à s'assurer que les impôts sont payés à temps, que les permis sont achetés pour conduire ou porter des armes à feu, ou que des minorités particulières, comme, par exemple, les nouveaux immigrants, sont traitées convenablement.

Mais notre propos ne se concentre pas uniquement sur ce j'ai nommé « l'œil fixe du gouvernement », car un peu de direction-par-surveillance est faite par des agences que nous n'associerions pas avec une quelconque structure gouvernementale. Prenez, par exemple, *Tesco*, une chaîne de supermarchés britannique majeure. Grâce à une filiale, *Tesco* dirige une base de données appelée le *Creuset* qui détermine le profil de chaque consommateur au Royaume-uni avec des détails "de personnalité", des habitudes de voyage, des préférences commerciales, les niveaux de scolarité, d'appartenance ou non au mouvement écologique, et le degré de générosité caritative. Le creuset, cette banque de données, avance que dans un monde parfait, nous saurions tout ce dont ont besoin les consommateurs ... leurs attitudes, leur comportement, et leur style de vie. En réalité nous ne saurons jamais autant que nous le voudrions.

La filiale *Tesco* utilise un système logiciel appelé le *Zodiaque* pour la « définition du profil intelligent » visant, avec le concours du *Creuset*, la production d'une carte qui permettrait de savoir ce que les individus pensent au sujet du travail et du magasinage. Ainsi, les consommateurs sont classifiés dans une des dix catégories suivantes: richesse, promotions, voyage, charité, écologie, loisir, crédit, style de vie, personne traditionnelle ou non.

Le « *Club card* » est utilisé comme une source de données, mais il existe aussi des courtiers qui disposent d'informations énormes : *Experian*, *Claritas* et *Equifax*, également d'autres geysers publics comme les listes électorales, le *Bureau du cadastre* et le *Bureau National des Statistiques*. Pourquoi tout cet arsenal est-il valable, mobilisable? Seulement parce que la compagnie sait sur quel point concentrer ses énergies, beaucoup mieux que des clients qui se présentent à la cour avec des arguments souvent ignorés.

Un autre exemple pour expliciter. Au Canada, un cadre chez *Canadian Tire*, la compagnie d'électronique, d'articles de sport, d'automobiles et d'ustensiles de cuisine, a décidé en 2002 de faire un inventaire précis de toutes les ventes par carte de crédit. Que voulait-il montrer ? Ses résultats donnèrent comme hypothèses que les gens achetant l'huile de moteur générique allaient, probablement, moins payer de dettes; les gens achetant des moniteurs de monoxyde de carbone ou des pièces de protection pour les pattes des meubles afin de protéger les planchers rembourseraient rapidement, à la différence de ceux optant pour des accessoires de voiture à l'avant chromé. Prendre une bière dans un bar particulier à Montréal a été associé à de mauvais risques, mais acheter des graines haut de gamme pour les oiseaux ne l'était pas. La définition du profil psychologique était l'étape suivante (associer les gens qui protègent leurs affaires, leur niveau de crédit, à ceux qui se soucient de protéger leur plancher des pattes de meubles nécessite un travail approfondi sur les attitudes et comportements). Par ce moyen, l'entreprise prédit leur comportement, par exemple : quoi couper, quand ils vont s'inscrire pour un « *shower* » de bébé ou une liste de mariage quand la limite de leur marge de crédit est atteinte? Et même : quand auront-ils besoin de thérapie de couple?

Les dernières utilisations pourraient facilement envoyer des signaux de mauvais risques sur les gens perdant leur emploi. Aussi est-il approprié de se poser la question quant au bien fondé de cet usage qui est pour le moins pénalisant? C'est une question sur laquelle nous reviendrons quand nous aurons considéré un peu plus d'exemples.

L'utilisation de données personnelles pour toutes sortes d'objectifs, souvent bien au-delà de ce que nous pourrions imaginer, montre que cela signifie quelque chose d'en parler comme d'un paradigme ayant pour appellation « la surveillance ». On peut nous observer dans le détail, nous passer au crible du tamis informationnel, fouiller notre vie intime par les profils construits non seulement par la police ou des responsables de la sécurité, mais aussi par des sociétés. Nous ne pouvons pas admettre que traîner dans un bar peut être associé au non paiement de factures, de carte de crédit, mais pour la compagnie nous faisons partie d'un ensemble de statistiques, dans lequel on ne peut pas avoir entièrement confiance. Ici aussi, nous pouvons discerner les trois « logiques » en action : l'économique, l'organisationnelle et la technologique. Ces données

personnelles sont étonnamment d'une grande valeur (il existe clairement un grand marché pour elles), particulièrement pour les organisations tenant à réduire les risques auxquels elles font face (comme les défauts des détenteurs de carte de crédit) et le logiciel intelligent et la statistique sont disponibles pour aider à maximiser leur utilisation (cela fait partie de la technologique).

