Criminologie

Mots et mondes de surveillance
Contrôle et contre-contrôle à l'ère informatique

Gary T. Marx

Volume 39, Number 1, Spring 2006

Le cybercrime

URI: https://id.erudit.org/iderudit/013125ar
DOI: https://doi.org/10.7202/013125ar

See table of contents

Publisher(s)

Les Presses de l'Université de Montréal

ISSN

0316-0041 (print)
1492-1367 (digital)

Explore this journal

Cite this article

Marx, G. T. (2006). Mots et mondes de surveillance : contrôle et contre-contrôle à l'ère informatique. *Criminologie*, *39*(1), 43–62. https://doi.org/10.7202/013125ar

Article abstract

So far, the study of surveillance as a sociological phenomenon has suffered from a number of shortcomings mostly due to oversimplified categories of objectives, targets, agents and methods, as well as a lack of attention paid to the dynamics of surveillance and counter-surveillance activities. This paper offers suggestions which may be helpful to alleviate both types of problems. It also shows why more empirical observation is required before claims of impending doom, either from insufficient or from excessive surveillance, is to be considered.

Mots et mondes de surveillance

Contrôle et contre-contrôle à l'ère informatique[1]

Gary T. Marx
Professor Emeritus of Sociology
Massachusets Institute of Technology (M.I.T.)
gtmarx@garymarx.net

RÉSUMÉ • On a jusqu'ici peu étudié la surveillance en tant que phénomène sociologique, c'est-à-dire en portant attention aux dynamiques d'action et de réaction dans lesquelles s'engagent ses acteurs. On a également beaucoup trop simplifié les catégories conventionnelles des objectifs, des cibles, des acteurs et des méthodes de surveillance. Ce texte offre un certain nombre de solutions visant à éliminer ces problèmes. L'auteur y montre également à quel point les pronostics alarmistes dénonçant la surveillance excessive, aussi bien que l'insuffisance de surveillance, sont dépourvus des assises empiriques nécessaires.

ABSTRACT • So far, the study of surveillance as a sociological phenomenon has suffered from a number of shortcomings mostly due to oversimplified categories of objectives, targets, agents and methods, as well as a lack of attention paid to the dynamics of surveillance and counter-surveillance activities. This paper offers suggestions which may be helpful to alleviate both types of problems. It also shows why more empirical observation is required before claims of impending doom, either from insufficient or from excessive surveillance, is to be considered.

Introduction

Les problématiques de cybercriminalité et de contrôle contenues dans ce numéro se situent sur le terrain plus large de l'analyse sociologique de la surveillance. Les technologies de la surveillance fragmentent maints

1 Traduit de l'anglais par Stéphane Leman-Langlois.

aspects de nos vies et les reconstruisent sous des formes qui étaient auparavant impossibles, voire inimaginables, comme si la technologie s'employait à suivre l'injonction de Georg Simmel de « séparer ce qui est connecté et de connecter ce qui est séparé ». Ceux qui étudient la surveillance et le contrôle social se doivent de procéder de la même manière, et cette approche est centrale à notre projet de mieux comprendre le fonctionnement de la surveillance en analysant ses variations. Il faut montrer à quel point certaines choses d'apparence similaire sont différentes et combien d'autres, qui semblent différentes, peuvent se ressembler.

L'étude de la surveillance, malgré son dynamisme et sa pertinence à notre époque, a jusqu'ici rarement porté sur les processus sociaux qui sont centraux à son objet. Les études comparant des cas, des époques et des cultures sont encore plus rares. Une grande partie de la littérature actuelle est, dans certains cas, trop concentrée sur les détails empiriques offrant des descriptions minutieuses (et souvent révoltantes) de divers modes de surveillance, mais sans conceptualisation ni cadre théorique qui aideraient à mieux interpréter les phénomènes décrits. Dans d'autres cas, au contraire, la production est trop abstraite sans les fondements empiriques qui permettraient d'en assurer la validité. En général, en mettant l'accent sur les structures plutôt que sur les procédés, les auteurs se privent des outils nécessaires à la compréhension des interactions fluides et dynamiques qui lient les systèmes de surveillance à leurs sujets. Enfin, on a trop souvent limité, voire confondu, le concept de surveillance à celui de domination (sans contredit une de ses formes centrales, mais non la seule).

Dans les observations qui suivent, je propose un nombre d'idées, à michemin entre l'abstraction et l'empirisme, qui aideront à reconnaître certains phénomènes empiriques et qui pourront donner lieu à des hypothèses testables. Je présenterai certaines dynamiques contrôle/contrecontrôle et je conclurai avec des observations plus générales sur le contrôle social et les nouvelles formes de surveillance.

