INTRODUCTION

Qu'est-ce que la surveillance ?

Stéphane Leman-Langlois

Depuis le 11 septembre 2001 la sociologie de la surveillance est un espace de construction empirique et théorique intense. Un grand nombre d'ouvrages qui en ont résulté commencent d'ailleurs par cette formule, déjà sans aucun doute la plus usée des sciences sociales. La multiplication des formes de contrôles, la préoccupation pour la sécurité et la prévention, presque toujours poursuivies à l'aide de dispositifs technologiques, ont projeté la surveillance dans la culture populaire et dans les bureaux des chercheurs universitaires. La rapidité avec laquelle les gouvernements du monde ont, sans la moindre hésitation, rongé l'espace des libertés individuelles au profit de notions plus ou moins occultes, plus ou moins fumeuses de sécurité nationale, de prévention et de gestion des risques, de guerre au terrorisme, etc. ont également joué un rôle. Ainsi, la sociologie de la surveillance est souvent en équilibre précaire entre l'observation scientifique de pratiques et de phénomènes sociaux et les considérations éthiques. En fait, on détecte souvent chez les sociologues de la surveillance un scepticisme, voire une aversion pour la surveillance qui vient colorer l'analyse. La raison est principalement que la surveillance est perçue comme la conséquence et le renforcement de différentiels de pouvoir antidémocratiques. Les contributions à cet ouvrage, individuellement et collectivement, manifestent une volonté de départager les modes, techniques et contextes de surveillance d'une manière suffisamment fine pour permettre de mieux faire la part des choses.

Dans la mesure où l'objet surveillance était à l'agenda scientifique et populaire avant le 9/11, c'était surtout à travers une série de scandales

causés par les appareils de renseignement policier et de sécurité nationale. Le Canada a connu les siens avec les dérapages de la Gendarmerie Royale du Canada dans les années 1960 et 1970 ; les États-Unis eurent entre autres l'implosion du programme COINTELPRO (Counter Intelligence Program) du FBI en 1976, sous l'enquête du comité Church (Brodeur et Leman-Langlois, 2006) ; la France eut son « opération satanique » (nom de code de l'opération) de la Direction générale de la sécurité extérieure (DGSE), qui coula le Rainbow Warrior en 1985, tuant un photographe, afin de museler l'opposition de Greenpeace aux essais nucléaires français dans le Pacifique. Pour sa part, la Direction de la surveillance du territoire (DST) avait été prise la main dans le sac lors de l'installation de micros dans la salle de rédaction d'un quotidien en 1973.

Au début des années 1990, des régimes totalitaires autrefois soutenus par Moscou furent renversés ou remplacés et l'ampleur de leur appareil de renseignement clandestin apparut enfin au grand jour. L'affaire des dossiers de la police secrète Est-Allemande, la Stasi, en est l'exemple le plus frappant. En 1990, alors que le régime périclitait, des citoyens prirent d'assaut les bureaux centraux de la Stasi à Berlin-Est, ayant eu vent de la vaste opération de destruction de documents entreprise par les policiers. Les envahisseurs réussirent à sauver de la destruction près de 45 millions de pages de documents amassés pour le compte du ministère de la Sécurité de l'État (MfS, Ministerium für Staatssicherheit ; Koehler, 1999). On y trouva des informations sur la plupart des citoyens est-allemands, dont ceux qui étaient sous surveillance du MfS, et surtout ceux qui collaboraient avec lui. L'étendue de la collaboration rendit nécessaire l'élaboration d'un processus officiel, contrôlé, d'ouverture des dossiers, qui fut supervisé par une commission gouvernementale. On estima qu'entre 500 000 et 2 millions de citoyens est-allemands avaient collaboré avec la Stasi de manière régulière ou occasionnelle (Koehler, 1999 : 8). Cet appareil de surveillance et de répression fut l'objet de plusieurs recherches mais fut surtout considéré comme une caractéristique des États totalitaires.

Tous ces scandales, à l'Ouest et à l'Est, eurent pour effet d'attirer l'attention médiatique, populaire et bien sûr scientifique sur une modalité bien spécifique de la question de la surveillance : celle qui vise à protéger les fondations du statu quo politique. Les années 1960 et 1970, époque de « désubordination » (du mot de Miliband, 1978) où l'autorité

morale des institutions sociales est en chute libre, accueillent les abus de pouvoir des gouvernements comme des preuves additionnelles de l'illégitimité des pouvoirs établis. Ces gouvernements, qui étaient fortement engagés dans de multiples activités de « haute police » (selon la fameuse appellation de Brodeur, 1983), fonctionnaient à partir d'une définition très large du concept de sécurité de l'État, qui incluait sa protection contre toute dissidence. Ainsi, la surveillance des activités politiques apparut comme antidémocratique et c'est cet objet particulier qui entra dans la culture. Les films hollywoodiens de l'époque illustrent bien cette paranoïa anti-étatique (Three Days of the Condor, All the President's Men, The Parallax View, etc.) ; on était très loin de l'approche glorificatrice de la surveillance, des technologies, du secret d'État, etc. qui régna suite au 9/11.

Non pas que les abus étatiques de la surveillance soient sans intérêt, bien sûr, mais dans une certaine mesure le fait que l'objet ait apparu sous cette guise a laissé comme héritage une approche de la surveillance centrée sur la dénonciation de l'État répressif, sur l'image du Big Brother techno-totalitaire d'Orwell, sur une suspicion généralisée de toute surveillance et sur la nécessité absolue de protéger la vie privée dans sa version la plus idéalisée. Ainsi, un recentrage est de mise et devrait nous aider à mieux saisir à la fois les facettes infiniment variées et les caractéristiques généralisables de cette activité que nous nommons surveillance, souvent sans la définir au-delà d'exemples ou d'illustrations.