Donc nous habitons un monde observé de près tant visuellement (appareils photos, caméras de surveillances vidéo omniprésentes) que pratiquement (profils numériques par lesquels on « nous voit » métaphoriquement). L'image vidéo a ses conséquences, tout comme l'image numérique. Maintenant nous ferons un zoom pour analyser plus étroitement le travail des organisations et pourquoi elles désirent ardemment la récolte des données. C'est le premier aspect de la vie dans une culture de surveillance.

LA SURVEILLANCE COMME MODE DE VIE : LES ORGANISATIONS NOUS OBSERVENT

C'est sans exagération aucune que nous pouvons dire que la surveillance représente l'aspect le plus important dans la vie organisationnelle d'aujourd'hui. Il s'est étendu pour devenir l'élément-clé avec lequel les organisations travaillent, ou opèrent. L'ingrédient essentiel de gestion réussie c'est celui qui permet de connaître en détail les consommateurs, les clients, les citoyens, les étudiants, les contrevenants, les voyageurs ou les patients avec qui l'organisation a à faire. Bien que les hommes d'affaires puissent dire qu'ils veulent connaître leurs clients comme les banques démodées les propriétaires de magasin de proximité, en réalité ils trouvent les voies et moyens de tout savoir d'eux. Les structures gouvernementales ou de la sécurité des frontières collectent les données personnelles et cherchent les façons ingénieuses de mettre ces données ensemble dans des groupes significatifs pour que les tendances puissent être perçues et le comportement prévu.

Pour le dire autrement, les organisations s'efforcent d'enlever les couvertures afin de nous rendre de plus en plus visibles à elles. Selon notre point de vue, comme citoyens ordinaires, voyageurs, ouvriers ou consommateurs, nos vies sont de plus en plus transparentes à toutes les pratiques de gestion des agences. La tendance ne montre aucun signe de ralentissement. Plus dramatiquement nous sommes nus en ce monde. Les choses remontent loin. En effet, déjà dans les années soixante, le sociologue américain pop Vance Packard a écrit *La société nue*. Un fabricant pourrait-il oser contrôler des machines pour vérifier si elles sont utilisées à un bon niveau de rendement, se demanda-t-il, ou un magasin suivre secrètement des clients pour des vols éventuels ou des achats orientés, ciblés? Un demi-siècle plus tard, nous aurions été surpris s'ils n'avaient pas mis en pratique les prédictions de Packard. Comme nous

l'avons remarqué dans le domaine de la sécurité le « passager nu » des compagnies aériennes est maintenant une réalité littérale et pas une fiction ou une conjecture de sociologue. Sans doute, la surveillance Internet a grandi exponentiellement puisque, depuis 1991, le *World Wide Web* est utilisé sans restriction, à une grande échelle. La recherche de nouveaux logiciels pour rendre les utilisateurs transparents aux organisations est constante. En 2009, par exemple, « *Webwise* » est devenu disponible, il permet aux fournisseurs d'accès à Internet de proposer des placards publicitaires aux clients, basés sur des habitudes navigantes en ligne plutôt que seulement sur le contenu d'une page simple; ce moyen est opérationnel actuellement. Irrité, Berners-Lee, le fondateur du Web, a protesté en ces termes : « je veux savoir que quand je clique pour un contact, ça doit rester entre moi et le Web, et que le fournisseur d'accès à Internet ne va pas immédiatement me ranger dans des catégories pour la publicité ou l'assurance ou pour l'utilisation gouvernementale ». Si mon courrier n'est pas lu et que la société de téléphone n'écoute pas mes appels, a-t-il continué, pourquoi Internet ne devrait-il pas s'aligner sur ces comportements éthiques, d'autant plus qu'il est souvent utilisé pour des échanges intimes ?