1. Qui, quoi et comment surveiller ?

Bien que de multiples formes de structures sociales puissent définir et modeler les relations de surveillance, la plupart des recherches dont nous disposons se concentrent sur la *surveillance organisationnelle*. Ce type de surveillance implique des surveillants *internes* et *externes* et vise des *indi-*

vidus dans des contextes gouvernementaux ou commerciaux. Sans nier l'importance sociale, théorique et quantitative de ces mondes de surveillance, il faut réaliser qu'ils prennent place dans une catégorie plus large contenant d'autres types de relations surveillant-surveillé. Cet élargissement de la notion de surveillance porte à conséquence aussi bien au chapitre de notre connaissance scientifique qu'à celui de l'élaboration de politiques.

Identifions d'abord un certain nombre de *rôles* que peuvent jouer les acteurs de la surveillance. Ces rôles se divisent en deux catégories principales, celle de l'*acteur* surveillant (observateur, inspecteur, moniteur, garde) qui désire obtenir des informations sur un *sujet* de surveillance (observé, suspect, cible, sujet d'intérêt). En réalité, tous les acteurs jouent des rôles dans les deux catégories, à des degrés différents et changeants selon l'évolution du contexte social. Il faut également ajouter à cela le phénomène de plus en plus commun de l'*autosurveillance*, qu'elle soit le fait de nouvelles technologies (tests d'alcoolémie, de pression circulatoire, d'identité, de comportement) ou simplement au sens classique/moderne de la dissuasion, où l'individu évite lui-même certaines activités, états ou lieux parce qu'il croit courir un risque de détection et de sanction.

Les agents surveillants peuvent être subdivisés en deux groupes : dans le premier, la surveillance est *centrale* à leur rôle, comme, par exemple, les policiers, détectives privés, espions, journalistes d'enquête et superviseurs. Dans le second, la surveillance est une activité *périphérique*, secondaire au rôle principal de l'acteur, comme pour les caissières qui doivent s'assurer que personne ne vole à l'étalage, les dentistes et autres professionnels de la santé qui sont tenus de rapporter aux autorités les cas où ils soupçonnent que des mineurs auraient été violentés. À notre époque, deux tendances déterminantes sont reconnaissables : d'une part, les fonctions de contrôle social sont de plus en plus spécialisées, d'autre part, une multitude de fonctions secondaires de contrôle sont diffusées dans des occupations variées.

De plus, il faut savoir distinguer la surveillance organisationnelle de la surveillance non organisationnelle, ou personnelle, menée par les individus. Comme le *sujet* de la surveillance peut être un individu ou une organisation, nous obtenons donc quatre types analytiques de relation : la surveillance organisationnelle d'individus ou d'autres organisations et la surveillance individuelle d'autres individus ou d'organisations.

Le premier type est celui dont les médias parlent le plus souvent et, sur le plan juridique, celui dont les manifestations concrètes prêtent le

plus à controverse à cause de son incidence sur la vie du citoyen (Rule, 1973 ; Gandy, 1993 ; Smith, 1994 ; Lyon, 2003). Par comparaison, le champ de la surveillance interorganisationnelle semble plus équilibré, tout comme celui de la surveillance interindividus, qui, par ailleurs, est extrêmement commun (tout en étant étrangement négligé par la recherche). Ce dernier type est tout particulièrement stimulé par la large disponibilité d'outils technologiques de plus en plus sophistiqués, visant des usages sécuritaires, stratégiques ou simplement l'amusement. Ici, la surveillance peut impliquer des rôles relationnels, comme lorsque les enfants sont surveillés par leurs parents ou un des époux par l'autre ou quand des amis gardent contact pour se protéger mutuellement. Dans d'autres cas, ces rôles sont absents et la surveillance devient son propre but ; l'exemple le plus évident étant celui de voyeurs, dont les activités n'ont aucun impact sur leur cible (Marx, 2003).