Surveillance : une définition

Étrangement, la plupart des ouvrages sur la surveillance ont tendance à éviter ou à ignorer, sans doute à cause de son apparente simplicité, le problème de la nature de l'objet et la manière dont on la définit. Dans plusieurs ouvrages, la notion de surveillance se limite à la collecte de renseignements divers (données, images, sons), et surtout par les gouvernements et leurs agences. Ce dernier aspect est d'ailleurs une des failles les plus souvent identifiées de la célèbre analyse de Foucault, fondée sur le panoptique de Bentham (1977). Dans d'autres, elle est si large qu'on a peine à en identifier les caractéristiques, le fil directeur, la « surveillance » censée être décrite (par exemple dans un collectif, par ailleurs excellent, dirigé par Deflem, 2008).

En tout premier lieu, la surveillance est l'acquisition, temporaire, permanente ou à durée variable, **d'information**. Cette information peut être visuelle, auditive, ou autre ; elle est souvent le produit de nos sens ou de technologies visant à les seconder, mais le lien sens-surveillance n'est pas déterminant. Plusieurs formes d'information ne correspondent pas aux sens humains (par exemple, la structure de l'ADN d'un individu). Bref, la relation sens-surveillance est surtout culturelle et a-scientifique. Elle repose d'ailleurs sur une compréhension aristotélicienne de nos sens, limitée aux 5 variétés archi-connues, mais qui n'a plus cours aujourd'hui. Elle oblige également à réfléchir à la surveillance comme une extension de ces sens, ce qui est trop limitatif.

L'information collectée peut porter sur un individu particulier, sur un type d'individu, sur un endroit où des personnes non identifiées au préalable ont été détectées, sur des traces informatisées de transactions diverses sur Internet et dans le monde physique (des traces de consommation, par exemple). Toutes ces informations peuvent être conservées séparément, ou mises en commun pour déceler des patterns ou extrapoler des éléments manquants à partir de ce qui est connu à l'aide d'une boîte à outils de théories sociologiques, psychologiques, démographiques et économiques.

Le dictionnaire permet la « surveillance » d'une plante, d'un chien, d'un volcan ou de la température à l'aide d'un thermomètre, mais il est utile de limiter notre conception de la surveillance à celle qui s'applique à des **objets sociaux**, l'ensemble des éléments qui forment notre réalité subjective. Spontanément, il s'agit bien sûr principalement des personnes et de leurs interactions, qu'elles soient individuellement, spécifiquement surveillées, ou qu'elles se trouvent à entrer dans un champ de surveillance portant sur une population, sur un espace ou sur un flux d'information. Entre autres, la surveillance d'espaces, qu'ils soient publics, privés ou « privés de masse », vise surtout (mais pas uniquement ; on surveille également les objets eux-mêmes, comme un toit qui coule, une poubelle qui déborde ou un serveur qui commence à surchauffer) à détecter et à contrôler les comportements proscrits et à encourager les comportements désirés, peu importe qui s'y adonne (sur ce, voir le chapitre 11, ci-dessous). Lorsque qu'on surveille des machines, des processus automatisés ou des transactions financières, par exemple, c'est généralement parce qu'on peut

supposer que des personnes en sont directement ou indirectement responsables ou dépendantes.

L'objet de la surveillance reste un problème de taille, parce qu'il est à l'occasion difficile ou mal avisé de distinguer les objets physiques, inanimés, des objets sociaux. Au premier abord, il semble utile d'éviter de parler de surveillance lorsque l'objet surveillé est un chien ou un volcan. Cependant, comme Latour (2005) l'a déjà noté, les objets inanimés, ou du moins non-humains, qui font partie de la manière dont nous appréhendons notre contexte social détiennent un pouvoir de modifier nos perceptions, nos attitudes et nos actions et sont donc eux aussi des « acteurs » et non les simples détails d'un décor dans lequel se joue le social. Ainsi, si un géologue surveille l'activité sismique du sud des États-Unis pour sa thèse sur le mouvement des plaques tectoniques, il ne s'agira pas de « surveillance » au sens où elle est entendue dans cet ouvrage. Par contre, s'il le fait pour conseiller des personnes qui se proposent d'acheter un condominium situé sur la faille de San Adreas, ou pour en informer leur compagnie d'assurance habitation, son activité devient sociale et compatible avec notre compréhension de la notion de surveillance.

En ce qui a trait à l'objet de la surveillance, un dernier aspect doit être souligné. Presque toutes les activités de surveillance, qu'elles soient assistées par une technologie ou non, ont la capacité de recueillir des informations sur une foule d'objets variés. Par exemple, si un adepte de la surveillance vidéo dirige une webcaméra vers le stationnement où est garée sa voiture de collection, c'est moins pour observer la voiture que le comportement d'éventuels humains qui pourraient s'en approcher. Évidemment, si la branche d'un arbre à proximité menaçait de s'écraser sur son pare-brise, il serait aussi heureux de pouvoir l'éviter. Dans ce cas, bien que l'objet social ne soit pas l'unique, ou peut-être même la plus importante cible de cette surveillance, sa présence suffit à glisser cette dernière sous le microscope d'une sociologie de la surveillance.