Une bonne question, sans aucun doute, mais il n'est pas sûr que beaucoup d'opérateurs y prêteront attention. Pour eux ce ne sont pas non seulement des données Internet constamment maquillées à des fins commerciales, mais des informations sur lesquelles les gouvernements aimeraient mettre la main, donc monnayables d'une manière ou d'une autre. La proposition la plus audacieuse est jusqu'à présent apparue en Grande-Bretagne en 2008, pour une base de données contenant tous les appels téléphoniques, des courriers électroniques et l'utilisation Internet (incluant des services Internet de liaison sonore comme *Skype*) dont les enregistrements seraient conservés pendant une année.

Le Royaume-Uni a soutenu un tel projet depuis les attentats à la bombe de Londres en 2005, mais il semble maintenant être également appuyé par l'Union Européenne. En 2009, une Directive de l'Union Européenne est entrée en vigueur afin de contraindre des fournisseurs d'accès Internet à conserver toutes les informations des courriels et des visites de site Web aussi bien que des coups de téléphone et des *sms*. Dans ce cas, la surveillance de la population de tout un pays serait conduite également par l'utilisation de l'internet pour des buts de sécurité et de maintien de l'ordre.

Il est incontestablement clair que des organisations de toutes sortes nous observent mais la question qui s'impose devrait être celle-là : pourquoi ? Les différentes pressions des organisations peuvent s'expliquer par la recherche de l'efficacité, la productivité, la vitesse, la concurrence, et d'autres choses de ce genre. Il est évident que de plus en plus on voit le traitement des données personnelles comme une façon d'atteindre ces buts. En effet, les pratiques de surveillance peuvent être pensées, voire légitimées comme la méthode préférée et privilégiée des organisations qui fonctionnent, et

tiennent un couloir dans la course aujourd'hui. Comment cela est-il arrivé ? Par un certain nombre de courants culturels profonds qui positionnent la surveillance comme une solution aux problèmes sociaux et politiques, mais également sur le plan organisationnel il y a deux jalons majeurs que nous devons examiner objectivement. Le premier renvoie à la première expansion moderne de la bureaucratie, qui à partir de règles raisonnables a pris l'habitude d'augmenter l'efficacité, et le deuxième à l'utilisation moderne postérieure d'informations et des technologies de communication pour ajouter la vitesse et la flexibilité au mélange. Laissons la question bureaucratique de côté pour le moment, concentrons-nous de nouveau sur l'utilisation des nouvelles technologies.

Au début des années 1990, le traitement des données personnelles est devenu de plus en plus important dans les organisations et les conséquences de la surveillance multipliées une fois de plus. Le courrier indésirable était déjà une irritation mineure, mais maintenant des messages marketing viennent avec le nom du propriétaire "personnalisant" des annonces pour tout : de la pizza au parfum et des divans aux couches pour bébés. Oui, les couches! D'une façon ou d'une autre ces agents de marketing savaient qui attendait des bébés, qui partait à la retraite bientôt, qui étaient des fins connaisseurs en vins et qui aime changer fréquemment de voiture. Maintenant qu'*Amazon.com* est bien connu pour, étrangement, aider des clients à choisir les livres qui leur conviendraient, une telle connaissance organisationnelle de nos habitudes de dépenses est somme toute banale. Mais dans les années 1990, pour quelqu'un qui y a réfléchi deux fois, il y avait quelque chose de sinistre, voire d'inquiétant dans les annonces personnalisées. Comment ont-ils pu savoir ?

La réponse est qu'un peu de travail à faible composante technologique se faisait à l'arrière-plan, des ouvriers d'entrée de données, féminins principalement, mal payés assemblaient des informations dans le domaine public - à la maison, sur la propriété de véhicule, des comptes rendus d'audience, des résultats scolaires, des adresses, des numéros de téléphone, etc. sur des individus. Aujourd'hui, construisant sur cela, la méthode des agences consiste à s'appuyer sur une telle récolte de données. Celles-ci classent les populations dans des catégories pour qu'elles puissent être traitées convenablement et souvent pour vendre les informations aux grands courtiers de données. Les clients des années 1990 ont été étonnés d'apprendre que les sociétés savaient beaucoup de choses de leur vécu antérieur.