Dans sa forme organisationnelle, la surveillance implique la présence de *membres*. J'appelle *membres* les individus qui sont formellement liés à l'organisation (par des règles explicites ou implicites) ou simplement sous une forme potentielle ou contingente, contextuelle. À l'occasion, les membres sont *internes* à l'organisation, comme les employés qui sont volontairement liés à l'organisation pour laquelle ils travaillent, ou les pensionnaires gardés contre leur gré dans des institutions totalitaires comme celles étudiées par Goffman (1961). Certains membres sont *externes* à l'institution, c'est-à-dire que leur relation à l'institution est occasionnelle ou simplement potentielle et qu'ils sont surveillés même s'ils ne font pas partie intégrante de l'organisation (par exemple, les clients d'une entreprise, les individus suspectés d'un crime, les utilisateurs de sites sur la toile, les spectateurs d'émissions télévisées, etc.). La surveillance de membres externes peut prendre plusieurs formes, dont la surveillance de la *conformité*, lorsque l'organisation tente de vérifier si les individus et autres organisations sous son autorité respectent les règles établies, et la surveillance de *prospection*, par laquelle l'organisation surveille l'apparition de nouveaux sujets à des fins de marketing d'idées, d'interventions, de biens ou de services.

Les organisations surveillent également leur environnement, pris au sens large, pour accumuler des connaissances sur les mouvements sociaux, politiques, démographiques, etc. C'est une surveillance externe de non-membres, qui comprend, par exemple, les renseignements commerciaux et industriels, incluant l'espionnage. Beaucoup de départements de recherche et développement tombent dans cette catégorie.

L'impasse panoptique

Bien que plusieurs interprètes de Michel Foucault aient choisi de réduire le phénomène de la surveillance technologique à une dynamique de domination par les élites, il est relativement facile de voir combien cette approche est simpliste. Mon découpage conceptuel précédemment mentionné ainsi que des observations empiriques récentes (Gilliom, 2001 ; McCahill, 2002 ; Newburn et Hayman, 2002 ; Tunnell, 2004 ; Smith, 1994 ; Nelkin et Tancredi, 1994 ; Norris *et al.,* 1998 ; Norris et Armstrong, 1999 ; Curry, 1997 ; Monmonier, 2002 ; Regan, 1995 ; Bennett et Rabb, 2003) montrent bien que la question est immensément plus complexe.

La thèse plutôt sclérosée de la domination donne beaucoup trop d'homogénéité, de capacités, de compétences et de pouvoir aux soi-disant élites dans nos sociétés démocratiques. De surcroît, ces recherches procèdent d'une ignorance plus ou moins voulue de la variété des impacts, des objectifs (Leman-Langlois [2002] a tenté de montrer comment les technologies de surveillance transforment, non seulement les moyens de regarder, mais aussi les cibles du contrôle social), des rôles, des usages, des contextes de la surveillance, de ses agents et de ses sujets. Cette variété disparate est de plus en plus marquée avec la démocratisation de technologies à la fois de plus en plus puissantes et de plus en plus faciles à utiliser. Enfin, l'application de la thèse de la domination requiert également une sous-estimation des capacités des sujets de résister ou de déjouer la surveillance, combinée à une surestimation de l'efficacité réelle des technologies existantes ou futures.

La surveillance-domination tend à supposer que les différentiels de pouvoir sont stables et durables et que la surveillance et ses technologies servent nécessairement les desseins des puissants sur les dominés, tout en laissant généralement la nature de ces desseins à l'imagination du lecteur. La relation surveillant-surveillé doit plutôt être comprise en fonction de deux facteurs centraux : 1) la surveillance est réciproque ou non réciproque ; 2) il y a consensus ou conflit entre les parties au sujet des objectifs de la surveillance.

J'appelle surveillance *réciproque* ou *symétrique* les cas où les différentiels de pouvoir sont moindres ou inexistants. Elle y est bidirectionnelle ou mutuelle, sans nécessairement être égale, comme dans les jeux joués à tour de rôle et les sports d'équipe, ainsi que dans des contextes beaucoup moins réglementés, comme celui des rivalités industrielles ou étatiques. Les agents de renseignement travaillant pour des États ou des compagnies

rivales sont souvent le miroir les uns des autres, sur l'offensive pour la collecte et la défensive lorsqu'il s'agit de protéger les informations dont ils ont la garde.

La surveillance *non réciproque* est unidirectionnelle : les informations personnelles partent toujours d'un sujet observé vers un observateur. Dans ces contextes, il est approprié de parler de contrôle social, que ce contrôle soit celui que les gardiens de prison exercent sur la population détenue, celui des policiers sur les suspects, des parents sur leurs enfants, des psychiatres sur leurs patients, des maîtres sur leurs esclaves, des gérants sur leurs employés, des agents de services de renseignement sur les passagers, des détaillants sur leurs clients. Dans tous ces cas, l'information coule dans un sens unique et est utilisée pour contrôler, gérer, prendre des décisions face au comportement des sujets et les appliquer. Prenons pour exemple la Recording Industry Association of America (RIAA) qui *patrouille* désormais les réseaux P2P (*peer to peer*) d'échange de fichiers musicaux en ligne afin d'identifier et de punir les pirates qui y sévissent et d'y recueillir des statistiques qui serviront ses pressions auprès des gouvernements afin d'obtenir de nouvelles lois protégeant son commerce (Leman-Langlois, 2005). Ce type de surveillance semble davantage le propre d'organisations bureaucratiques, qui ont d'inscrite, dans leur structure même, l'autorité différentielle qui caractérise la surveillance non réciproque. Pourtant, on retrouve souvent le même type de contrôle à l'extérieur des bureaucraties.