Ajoutons enfin un troisième et dernier élément de définition, auquel la notion d'objet nous renvoie immédiatement : l'objectif, la fin prévue des informations recueillies. La surveillance vise un but extérieur à la simple collection d'information, qui peut être résumé par l'**intervention ou l'obtention d'un bénéfice** extérieur à la connaissance pure. Ceci ne suppose aucunement qu'elle soit couronnée de succès, ni que les individus,

informations, sites, surveillés soient aussi ceux qui seront la cible de l'intervention ou la source du bénéfice subséquents. On peut collecter des informations sur les habitudes d'une population de consommateurs afin de vendre un produit à d'autres.

La question du but d'une action de surveillance est malheureusement moins simple qu'il n'y paraît. Il arrive souvent que le but explicite soit l'expression d'un idéal qui n'est en pratique jamais réalisé. Une caméra de surveillance a peut-être été installée pour permettre d'identifier des criminels. Mais si, après plusieurs mois d'usage, on a plutôt pris des employés à flâner durant leur quart de travail, il y a déplacement important de l'objectif, qui est devenu, en pratique, la gestion du personnel. Plusieurs chapitres de ce livre montrent de tels exemples. Si ce glissement se fait généralement au sein de cette grande catégorie qu'est le contrôle social, il n'en reste pas moins qu'une différence parfois fondamentale existe entre les buts explicitement visés et ceux qu'on peut déduire de l'observation des pratiques de surveillance.

Par conséquent, la totalité des activités de surveillance visant à assurer la sécurité des personnes contre des actes dommageables commis par d'autres peuvent être conçues comme partie intégrante de ce qu'il convient d'appeler le contrôle social. Ce contrôle, s'il est surtout appréhendé à partir de ses actions sur les populations et sur les individus, n'en dépend pas moins, pour exister, d'une phase de surveillance. Ceci est aussi vrai du contrôle social officiel effectué par l'État que de celui, non-officiel, qui est appliqué par les parents, les voisins et les pairs. Cette dyade surveillance-contrôle existe également à travers les variétés de modes de contrôle social, qu'il soit punitif, réformateur, thérapeutique, compensatoire, etc. Ceci provient tout simplement du fait que dans notre culture, l'acte est la responsabilité de l'acteur et non du destin, de la nature ou du clan. Or, pour agir sur le responsable de la faute, il faut d'abord savoir l'identifier, le distinguer, puis l'extraire de la masse.

On le voit, la variété des objectifs, des agents, des cibles, des bénéficiaires, des sites et des techniques de surveillance donne lieu à un nombre probablement infini d'agencements possibles – on en trouvera de nouveaux d'ici à ce que le lecteur ait fini de lire ce paragraphe. Le présent ouvrage réfère à ces agencements sous le vocable de « sphères ». Ses auteurs n'entreprennent pas de faire l'inventaire entier de ces sphères ou de cartographier leur influence, leurs intersections ou leur ampleur, ce

qui serait une tâche impossible. La raison d'être de cet ouvrage est plutôt de tenter d'en dessiner certains des contours en procédant à un échantillonnage aussi large et aussi varié que possible de sphères de surveillance. Ce faisant, on apprendra que la surveillance est loin d'être une activité nouvelle et que plusieurs sphères de surveillance existaient bien avant l'invention de la caméra IP. On apprendra aussi que ces sphères se multiplient, se bousculent, apparaissent et disparaissent dans un cycle de plus en plus rapide. Trois moteurs, ou tendances, expliquent ce bouillonnement.

La multiplication des activités pouvant être surveillées

Grâce à l'informatisation, une portion de plus en plus grande de nos activités quotidiennes sont de facto surveillées, au sens où elles sont, de par leur nature même, automatiquement inscrites dans une ou plusieurs banques de données.

L'informatisation des contenus. Le premier type de contenu traditionnel à apparaître sur support informatisé est l'imprimé. Déjà, à partir de la fin des années 1980, les internautes de l'époque héroïque pouvaient consulter des documents officiels et des textes variés sur des sites institutionnels, dont ceux d'universités. Il fallait tout simplement disposer d'une connexion téléphonique et du savoir-faire technique nécessaire à l'installation et à la configuration des modems, pilotes et logiciels. Dès la fin des années 1990, les grands journaux sont disponibles en ligne (certains tenteront sans succès de vendre des abonnements électroniques, tentative qui semble faire un retour de nos jours). Le second type de contenu est la musique numérisée, qui existait déjà, sous forme de disques compacts, depuis le début des années 1980. Seulement, le format non compressé des disques et la faible capacité mémorielle des ordinateurs ralentissent son informatisation, qui devra attendre l'arrivée de formats compressés, dont le fameux MP3, ainsi que des disques rigides à haute densité (en 1983 un PC « XT » d'IBM était vendu avec un disque de 10Mo et le MacIntosh 128 de 1984 n'avait aucun disque rigide. De nos jours le PC moyen se vend avec un disque de 1To, soit l'équivalent de 100 000 PC XT). Viendra ensuite la vidéo, incluant la programmation télévisuelle et cinématographique.

Ce phénomène à grande échelle a motivé une série de nouvelles lois, stratégies, technologies visant à surveiller la distribution des fichiers informatisés et à redonner le contrôle des contenus à ceux qui en réclament la propriété. À date, toutes ces tentatives de contrôle des contenus ont été mises en échec. Cependant, un nombre d'effets secondaires sont tout de même visibles, entre autres ceux qui affectent la structure même d'Internet et les moyens d'y accéder, qui sont de plus en plus contrôlés (Leman-Langlois, 2005, 2006, 2008a).