Aujourd'hui, les sociétés savent non seulement cela mais peuvent, avec le *GPS*, suivre le positionnement terrestre de leurs clients à tout moment. En effet, une société américaine de téléphone, *Nextel*, a révélé ces informations aux agences d'application de la loi. En octobre de 2009, *Nextel*, grâce au portail de son représentant chargé de faire respecter la loi pertinente en la matière, a divulgué l'existence de plus de 8 millions d'emplacements clients.

La base de données *Marketing* aux fins de commercialisation était, peut-être, le site le plus évident, mais ce n'était en fait qu'un parmi beaucoup de domaines où la soif de données s'est rapidement développée. Malgré quelques balises légales et techniques, des minces filets de données personnelles se sont transformés en une inondation telle qu'il est maintenant impossible de suivre tous les conduits et de remonter les ruisseaux jusqu'à leur source. Les données personnelles sont plus que jamais utilisées. Un peu comme les personnages du roman de Kafka, *Le procès*, nous ne saurons jamais exactement qui sait quoi et pourquoi ? Évidemment les conséquences suivront, et cela malgré que nous soyons conscients que nous sommes sous surveillance.

La surveillance comme mode de vie : nous savons que nous sommes observés.

Une petite dose d'observation, c'est certainement subtil; tout comme il existe quelques sphères de surveillance dont nous sommes inconscients, certains d'entre vous ont certainement manqué au moins quelques signes émis par des sociétés de surveillance. Nous n'avons, cependant, pas besoin de ce sixième sens qui nous signale un observateur caché. En effet, les têtes teintées des objectifs des caméras décorent le plafond et les publicités surgissent sur l'écran tout près, directement à partir de quelques mots-clés dans le courrier électronique fraîchement envoyé. Nous savons que même si nous conduisons sur une autoroute à péage – comme l'Autoroute 407 en Ontario - sans passer par les postes de péage, les appareils photos saisiront nos plaques d'immatriculation. Même si la voiture n'est pas munie d'un pare-brise transparent la facture sautera dans notre boîte aux lettres de toute façon. Nous pouvons commander une pizza d'une grande chaîne tout en étant conscients qu'ils connaissent nos préférences justes à cause du numéro de téléphone. Et nous devons leur signifier de manière claire que, pour une fois, nous ne voulons pas une pizza avec la recette habituelle.

Au-delà de l'appétit des organisations pour nos données personnelles, il faut noter un aspect non moins important de la culture de surveillance à savoir que les sujets le savent, en sont conscients. La surveillance, de notre temps, peut être discrète dans certaines situations, mais dans beaucoup d'autres, le sujet est en même temps objet de ce contrôle. En effet, l'employé de bureau chargé des entrées de données ou l'opérateur du centre d'appels n'ignorent pas que les sollicitations sont comptabilisées et contrôlées à des fins d'évaluation qualitative. Le camionneur est conscient que le camion porte un « Comment est ma conduite ? », affiché à l'arrière, grâce auquel les autres automobilistes peuvent appeler l'employeur quand certains bons ou mauvais comportements de conduite sont observés. Le consommateur se promenant dans la rue, faisant du lèche-vitrine, peut, clairement, voir le signe indiquant que le magasin est sous surveillance vidéo; au même moment le surfeur Internet est conscient que les sites visités incluent souvent leurs politiques privées qui expliquent dans quel but les données personnelles, amassées par le propriétaire, peuvent être utilisées.

Les comportements des citoyens conscients des effets de la surveillance peuvent changer. L'employé de bureau, à ma pharmacie locale ne manque jamais de me demander si je possède une « *Carte Optimum* » de fidélité quand je fais un achat. Je réponds invariablement non et ensuite je n'ai droit à aucun remerciement quand on me demande si je voudrais en bénéficier. D'autres magasins veulent des numéros de téléphone et des codes postaux et, de nouveau, on peut entendre des réponses variées. Certains se conforment simplement à la demande, d'autres questionnent sur la pertinence d'avoir telle ou telle carte ou refusent poliment. Un tel refus s'appuie, évidemment, sur la connaissance préalable que de telles données apparemment innocentes peuvent devenir une clé pour l'accès à d'autres données personnelles. Et il faut le dire sans ambages, les interrogations que suscitent une telle surveillance quotidienne sont une pratique louable.