Lorsque la surveillance est utilisée comme une forme de contrôle, il faut différencier les cas où les intérêts des parties divergent de ceux où ils convergent. Pour qui profite d'une forme de surveillance ou d'une autre, il est utile de considérer quatre catégories principales : les élites qui cherchent à établir des politiques dont le but est de servir leurs intérêts ; les agents de surveillance qui doivent appliquer ces politiques ; les sujets surveillés ; la société ou la communauté en général (catégorie la plus difficile à définir et à identifier). Dans n'importe quelle situation, nous devons nous demander si une instance de surveillance est favorable, défavorable ou sans impact pour les objectifs d'un groupe ou d'un autre. Étant donné le foisonnement d'objectifs possibles et la variété infinie de modes de surveillance et de rôles joués par les individus dans ces contextes, donner une réponse utile à cette question peut s'avérer difficile.

En retournant ce kaléidoscope d'intérêts, de groupes et de technologies à usages multiples et imprévisibles, il est facile de comprendre que

la thèse panoptique doit être nuancée. De nouveaux modes de vie électroniques viennent restructurer la relation traditionnelle entre la stratification sociale et la surveillance. Chez Orwell, déjà, la cible de la surveillance n'était pas la masse des prolétaires mais les élites elles-mêmes. La réalité dépassant toujours éventuellement la fiction, plusieurs nouvelles technologies ont déjà la capacité d'inverser la direction traditionnelle de la surveillance, surtout en ce qui a trait à la documentation du comportement. Comme les privilégiés ont davantage accès à des formes de communication informatisée laissant de multiples traces de leurs activités, ils sont désormais plus faciles à surveiller que ceux qui mènent leur vie à l'écart du cyberespace. Comme les pauvres et les sans-abri sont *déconnectés*, ils sont à ce chapitre *moins* vulnérables à ces nouvelles formes de surveillance, et donc au contrôle potentiel qui en découle. La *visibilité* (décrite dans l'étude des bureaucraties de Coser, 1961) est donc une façon erronée de concevoir leur vulnérabilité à la surveillance : les privilégiés sont sans doute moins *visibles*, mais leurs ordinateurs, *BlackBerry*, cartes de fidélité, cartes *speedpass*, téléphones portables, etc., facilitent l'accumulation infinie d'informations sur leur comportement. La production intensive d'archives du comportement pourrait bien mettre fin à la domination des narratifs provenant des individus ou des groupes de statut plus élevé ; les traces informatiques révéleront la corruption de politiciens, les caméras vidéo montreront les abus de policiers. Ericson et Haggerty (1997) ont déjà montré comment la consultation de bases de données par les policiers laisse des traces qui permettent de surveiller leur performance au travail. La surveillance des lieux de travail permet de discipliner les employés, mais aussi de révéler la délinquance des employeurs en matière de sécurité au travail. Par conséquent, lorsque les intérêts des surveillants et des surveillés divergent, il est possible que les surveillés puissent retourner la technologie à leur avantage.

Par ailleurs, même en nous limitant aux contextes organisationnels traditionnels, force est de constater que les objectifs de la surveillance ne sont pas toujours conflictuels. Souvent les surveillants et les surveillés s'entendent sur le besoin de surveillance : les clients des grands magasins désirent eux aussi se trouver dans un environnement sécuritaire, où les prix ne sont pas gonflés par des vols à l'étalage trop fréquents. La surveillance des centres commerciaux par caméra aide également à retrouver des enfants perdus, à discerner des dangers potentiels et à venir en aide à des visiteurs en difficulté. Des programmes d'exploration de données, tels que CAPPSII, violent la vie privée de tous les voyageurs,

mais peuvent également augmenter leur sécurité. L'analyse automatique des habitudes d'utilisation d'une carte de crédit vise à modifier le comportement de son détenteur par un marketing mieux ciblé, mais peut également permettre de détecter les utilisations frauduleuses de cartes volées. Le dépistage des employés sous influence de drogues ou d'alcool aide à assurer que les lieux de travail sont sécuritaires pour tous.