La démocratisation des accès. À partir de l'avènement du *World Wide Web*, la toile mondiale issue des laboratoires du CERN en 1994, de nouveaux protocoles de communication informatisée marient l'hypertexte à Internet et permettent l'inclusion de graphiques. L'accès aux contenus est ainsi grandement simplifié et à la portée de ceux qui n'ont aucune compétence particulière. Ceci, en combinaison avec l'arrivée sur le marché de nouveaux logiciels de furetage plus intuitifs et gratuits (à commencer par Lynx et NCSA Mosaic, qui seront suivis de Netscape et d'Internet Explorer). En 1995, Microsoft développe également un système d'exploitation (Windows 95) qui inclue la spécification « plug and play », facilitant – voire automatisant – à l'extrême les connexions matérielles et l'installation des pilotes nécessaires à l'accès à la toile. Windows 95 dispose également d'une interface d'utilisation simplifiée mettant fin à la nécessité du recours à la rébarbative ligne de commande MS-DOS, qui effrayait encore beaucoup des utilisateurs des versions précédentes du système (à l'époque, Apple ne représente qu'une part négligeable du marché). Cette démocratisation des accès fait exploser le nombre d'internautes, la quantité et la variété des activités qu'ils entreprennent en ligne, ainsi que les préoccupations pour la sécurité de ces activités.

Cette préoccupation engendrera entre autres un débat sur la robustesse du chiffrement qui peut être mis à la disposition d'utilisateurs ordinaires. Au départ, le gouvernement étatsunien tente de maintenir cette puissance sous les 40bits, un chiffrement minimal qui permet le décryptage par la force brute des ordinateurs de l'État. Ceci étant jugé insuffisant pour sécuriser les transactions en ligne, en 1993 la National Security Agency (NSA) suggère de permettre aux usagers de chiffrer à une puissance beaucoup plus élevée, mais en créant une « porte arrière » accessible aux autorités. Ce chiffrement serait basé sur un support matériel, une puce du nom de « Clipper », et toute autre forme de cryptographie serait

criminalisée. Le projet est abandonné en 1996, en partie parce qu'un chercheur démontre que la porte arrière du Clipper est mal protégée, mais surtout sous la pression d'organismes de défense de la vie privée. Cependant, il montre bien à quel point les gouvernements insistent, dès les débuts d'Internet, sur sa transparence[1]. À l'été 2010, les téléphones intelligents de la compagnie Research in Motion (RIM), les fameux Blackberry, sont interdits dans plusieurs pays parce que la police est incapable de déchiffrer et d'épier les communications de leurs propriétaires. Ce mini-scandale ne s'applique réellement qu'à une clientèle extrêmement limitée : non pas les utilisateurs de Blackberry en général, mais seulement ceux qui utilisent ses services aux entreprises. Cependant, il souligne que les pays en question sont satisfaits de l'accès qu'ils ont déjà aux conversations tenues sur tous les autres téléphones.

La démocratisation des accès a également un effet pervers important : la structure même d'Internet est disjointe, tendue entre décentralisation et centralisation, parcourue de goulots d'étranglement et soutenue par des logiciels hétéroclites de fiabilité hautement variable (Zittrain, 2008). Cette fragilité, ou « vulnérabilité » si on veut employer le vocabulaire consacré (mais moins neutre puisqu'il implique une menace correspondante), a donné lieu à une série de débats autour de la sécurité du net. Une bonne part de ces débats s'échafaudent sur la notion de « cyberguerre » et évoquent des questions de sécurité nationale. Bien sûr, la notion de cyberguerre implique aussi qu'une sécurisation, une surveillance et un contrôle beaucoup plus rigoureux sont désormais indispensables pour assurer la « cyberpaix ».

Augmentation exponentielle des techniques de surveillance

Si les moyens classiques de surveiller demeurent à notre disposition, des dizaines de milliers de nouveaux produits sont offerts sur le marché spécialisé et aux consommateurs chaque année. L'existence de certains

1. Il faut toutefois noter que ce fétichisme cryptographique est aussi en partie dû à la persistance d'attitudes datant de la guerre froide, alors que la capacité de chiffrer et de décrypter était considérée comme faisant partie du système de défense des nations et confiée à des experts tenus au secret. La démocratisation de la cryptographie, lancée par le PGP (Pretty Good Privacy, avec clé minimale de chiffrement à 128 bits) de Philip Zimmermann en 1991, se frotta donc à un establishment très solide.

de ces produits engendre de nouvelles formes et de nouvelles cibles de surveillance ; par exemple, les conjoints peuvent se doter de logiciels de surveillance afin de découvrir ce à quoi leur être aimé passe son temps lors de sessions prolongées devant son ordinateur.

Développements dans la science de l'identification. Ici plusieurs nouvelles technologies ont soulevé la question de la surveillance dans la culture générale et dans l'agenda de recherche des universitaires. Qu'il soit question d'ADN, de biométrie, de puces radio lisibles à distance, de reconnaissance des personnes par leur visage, par leur démarche, leur voix, leurs empreintes digitales, la géométrie de leur main, de leur squelette, etc., ces technologies ont connu un développement fulgurant dans la dernière décennie, ce qui a fait grandement baisser leur coût. Déjà omniprésentes dans la culture populaire, elles le seront aussi bientôt dans nos activités quotidiennes. Elles sont déjà courantes dans plusieurs contextes, de l'accès aux services gouvernementaux (passeport biométrique à puce, permis de conduire « Plus » au Québec, etc.) aux activités et déplacements liés au travail (carte à puce d'employé, journalisation des activités, surveillance par GPS, etc.) et aux loisirs (reconnaissance du visage dans les casinos, billets d'entrée à radioétiquette, contrôles d'accès biométriques, lecteurs d'empreintes digitales sur les ordinateurs portables, etc.).