Cependant, de tels actes individuels, cognitifs, de résistance, bien qu'importants ne seront probablement pas très efficaces eu égard à l'énorme déséquilibre par rapport au pouvoir des organisations détentrices de systèmes de surveillance. Il est vrai aussi que quelques actions de citoyens face à la surveillance peuvent être significatives, par exemple lorsque des photos ou des films vidéo sont utilisés suite aux manifestations comme celles de l'élection contestée, en Iran en 2009. Mais plus souvent, les actes de protection de soi – qui sont aussi des signes que nous sommes conscients de la surveillance - tels que le fait de mentionner le caractère privé des photos sur *Facebook* ou de questionner le fait d'avoir au centre-ville un appareil enregistreur n'auront pas beaucoup d'effet. Cependant, au moment où nous sommes encouragés par beaucoup de moyens à nous assurer de notre propre protection contre les dérives de la culture de surveillance, la question essentielle, de l'ordre du politique touche au défi qu'il faut relever contre les organisations afin qu'elles s'imposent une éthique de gestion des données privées récoltées souvent à l'insu des citoyens. La responsabilité des organisations de surveillance est bien plus significative que notre responsabilité personnelle en tant que cibles.

Beaucoup plus peut être dit de la résistance à la surveillance, mais à cette étape c'est l'examen valable d'un autre phénomène qu'il faut entrevoir : les moyens qui font que la surveillance ne peut pas être totalement évitée ni adoptée. Les cultures de surveillance semblent engendrer d'autres niveaux d'observation. Plutôt que d'éviter la surveillance, certains, apparemment, s'en accommodent.

La surveillance comme mode de vie : nous pouvons aussi surveiller.

Nous sommes observés et nous en sommes conscients mais nous en soucions-nous ? Une troisième dimension de la culture de surveillance fait que nous répliquons aujourd'hui à la surveillance. Certains font de la surveillance pour eux-mêmes. En effet, pourquoi les organisations devraient-elles avoir un monopole du contrôle ? Nous aussi

nous pouvons observer. Les voies banales incluent des téléphones portables utilisés pour trouver d'autres utilisateurs de *GPS*, certains utilisent des réseaux médiatiques sociaux comme *Facebook* pour découvrir des détails sur des voisins, des collègues ou des amis, d'autres installent *nannycams* pour surveiller la gardienne ou espionner la navigation sur Internet de ses enfants.

Les moyens extrêmes de la surveillance cachée incluent celui de Steve Mann de l'Université de Toronto qui fait dissimuler une caméra dans ses verres ou, encore plus bizarre, mais aussi celui de Rob Spence qui consiste à installer une caméra vidéo numérique dans un œil artificiel. L'*effet Mann* est une histoire de technologies prothétiques pour prolonger les capacités visuelles et audio. Il a passé plus de 20 ans à perfectionner le métier. Il réalisera son objectif de caméras aériennes de centres commerciaux, enregistrera des échanges compromettants avec le personnel, et en détail. Rob Spence, originaire de Belleville en Ontario, est un cinéaste qui aspire à être ce qu'il appelle un « *eyeborg* », observant et enregistrant ceux qui se situent dans son champ visuel pour rendre les gens plus conscients de l'omniprésence de la surveillance, peut-être en tant que phénomène social.

Je soupçonne que peu d'entre nous aspirent à être *eyeborgs* mais cela ne signifie pas que nous ne nous engageons jamais dans la surveillance de bricolage. Si vous tapez sur *Google* le mot « surveillance » et même plus, si vous ajoutez le mot « caméra » beaucoup de suggestions vont apparaître pour répondre à toutes vos attentes quant à l'installation de votre propre système de surveillance et que la société vous vendra l'équipement à installer vous-même. « Protégez votre maison et vos biens contre les actes de vandalisme » vous en offre un; « La navigation libre, libérez le support technique, » un autre. Et bien sûr, pour des personnes à l'affût de bonnes affaires on promet « un assortiment de caméras de surveillance neuves ou usagées à bas prix » sur *e-Bay*. Tout cela repose sur l'idée qu'il faut d'être capable de vérifier qui est à la porte de la maison ou sur la propriété ou alternativement, pour les avoir à l'œil, comme sur votre gardienne d'enfants ou vos animaux de compagnie. Harold Hutt, le chef de la police à Houston, au Texas, pense que les caméras de surveillance domestique sont une si bonne idée qu'elles devraient devenir un élément du code de construction.