Efficacité et consentement ?

Les deux extrêmes de la technophilie et de la technophobie sont également coupables d'une exagération marquée à la fois des capacités réelles de la technologie de surveillance et de la passivité de ceux qui y sont assujettis. Les romanciers et les sociologues qui se sont penchés sur les excès de la rhétorique technodéterministe et sur le discours enthousiaste des chantres de la surveillance morale et économique, qui prônent une suite sans fin de remèdes technologiques aux remèdes technologiques existants, savent très bien que les choses se déroulent rarement comme on le voudrait. Le conte *Le Magicien d'Oz* nous rappelle à quel point ceux qui se cachent derrière le rideau varient en compétence, en intégrité et dans leurs desseins. Quelquefois, aussi, le système tombe tout simplement en panne.

Toutes les formes de surveillance, de l'enregistrement vidéo au test antidrogue, en passant par l'exploration de données informatiques, sont le produit de contextes sociaux, qu'elles viennent ensuite modifier à leur tour. McCahill (2002) a bien montré combien les relations et positions sociales ont un effet limitatif sur les systèmes panoptiques ; par exemple, les agents de sécurité surveillant un immeuble où ils vivent eux-mêmes peuvent modifier la manière dont ils utilisent les technologies et exercer une profonde influence sur l'intégration de différents systèmes de surveillance. Newburn et Hayman (2002) présentent un certain nombre de stratégies permettant aux policiers de se soustraire au regard de leurs propres caméras. Gilliom (2001) décrit la relation à l'occasion complice entre les agents de contrôle et les bénéficiaires de l'aide sociale.

Ainsi, l'utilisation à son plein potentiel de toute technologie de surveillance dépend du contexte social et des liens unissant les agents de contrôles les uns aux autres et avec les sujets de la surveillance. En inversant le dicton, quand on veut, on *ne* peut *pas nécessairement*, la surveillance désirée et organisée par les élites n'est ni immédiate ni automatique et dépend de qui sont leurs agents sur le terrain et d'où ils se trouvent. Ceux qui surveillent ont leur propre compréhension et interprétation

des objectifs organisationnels qu'ils doivent réaliser. Ils ont également leurs objectifs et désirs personnels, et ils peuvent utiliser les puissantes technologies mises à leur disposition pour les poursuivre.

Plusieurs recherches sur la police (Manning, 1992 ; Chan, 2003 ; Ericson et Haggerty, 1997 ; Meehan, 1998) ont documenté la fréquente rupture qui apparaît entre l'usage potentiel d'un outil et son usage réel. Toute machine doit être mise en marche ; elle doit fonctionner correctement ; son utilisation doit être à la portée de celui à qui on la confie ; l'information qui s'y trouve doit être valable ; les caméras doivent pointer dans la bonne direction ; la continuité de la garde des pièces à conviction doit être assurée si on veut pouvoir utiliser des preuves d'analyse biométrique. Bref, ceux qui utilisent les technologies de surveillance doivent avoir la compétence, le désir et la motivation nécessaires. Dans le cas de la police, la tendance organisationnelle à la protection de l'information est particulièrement forte et la prédisposition au partage très faible. Même lorsque des informations valides sont disponibles, les ressources pour les analyser et les mettre à profit sont insuffisantes (Chan, 2003).

Mise à part la complexité extrême de tous les systèmes interdépendants de surveillance, les objectifs multiples et contradictoires qu'on leur donne et les difficultés de prévoir le futur dans un contexte technologique évoluant rapidement, force est de constater que les caractéristiques qui font la puissance des technologies de surveillance, comme la vitesse et l'automatisation, seront toujours réduites, sinon mises en échec par ceux qui doivent les appliquer et qui sont affligés par les défauts de leur humanité (leurs intérêts personnels, empathie, réseaux individuels, préjugés, incompétence, égoïsme, etc.). Ces systèmes seront également déjoués par les actions de leurs cibles qui cherchent à éviter la surveillance.

2. Contrôle et contre-contrôle : les réactions à la surveillance

Il est vraiment douteux que l'ingéniosité humaine puisse créer une énigme de ce genre dont l'ingéniosité humaine ne vienne à bout par une application suffisante.

Edgar Allan Poe, *Le scarabée d'or*

Quelle que soit notre position éthique sur la question, il est utile d'approcher les comportements et structures liés à la surveillance comme dynamiques. Une grande partie de notre fascination pour l'étude des

règles, de leur application et de leur transgression vient précisément de cette interaction dynamique entre les agents de contrôle et leurs sujets, lorsque des groupes et des individus en interaction réagissent les uns aux actions des autres et ajustent leurs tactiques à l'environnement fluide du contrôle social.