Développement des technologies de surveillance. La technologie s'étant sans doute le plus disséminée cette dernière décennie est celle de la vidéosurveillance (Leman-Langlois, 2008, 2003 ; Leman-Langlois et Dupuis, 2007). Les systèmes de vidéosurveillance sont aujourd'hui beaucoup moins chers, infiniment plus performants, et souvent requis par les compagnies d'assurances. Si l'utilisation de caméras par les organisations policières reste sous-développée au Canada, pour des raisons budgétaires et juridiques, ce n'est pas le cas dans la plupart des autres pays. Quoi qu'il en soit, on oublie souvent que la police a un accès facile à d'autres systèmes de caméras existants, dont ceux installés par des entreprises privées ou par d'autres organismes gouvernementaux, à tous les paliers (les caméras de gestion de la circulation, entre autres ; sur ce, voir le chapitre 10 ci-dessous). À ceci, il faut ajouter un nombre grandissant de technologies qui sont moins visibles, mais souvent plus puissantes. Entre autres, la capacité de collecter, de stocker et de diffuser les informations produites par toutes les techniques ci-dessus a fait un bond quantique

spectaculaire, à un point tel que la quantité d'information disponible est en augmentation exponentielle. Ainsi, le problème principal de la surveillance aujourd'hui n'est plus le manque d'information mais bien l'insuffisance des capacités d'analyse : si vous n'avez pas le temps de lire un journal de 20 pages au petit-déjeuner, que feriez-vous d'une montagne de 1 000, de 10 000 puis de 100 000 pages ? Ce nouveau problème a encouragé le développement de plusieurs techniques d'analyse automatisée de l'information, remplaçant l'élément humain (exploration informatisée de données [*datamining*], analyse d'images, de sons).

La multiplication de technologies qui ont des fonctions secondaires de surveillance. Les téléphones portables intelligents, armés de senseurs GPS, ne sont pas des technologies de surveillance en tant que telles mais incluent plusieurs caractéristiques qui permettent à de nouvelles formes de surveillance de voir le jour. Leur usage du système GPS permet non seulement à plusieurs téléphones de donner leur position en temps réel, ce qui est utile aux parents d'adolescents aussi bien qu'aux organisations policières. De plus, lorsque leur caméra intégrée est utilisée, la longitude et latitude exacte de la prise de photo sont insérées dans les métadonnées Exif (Exchangeable image file format) associées au fichier image. Téléchargée sur Facebook, par exemple, cette image donnera donc, à tous ceux qui le désirent (et qui savent accéder aux données Exif, bien sûr, mais c'est un jeu d'enfant), le positionnement exact du photographe à la seconde où fut prise la photo. La voiture moyenne est dotée d'un ordinateur de bord qui emmagasine certaines données de conduite, pour un certain temps. La paire de jeans est équipée d'une étiquette RFID permettant la gestion des stocks, mais qui pourra aussi être lue et reconnue aussi longtemps que le consommateur ne l'aura pas retirée.

Transformation du contexte : la nouvelle (in)sécurité

Les États et les corporations mobilisent immédiatement le discours de l'insécurité pour justifier la mise en place de dispositifs de surveillance/sécurité nuisant à la conduite établie de nos activités quotidiennes. Cette nuisance peut être extrêmement légère, comme l'obligation de retirer nos souliers lors du filtrage de sécurité des aéroports, ou extrêmement onéreuse, comme la sur-multiplication des protocoles de sécurité visant la protection des espaces ou des systèmes informatiques. Ces nuisances sont

généralement accompagnées de sanctions plus ou moins sévères applicables à ceux que la surveillance aura identifiés comme fautifs ou à ceux qui refuseront de s'y prêter : manquer un avion, perdre son droit d'accès à l'Internet, perdre son emploi, être mis à l'amende, être incarcéré, et dans les cas extrêmes, la déportation, la torture et la mort.

Le terrorisme et le 11 septembre. L'ampleur de plusieurs actes terroristes récents, dont ceux du World Trade Center et du Pentagone en 2001, a eu un impact dans la population en général et à tous les paliers de gouvernement. La nécessité de *prévenir* la répétition de tels actes est devenue un leitmotiv de plusieurs discours communs sur le sujet. Or, la manière la plus évidente de tenter cette prévention se trouve au niveau immédiat de la prévention dite « situationnelle ». C'est un type de prévention dont la préoccupation centrale, voire unique, est l'augmentation de l'effort requis pour commettre le crime. Trois grandes catégories de moyens sont suggérés pour y arriver : améliorer la sécurité physique des cibles, intensifier leur surveillance ainsi que celle des malfaiteurs potentiels (Clarke, 1997). Le hic est que le nombre de cibles pratiquement infini qu'offre toute société ouverte diffuse les activités de surveillance dans les moindres racoins des villes, villages et campagnes (dans lesquelles on appréhende des actes d'« agro-terrorisme »). De plus, l'identité cachée de terroristes qui visent la courte carrière de l'attaque suicide, de son côté, diffuse la surveillance à l'ensemble de la population, où chacun devient suspect (bien que s'opère tout de même l'effet discriminant de certains stéréotypes).