Si pour Harold Hutt la sécurité publique est une priorité, ce n'est pas le cas des personnes déployant leur propre système de surveillance à des fins d'intérêt personnel ou de protection des membres de la famille de dangers éventuels. Il existe une intense activité dans le royaume appelé « *snooping* » ou l'espionnage des autres, particulièrement quand les parents sont concernés. Selon l'étude *Pew Internet* et *American Life* plus de la moitié des parents questionnés ont reconnu avoir utilisé le contrôle d'un logiciel pour s'informer des activités en ligne des enfants ou un filtre Internet pour bloquer l'accès aux sites inopportuns.

Donc la culture de surveillance devient visible non seulement dans les grandes corporations utilisant la haute technologie; ce qui signifie : suivre à la trace et contrôler nos activités quotidiennes. On peut aussi concevoir, plus ou moins consciemment, cette possibilité comme étant aussi des réponses à la surveillance. Je m'explique, de façon plus saisissante, la culture de surveillance est évidente quand les gens ordinaires commencent à utiliser eux-mêmes la surveillance pour organiser leurs vies, protéger leurs maisons ou leurs familles, ou vérifier ce que leurs associés ou enfants peuvent faire. Ou les parents. Quelques familles aux USA ont consenti à avoir leurs parents âgés, souffrant de la maladie d'Alzheimer ou de perte de mémoire, porteurs de la puce RFID¹ pour les empêcher de trop s'éloigner, et pour les retrouver quand ils sont perdus.

La culture de surveillance d'aujourd'hui est sans précédent. Jamais on n'a investi autant de temps, d'énergie et d'argent dans l'observation des d'autres avec autant de conséquences. Maintenant, après avoir analysé certaines des dimensions- clés de la culture de surveillance, que pouvons-nous en conclure ? Dans nos vies quotidiennes nous sommes observés par un nombre extraordinaire de moyens, mais conscients, nous avons fait la paix avec tout cela. En effet, inspirés, peut-être, par la fréquence et la disponibilité de nouveaux dispositifs de surveillance, beaucoup sont même disposés à adopter quelques stratégies de surveillance pour eux-mêmes. Il ne s'agit plus clairement et simplement en matière de surveillance de l'équation : nous et eux, ce qui signifierait qu'elle s'exerce de haut en haut, dans un sens unique. C'est plus complexe et j'utilise pour cela la notion de « culture de surveillance » pour mieux cerner la problématique. La Surveillance est devenue un mode de vie, un aspect- clé de notre appréhension du monde, de sa perception, intégré dans notre vie quotidienne, et parfois presque inconsciemment.

Rien à cacher, rien à craindre

Aussi, quel est exactement le problème ? Parce que nous nous sommes habitués à la surveillance, que nous nous sommes habitués à cette nouvelle réalité, que beaucoup de personnes ont installé leurs propres systèmes de surveillance privée, nous avons échoué sur la nature des questions de base à poser quant aux changements massifs survenus en très peu d'années. L'idée « d'une société de surveillance » a été une fois associée aux états policiers, à la répression et réprouvée à cause de son côté abject et hideux. Le roman classique d'Orwell, 1984, nous a donné un aperçu édifiant sur la langue de « *Big Brother* » pour décrire un État auquel nous résisterions à tout prix.

Mais malgré Orwell, la société de surveillance est arrivée, sans les lourdes bottes de la répression brutale, avec les habits neufs de l'efficacité technologique. Elle n'est pas

¹ RAdio Fréquence IDentification :

venue d'un État autoritaire, mais de corporations commerciales revendiquant la meilleure connaissance possible de leurs clients afin de leur fournir seulement les marchandises et les services souhaités. Elle n'est pas apparue sur « un écran de télévision » indistinctement avec le visage effrayant de *Big Brother*, mais sur un million d'écrans de sites de réseaux sociaux et d'appareils portatifs commercialisés comme commodes, rentables et personnalisés.