Variété des formes d'acceptation et de résistance

Tôt ou tard, il faudra bien se pencher sur l'infinie variété des réponses ouvertes et cachées à la surveillance, qu'il s'agisse de faire face à une forme particulière ou à un réseau de différentes technologies. Ces réponses incluent un refus de participer, des tentatives de sabotage ou les deux ; elles peuvent provenir d'individus ou de groupes plus ou moins organisés préexistants ou formés pour la cause.

En poussant quelque peu la distinction établie par Merton (1959) entre le conformisme d'attitude ou de comportement, on peut distinguer quatre grands groupes de cibles selon leur relation à un mode de surveillance : a) les *conformistes*, qui sont pleinement d'accord avec le fait d'être surveillés ; b) les *opportunistes*, qui sont en désaccord, mais s'y soumettent tout de même ; c) les *rebelles*, qui la rejettent tout simplement ; d) les *manipulateurs*, qui s'y soumettent en apparence tout en cherchant des moyens de la déjouer. Un bon exemple de rebelles serait celui des communautés défiant ouvertement les efforts de la RIAA pour contrôler les réseaux P2P (en particulier, *ZeroPaid*, à www.zeropaid.com et *P2PNet* à p2pnet.net).

Quand une masse critique de citoyens s'opposent carrément à une technologie de surveillance, pour une raison ou pour une autre, il est possible qu'elle soit tout simplement abandonnée, ce fut le cas récemment du projet *Total Information Awareness* aux États-Unis (Brodeur et Leman-Langlois, sous presse). Cela soulève donc un certain nombre de questions sociopolitiques intéressantes : 1) À quel point et sous quelles conditions une opposition à une surveillance devient-elle *politique* ? 2) Qu'est-ce qui fait qu'une opposition non organisationnelle à la surveillance ait du succès, qu'elle atteigne ses objectifs matériels ou en ce qui a trait à la dignité et au sens d'autonomie et de liberté de ses participants ? 3) À quel point les actions résistantes d'individus, en s'accumulant, produisent-elles un effet social ? 4) Ces actions sont-elles originales ou proviennent-elles d'un effet d'entraînement, d'imitation d'autres individus ? 5) Reflètent-elles un courant social plus large ? 6) À quel point deviennent-elles un facteur pouvant conscientiser ou politiser les indi-

vidus et les pousser vers l'action politique organisée au lieu de rester purement individuelles ? 7) Les tentatives clandestines de subvertir les buts de la surveillance deviennent-elles éventuellement des facteurs de changement social ou, au contraire, servent-elles à stabiliser le statu quo en renforçant les apparences de légitimité de la structure surveillante (cette dernière question est particulièrement difficile à élucider, voir Ewick et Silbey, 1998 ; Handler, 1992 ; McCann et March, 1995 ; Scott, 1985) ?

Bien que ces questions de contrôle et de pouvoir déterminent lesquelles des formes de surveillance deviendront des problèmes sociaux, le pouvoir n'est pas un jeu à somme nulle. Au-delà des variations dans les contraintes normatives formelles et éthiques qui encadrent les puissants, le pouvoir est souvent limité parce qu'il est le produit de valeurs conflictuelles et d'interdépendances entre les membres d'une société, et parce qu'il se déploie dans un contexte large et décentralisé d'économie de marché. S'il est impossible de tirer le plein potentiel des technologies de surveillance, c'est en partie à cause des difficultés logistiques et économiques provenant de la technologie elle-même (on ne peut pas multiplier les caméras à l'infini). Enfin, même dans la mesure où on pourrait optimiser les technologies, il n'en reste pas moins que les situations humaines qui doivent être surveillées sont beaucoup moins claires et déterminées que les technologies qu'on veut utiliser pour les voir, elles sont subjectives et demandent interprétation. Sans compter que les actions des surveillants sont également sujettes à interprétation et à récupération par les surveillés.

Les stratégies de neutralisation de la surveillance illustrent bien la nature changeante de l'infraction et de l'application de la loi dans une société où les ressources matérielles et culturelles pouvant servir aux deux sont intarissables (Marx, 2003). Malgré les scénarios apocalyptiques de perte de vie privée, de liberté et d'identité dans les démocraties libérales, les avantages produits par la technologie sont souvent de courte durée et accablés de vulnérabilités ironiques. Les multiples facteurs de vulnérabilité mentionnés précédemment devraient rétablir un certain scepticisme et contrer à la fois le réflexe de paranoïa irréfléchie contre la technologie et le marketing sauvage de solutions douteuses visant des contextes sociaux mal compris.