En résumé, l'ère sécuritaire post-9/11 a eu quatre effets fondamentaux sur la pratique de la surveillance :

- Les infrastructures essentielles, en particulier celles des transports aériens, sont sujettes à une surveillance intense fondée sur la réponse aux incidents, une « sécurité réactive ». Tout nouvel incident est interprété comme une menace de répétition future et une stratégie, tactique ou technologie est immédiatement appliquée à sa prévention.
- Les organismes de renseignement, dont le foyer principal était le Bloc communiste, se tournent vers la criminalité transnationale à partir des années 1990 et vers le terrorisme après 2001. Dans la plupart des pays occidentaux, la lutte au terrorisme a engendré plusieurs types de nouveaux pouvoirs de surveillance, en matière d'interception des communications, de collecte de renseignement auprès de sources non coopératives (la torture aux États-Unis ou, en plus civilisé, la fin du traditionnel droit au

silence telle que décrétée au Canada en 2001), de collecte de données en vrac dans de plus en plus d'endroits auparavant jugés privés (bibliothèques, entreprises de télécommunications, hôpitaux).
– Comme le terrorisme est d'abord perçu comme une menace transnationale, la surveillance du mouvement des personnes a été sensiblement intensifiée (Scherrer, Guittet et Bigo, 2010). La collecte de données sur les voyageurs, sur les interdits de séjour ou de vol, le resserrement des contrôles de l'immigration sont autant d'exemples.
– Enfin, de nouveaux budgets ont également été consacrés à la mise à niveau et à l'élargissement de l'usage de technologies déjà existantes, comme les caméras de surveillance dans les transports en commun.

Bref, l'étude de la surveillance, ayant pris ses sources dans les abus de pouvoir gouvernementaux à l'Ouest et à l'Est, est désormais en grande partie amalgamée aux questions de sécurité nationale et de sécurité anticrime. En fait, dans toute une zone du champ d'étude le mot sécurité remplace entièrement celui de surveillance, jugé péjoratif ou politiquement miné. Pour le citoyen, le besoin de sécurité absorbe toute la question de la surveillance. Pour le politicien, la notion de surveillance soulève des questions de vie privée mais celle de sécurité est plus difficilement controversée, ce qui permet de tenir un discours exhortatif beaucoup moins risqué. Pour l'entrepreneur, la sécurité est un marché en pleine expansion mais la surveillance est souvent réglementée.

Quoi qu'il en soit, nommée ou non, la surveillance est promise à un brillant avenir, où se combinent une volonté populaire de surveiller et d'être surveillé ainsi que le foisonnement des cibles, des moyens, des agents, des bénéficiaires et des commanditaires de la surveillance. Bref, la situation est pratiquement l'inverse de l'Océania d'Orwell, où la surveillance était centralisée et radicalement coercitive. Cependant, cette transformation ne doit pas être comprise comme une simple *augmentation* de la quantité ou de la qualité de la surveillance. En fait, les nouvelles techniques, stratégies et méthodes sont souvent dysfonctionnelles : mal ciblées, mal conçues, mal gérées, redondantes, défectueuses, facilement contournées, neutralisées ou subverties. … Alors que le traditionnel espionnage entre voisins dans le village d'antan, assorti de commérages et d'une stigmatisation indélébile, était pratiquement totalitaire. La seule augmentation indiscutable et sensible est celle de la variété des cibles et des moyens de surveiller. Toutefois, certaines tendances larges restent à

explorer et à évaluer, dont surtout celle qui fait de la surveillance, sous une forme ou une autre, une solution à un éventail presque infini de problèmes personnels, administratifs et sociaux.

Enfin, si la surveillance contemporaine est largement tributaire de l'apparition et du développement de nouvelles technologies, il ne faut pas oublier que des formes non-technologiques, ou extrêmement « low-tech » de surveillance continuent d'exister en parallèle. Les policiers continuent de surveiller à pied ou en voiture, les voisins continuent de regarder par leur fenêtre, les douaniers continuent d'ouvrir les bagages, les fraudeurs continuent de fouiller dans les déchets pour trouver nos informations personnelles.

Des questions

Le foisonnement des sphères de surveillance soulève plusieurs questions. S'il ne suppose pas une opposition entre surveillance et vie privée – au contraire, on a vu que la vie privée n'est défendue qu'au prix d'une forme ou d'une autre de surveillance –, il implique tout de même une relation entre le domaine de l'individu et celui de la diffusion (ou du moins de l'accessibilité) de l'information, du *privé* et du *public*. Cette relation s'articule au plan de notre volonté de contrôler nos informations et à celui de la confiance que nous avons en ceux avec qui nous la partageons (qu'il s'agisse d'États, de corporations ou d'autres individus). Il faut donc parler non pas de caractéristiques objectives des humains ou des informations, mais bien de la culture, du discours qui domine au sujet de la nature, de la quantité et de la granularité, ou précision de l'information personnelle que nous sommes prêts à partager, avec qui et dans quel but. Or, cette culture fluctue énormément dans le temps et dans l'espace et d'un groupe social à l'autre. Il n'existe pas de « vie privée » qui signifie la même chose pour tous, en tout temps – pas plus qu'il n'existe de niveau précis de transparence qui soit acceptable ou inacceptable pour tous. En fait, comme je l'ai suggéré ailleurs (Leman-Langlois, 2008a), la notion de vie privée est mieux comprise à travers les concepts de propriété et de contrôle de l'information individuelle qu'à travers ceux de secret, de vie intime, etc. À qui ai-je donné mon information, dans quel but, et pour combien de temps ?