Cependant, le problème est que les sociétés de surveillance d'aujourd'hui sont profondément ambiguës. On ne voit pas généralement l'efficacité, la commodité et la personnalisation comme des ennemis. Et elles ne sont non plus juste un cheval de Troie afin de duper les gens qui pensent qu'un cadeau dissimule toujours un ennemi. Non, mais les prestations sociales que promeuvent à un certain degré les nouvelles technologies de surveillance étendent les modes douteux de contrôle et de dépistage. La question cruciale à se poser sur la nouvelle visibilité est : comment son système fonctionne-t-il? Dans les sociétés où la présomption d'innocence est acceptée comme une réalité établie et protégée par la Loi, vous êtes supposés n'avoir rien à cacher, ni rien à craindre. Par conséquent les autorités ont le droit de découvrir et de viser dans le cadre de la Loi seulement ceux qui ont quelque chose de grave à cacher. Bien sûr, aucun système n'est parfait, mais on a confiance en cette règle. Aujourd'hui, la devise « rien à cacher, rien à craindre », n'est systématiquement sapée par l'ampleur de la nouvelle surveillance.

Rappelez-vous les exemples du bar et de la graine pour les oiseaux ? L'endroit où vous voulez prendre une bière à Montréal boire peut vous être préjudiciable pour le crédit bancaire. Vous êtes simplement mal catalogué selon *Canadian Tire*. Rappelez-vous le *Tesco-zodiaque* « le ciblage intelligent et la définition du profil »! Le point capital consiste à situer les gens dans des catégories significatives pour qu'ils puissent être traités différemment. La même chose est valable avec le logiciel « *webwise* » qui classe les gens grâce à leurs habitudes de navigation, pas seulement par leur visite d'une page web. Vous faites partie du monde où vous naviguez. De telles décisions d'évaluations automatisées sont faites à partir de tout, de la solvabilité aux niveaux de service après-vente et de la vitesse Internet quant à la capacité de tenir un compte bancaire. Et si vous êtes déjà marginaux ou désavantagés, le système s'assurera que ces vulnérabilités sont amplifiées, par les effets de ce qu'Oscar Gandy appelle "*l'inconvénient cumulatif*".

Mais ça ne s'arrête pas là. Ces types de classifications sont également utilisés par la police, les services de renseignement et d'autres autorités. Après le 11 septembre 2001, l'organisme qui allait devenir la Sécurité intérieure a fait une priorité de l'appel « *Customer Relationship Management* » société qui aide à localiser et identifier les clients potentiels, mais pas les terroristes. Mais aussi, à classer, regrouper ou exclure certains groupes de travail ici même. Et de semblables stratégies déclenchant

l'inclusion d'innocents sur les « *no-fly lists* » (listes d'interdiction de vol en avion dans certaines zones) et sur des listes de surveillance; incluant des maisons ordinaires à l'intérieur des « *hotspots* » de police; dans la ville, classant les piétons pacifiques comme «suspects», quand ils s'aventurent involontairement sous les caméras de lieux publics ou de shopping, ou tout simplement en rentrant du travail. Ce sont les garçons canadiens, d'une grande école comme Alistair Burt, qui se sont vu refuser la permission de monter à bord des avions pour des vacances familiales. N'oublions pas les citoyens «suspects» comme Maher Arar, Ahmad El Maati, Muayyed Nureddin et Abdullah Almalki qui ont atterri dans les salles de torture syriennes en 2002 et 2003. Même sans motif valable et n'ayant rien à cacher, vous pouvez toujours finir suspect.

Voilà pourquoi, malheureusement, nous autorisons les sociétés de surveillance à se développer sans entrave. Leurs effets positifs peuvent bénéficier à certains groupes de personnes, mais leur impact négatif se fait sentir parmi ceux qui, en raison de leur situation économique, leur origine ethnique ou leur sexe, sont déjà défavorisés. D'autre part, comme le prouvent les exemples des buveurs de bière de Montréal ou des vacanciers adolescents, les décideurs montrent que, n'importe qui peut être affecté. Il existe quelques garanties réelles : les lois sur la protection des données et la vie privée. Mais elles ont tendance à être efficaces uniquement dans des cas extrêmes, lorsqu'il ya une évidente ou médiatisée violation de la Loi. La plupart du temps, les risques réels de la nouvelle surveillance affectent négativement les personnes lorsque ces systèmes fonctionnent correctement, aux fins prévues, et dans les limites du droit. Le « Tri social », en particulier lorsqu'il utilise les bases de données consultables et ceux de la communication en réseau, fonctionne par la catégorisation automatique des données de la population afin que les différents groupes puissent être traités différemment. Le simple fait d'appartenir à un groupe statistique vous expose à l'inclusion ou à l'exclusion, l'accès ou le déni. N'avoir rien à cacher n'aide tout simplement pas.