Évidemment, malgré les facteurs qui rendent la surveillance difficile ou qui la déjouent d'une manière ou d'une autre, en tout et pour tout subsiste une asymétrie dans les systèmes de surveillance formels et dans

les accès à l'information dans les organisations hiérarchisées et autres contextes socialement stratifiés. Cette asymétrie, bien que jamais absolue, n'est pas toujours facile à identifier ou à mesurer parce qu'elle est souvent parfaitement intégrée dans l'environnement physique et culturel. Souvent, seules des expériences en subversion et bris de règles sociales peuvent les révéler, comme la *sousveillance*, concept inventé par l'informaticien Steve Mann (Mann *et al.,* 2003). Avec la *sousveillance* (le port d'ordinateurs et de caméras intégrés aux vêtements), Mann permet de reconnaître les règles implicites qui structurent les comportements d'observation et révèle les réactions des gens face aux modifications des modes de surveillance et d'observation auxquels ils sont confrontés.

Mais la jungle l'est aussi !

D'un point de vue strictement scientifique, s'il faut reconnaître la complexité des relations de surveillance et accepter l'existence de fonctions prosociales, voire antiélites aux technologies, il ne faut pas non plus trop amoindrir l'importance des formes plus draconiennes de la surveillance appliquée au contrôle social. En fait, ces formes continuent d'être au centre des développements structuraux et sont clairement prédominantes dans la sphère sociopolitique. Une technologie d'apparence inoffensive et potentiellement utile au travail, à la maison, au centre commercial, dans des institutions ou sur la voie publique a des conséquences différentes lorsqu'on la plonge dans des champs sociaux stratifiés où les objectifs individuels et organisationnels sont en conflit. Ces technologies deviennent des instruments de contrôle d'activités jusque-là disparates, peu visibles et géographiquement dispersées en centralisant leur collecte, analyse et utilisation.

L'ironie, souvent soulignée, des agents de contrôle emprisonnés dans les filets de leur propre organisation totalitaire, et s'y enfonçant toujours plus avec leurs activités de surveillance, est maintenant exagérée par la puissance de la technologie d'identifier, de traquer et de documenter *tout* ce qu'elle détecte. Le gardien de prison travaillant sous les caméras qu'il utilise pour surveiller ses pensionnaires devient lui-même le sujet de surveillance par la bureaucratie de l'établissement. Et son syndicat l'en protège peu, puisque le discours voulant que la caméra protège le gardien est parfaitement accepté.

L'impression généralisée liée à l'incertitude du contrôle — sommes-nous surveillés à cet instant ; la technologie représente-t-elle la réalité dans son ensemble ; ce que les surveillés vivent correspond-il à ce que les

surveillants perçoivent avec leur technologie ? — s'applique aussi bien aux gardiens qu'à leurs sujets. Dans les contextes à haute *visibilité* d'environnements informatisés, même les responsables de la surveillance ne peuvent jamais être certains d'être eux-mêmes sous surveillance ou non, que ce soit par caméra, par leurs traces informatiques ou à l'aide de tests divers, par exemple, pour évaluer leur réponse à des situations d'urgence. Les gestionnaires et la direction de leur organisation peuvent abuser grossièrement de ces informations à tout moment : immédiatement, ou plusieurs années après les faits, dans des contextes entièrement différents.

« La technologie n'est-elle pas neutre ? », demanda-t-on un jour à Orwell. Ce à quoi il aurait répondu : « Oui, mais la jungle l'est aussi ! ». Comme pour l'égalité des individus de *La ferme des animaux*, la neutralité est plus neutre pour certains que pour d'autres. Par exemple, dans la prison décrite par Newburn et Hayman (2002), malgré la nature omnivore, neutre, égalitaire de l'observation vidéo, on ne trouve pas de caméra de surveillance dans le bureau du directeur, dans la salle de repos des gardiens ou dans les toilettes qui leur sont réservées. Les cellules ne sont pas équipées de moniteur permettant aux détenus de surveiller les gardiens. On interdit également aux détenus de posséder des téléphones portables équipés de caméra. Un autre exemple de contraste des facultés de surveiller est celui des organisations dédiées à la sécurité nationale tels la National Security Agency (NSA) des États-Unis, la Direction de la surveillance du territoire (DST) française, le Security Service (MI5) du Royaume-Uni ou le Centre de la sécurité des télécommunications (CST) au Canada, qui travaillent à la fois à la transparence du monde social et à l'opacité de leurs activités.