Au-delà de notre relation à l'information, une foule d'autres questions découlent de chacun des trois foyers de la définition de la surveillance donnée ci-dessus : le produit, l'objet et l'objectif de la surveillance.

Ainsi, un premier groupe de questions de recherche portent sur la *véracité* et sur la pertinence des informations collectées ou données. La provenance, la nature (audio, vidéo, rapport d'observation, base de données, etc.), la quantité, la compatibilité des informations sont ici des aspects fondamentaux. Pourtant, en général, les montagnes d'information recueillies restent partielles, erronées et dénuées de *signification*. Les employeurs naïfs visitent Facebook pour se faire une idée du caractère de leurs futures recrues, croyant y retrouver des vérités. Les bases de données policières contiennent jusqu'à 40 % d'erreurs. Les caméras de surveillance ne font jamais voir qu'un découpage spatiotemporel artificiel de la réalité. Bref, le fait qu'une technologie ou une technique de surveillance semble objective, voire scientifique, ne garantit pas son exactitude et encore moins sa pertinence. De plus, ces machines ne se construisent pas d'elles-mêmes et comme l'être humain est une machine à interpréter, non à expérimenter (Leman-Langlois, 2007), les concepteurs et programmeurs des machines à surveiller ne peuvent que leur imposer leurs propres conceptions subjectives de la réalité (Brodeur et Leman-Langlois, 2006).

Un second groupe de questions qui s'imposent portent sur l'objet de la collecte d'information et vise l'étude de l'emplacement des *limites* à la collecte de données, aux types d'information qui font varier cette limite, aux facteurs qui la font se déplacer, à ceux qui la différencie chez les individus et les groupes, à ceux qui bénéficient ou qui pâtissent de son déplacement. Dans cette optique, le fonctionnement et les conséquences pratiques des règles officielles portant sur la surveillance, dont les lois, les règlements et les avis d'institutions et d'organismes gouvernementaux est fondamental.

Il faudra également s'intéresser aux *agents* qui sont impliqués dans un réseau de surveillance. Au-delà de la bonne vieille question de Juvénal, qui surveillera les surveillants ?, force est de remarquer que la plupart du temps les surveillants sont eux-mêmes des employés surveillés, souvent davantage que leurs cibles quotidiennes. Quant aux surveillés, la supposition qu'ils sont les cibles inconscientes, involontaires, contraintes ou dédommagées d'une surveillance qui va à l'encontre de leurs intérêts est

visiblement fausse. Si beaucoup de ces cas existent, il y en a d'autres où l'objet de la surveillance est un participant enthousiaste à l'activité – c'est la pierre angulaire des services de réseautage social. Il faut aussi noter la fluidité et le flou qui entourent ces rôles idéaux, puisque tout individu est toujours à la fois ou à tour de rôle surveillé *et* surveillant, selon les caractéristiques de l'endroit, du temps et des autres individus qui l'entourent (physiquement ou virtuellement). D'où l'intérêt d'approcher une sphère de surveillance comme un réseau d'acteurs liés les uns aux autres par des relations complexes de surveillance, de contre-surveillance, d'évitement, de neutralisation et de subversion de la surveillance.

Enfin, l'*objectif* de la surveillance ouvre une série de questions qui lui sont propres. Dans un réseau de surveillance, chaque individu poursuit des objectifs personnels qui doivent s'insérer (tant bien que mal) dans les objectifs de son organisation et/ou de divers groupes sociaux dont il fait partie. En fait, pour une population entière d'acteurs de la surveillance, cette dernière est d'un intérêt entièrement périphérique : ceux qui développent, distribuent, installent et maintiennent les technologies de surveillance sont principalement motivés par le profit ou par les problèmes d'ingénierie qu'elles représentent.

À ceci, il faut ajouter ce que Marx (2007) appelle la *réciprocité* de la surveillance : les surveillés savent-ils ce que les surveillants font ? Partagent-ils les mêmes objectifs ou idéaux (les voyageurs aériens et les agents de vérification des bagages), ou sont-ils en conflit (les agents de surveillance et les bénéficiaires d'aide sociale) ?

Cet ouvrage

Les auteurs rassemblés ici ont mené des recherches terrain dans différentes sphères de surveillance. Dans le premier chapitre, Benoît Dupont montre les dynamiques qui s'installent entre les dispositifs de surveillance et leurs cibles sur Internet. La nature distribuée du réseau de communication, ainsi que la disponibilité de plusieurs moyens technologiques de déjouer ou d'échapper à plusieurs formes de surveillance automatisée est un sujet de toute première importance puisque, comme mentionné, la majorité de nos activités quotidiennes passent désormais par Internet : transactions bancaires, recherche de services de garde pour les enfants, services gouvernementaux, jeux, divertissements, actualités,

etc. En fait, de plus en plus de ces activités ne sont disponibles qu'exclusivement à partir d'Internet. Ce premier chapitre a également l'utilité non négligeable de présenter une des images qui a lancé les études sur la surveillance : le panoptique de Bentham, tel que revu par Foucault.

Le chapitre suivant porte sur un cas plus spécifique de surveillance : l'émergence de bases de données sur les délinquants sexuels ouvertes au public, aux États-Unis. Laurin et Leman-Langlois y décrivent la genèse politique de la « loi de Megan » de 1994, au New-Jersey, qui stipulait que les membres du public ont droit de savoir si des personnes condamnées pour délinquance sexuelle résident dans leur quartier. Au départ, cette information devait être communiquée par lettre à chaque résidence, mais ce système évolua très rapidement et tout naturellement vers une interface web où les citoyens peuvent identifier leurs voisins libérés de prison. Cet outil fut réclamé, offert et développé au nom de la gestion personnelle des risques pour les parents inquiets des dangers planant sur leur progéniture.

Au chapitre suivant, Bigo et Piazza décrivent la tendance lourde à l'échange international de données personnelles, en Europe et de manière globale. La confluence des objectifs d'organismes de sécurité internationaux extrêmement puissants et de technologies capables de manipuler et d'analyser d'énormes quantités de données porte à croire que cette tendance de « gouvernementalité par l'inquiétude » ne peut que s'amplifier à moyen terme. Les conséquences de cette surveillance globalisée restent à identifier pleinement, mais déjà des coûts élevés pour les sociétés et pour les individus sont évidents, comme le contrôle de groupes ethniques et d'immigrants.

Mégie, dans le chapitre 4, nous présente la tendance vers une judiciarisation de la surveillance, dans laquelle le fonctionnement des tribunaux criminels, par leur insistance à présenter le produit de diverses formes de surveillance comme central à la preuve pénale, pousse l'ensemble du système de justice criminelle à donner priorité à la collecte de renseignement. Comme la collecte de renseignement est surtout une activité qui précède les infractions, ceci a pour effet d'étendre le filet de la surveillance à tous les comportements « pré-criminels ». De plus, bien que cette tendance, ait été lancée par les politiques de lutte à la criminalité organisée et au terrorisme, elle semble promise à s'élargir à l'ensemble des infractions.

Le chapitre 5, de Jobard et Linhardt, compare deux sphères de surveillance diamétralement opposées : d'une part, l'environnement social désorganisé, conflictuel et imprévisible d'une banlieue parisienne et, d'autre part, les procédés et tactiques hautement codifiés des dispositifs de sécurité de l'aéroport moderne. Ce contraste permet d'identifier certaines constantes de la surveillance, mais surtout deux grands types : la « surveillance libérale », pragmatique et limitée, et la surveillance « souveraine » qui vise à contrôler activement les habitants d'un territoire où l'État désire affirmer son pouvoir.

Au chapitre 6, Ribaux, Genessay et Margot nous amènent du côté de la pratique de la surveillance à travers les traces matérielles laissées par les activités criminelles. Dans la mesure où leurs auteurs sont engagés dans une carrière criminelle, les crimes laissent des traces qui peuvent faire l'objet d'une analyse scientifique qui permettra d'en dégager des patterns, d'en extrapoler des données manquantes, de dégager des tendances stratégiques, etc. Les auteurs suggèrent une formalisation de ces processus afin d'en tirer certaines conclusions pratiques pour l'amélioration de la lutte aux fraudes, trafics et autres crimes organisés.

Dans le chapitre 7, j'explore l'émergence de trois nouveaux types de sphères de surveillance à l'aide de certaines données colligées en collaboration avec un étudiant affilié à la Chaire de recherche du Canada en surveillance et construction sociale du risque. Il s'agit de la surveillance visuelle de certaines infrastructures municipales, dont nous avons étudié le développement dans la ville de Québec.

Au chapitre 8, Pratte et Leman-Langlois décrivent le fonctionnement de la salle de contrôle de vidéosurveillance d'un important centre commercial de Montréal. On y compare les activités de surveillance aux autres tâches confiées aux agents de surveillance et on y fait l'inventaire des objets et objectifs de cette surveillance, qui ne sont pas ceux auxquels on s'attend en général : entre autres, les locataires d'espaces commerciaux dans le centre sont sous surveillance beaucoup plus intensive que les délinquants potentiels.

La lecture des études hétéroclites qui précèdent peut laisser la tête qui tourne. On y passe d'activités policières et judiciaires à des environnements privés, du réel au virtuel, du contemporain aux Lumières, de la surveillance menaçante à la surveillance protectrice, du collectif à l'individuel, etc. Cependant, certains fils directeurs se dégagent rapidement.

Entre autres, on y voit, dans tous les cas, un processus de négociation de la surveillance entre divers acteurs, dont les surveillants, les surveillés, les bénéficiaires du produit de la surveillance, ceux qui auront à en défrayer les coûts, etc. La présence constante d'une forme ou d'une autre de négociation montre à quel point ces formes variées de surveillance ne sont pas imposées par une autorité centrale et encore moins par un État tout-puissant. On y voit également une variété de formes de résistance, qu'elle provienne du milieu professionnel des agents de surveillance, d'entreprises, de groupes militants ou d'individus isolés. Il est également évident que presque toutes les formes de surveillance sont elles-mêmes sous surveillance. L'agent de sécurité est surveillé par ses patrons, qui eux sont redevables à leurs clients, qui répondent à des exigences de certains secteurs du public et à des règlements officiels.

La fluidité et le dynamisme qui caractérisent tous les échantillons de sphères de surveillance décrits dans cet ouvrage est aussi à noter. Même si c'est évidemment sur Internet, environnement social expérimental par excellence, que ce bouillonnement est le plus marqué, les chapitres qui suivent démontrent que les bulles apparaissent sans cesse autour de nous.