Il est primordial de bien comprendre le sens particulier dans lequel la technologie peut être qualifiée de *neutre*, même lorsque qu'il subsiste un différentiel dans les probabilités d'en devenir la cible. En fait, il faut en différencier les usages potentiels des usages réels, sans quoi affirmer que la technologie est neutre équivaut souvent au mot d'Anatole France sur le droit égal des riches et des pauvres de dormir sous les ponts. Ainsi, les caméras, les micros, les détecteurs de mouvements, les enregistreurs de frappes et les bases de données sur l'usage d'Internet ne discriminent effectivement pas selon les groupes ethniques, les groupes d'âge, les sexes ou la classe sociale. Ils capturent tout ce qui peut être capturé. Il y a donc là, en effet, une certaine forme d'équité et d'impartialité, qui peut aider à mitiger les effets de la stratification sociale. Cependant, ce

potentiel *démocratique* de la technologie ne signifie en rien que tout individu est à possibilités égales d'être surveillé ou d'en surveiller d'autres, ou que l'accès de chaque citoyen à la technologie est comparable. Il ne faut pas non plus supposer que les ressources culturelles ou physiques pouvant permettre de déjouer la surveillance se retrouvent saupoudrées également ou aléatoirement à travers les strates sociales.

Si on considère le degré auquel une action est visible de l'extérieur, autrement dit, si les informations sur nos activités sont compartimentées ou agrégées, la question de la surveillance se déplace au niveau de la gestion des informations recueillies. En mai 2000, le ministère fédéral canadien du Développement des ressources humaines démantelait, à la suite d'un tollé de protestations, son *Fichier longitudinal sur la main-d'œuvre*. Celui-ci contenait 2 000 dossiers d'information sur 34 millions de Canadiens vivants ou décédés (c'est-à-dire qu'aucune information n'était jamais retirée de la banque, même à la mort du sujet [Commissaire à la protection de la vie privée du Canada, 2000]). Cet aspect est au centre de beaucoup de controverses actuelles au sujet de la formation et de l'association de bases de données privées et gouvernementales et la facilité avec laquelle on peut aujourd'hui former des métabases en utilisant des moteurs de recherche universels et des codes d'identification individuels homogènes (par l'identité réelle ou par des moyens anonymes ou *dénominalisés*).

Il faut également considérer la question de l'échelle et de la quantité des activités quotidiennes qui peuvent être sujettes à surveillance, leur concentration ou dispersion géographique. Ici, l'étude de McCahill (2002), comparant deux centres commerciaux, est lumineuse. Dans le premier, au centre d'un voisinage formé d'appartements à prix modique, étaient concentrés une foule d'endroits où prennent place des activités quotidiennes comme une épicerie, des bureaux gouvernementaux, une clinique, etc. Puisque les membres de la communauté y passaient de longues périodes en vaquant à leurs occupations ordinaires, faisant des appels téléphoniques, se prélassant sur des bancs, etc., leur présence devant les caméras de surveillance était, par conséquent, maximisée. Par contraste, les usagers du second centre commercial, situé dans une banlieue affluente, répartissaient beaucoup plus facilement leurs activités entre plusieurs sites, évitant ainsi la collecte en un seul endroit d'informations au sujet de leurs activités. Entre autres, la facilité de se déplacer en véhicule individuel, la disponibilité d'espaces personnels où se divertir et de téléphones à la maison et la capacité de s'offrir plusieurs biens

et services à domicile faisaient que leur présence devant les caméras du centre commercial était minimisée.

Une rhétorique de plus en plus commune conçoit la démocratisation des technologies comme une occasion de faire du citoyen ordinaire un agent de contrôle puissant, capable de surveiller les agents du contrôle social institutionnel (Brin, 1999). Ce point de vue ignore l'effet multiplicateur des institutions bureaucratiques sur le pouvoir des technologies de surveillance, qui donne un avantage insurmontable aux organisations. Sans compter que ces dernières, contrairement aux sujets qui leur sont subordonnés, ont le pouvoir de défendre l'emploi de ces technologies (par exemple, les restrictions de plus en plus communes sur l'utilisation de téléphones portables équipés de caméra).

Il faut également conserver à l'esprit que certains types de technologie sont favorisés, ce qui accélère leur développement et leur déploiement. Considérons un exemple fictif. Qu'arriverait-il si les pays en développement, les colonisés, les ouvriers, les défavorisés, les groupes ethniques minoritaires, les handicapés physiques et mentaux et les détenus avaient des ressources scientifiques et technologiques équivalentes à celles des pays occidentaux, des corporations transnationales, des forces militaires, des polices et autres institutions de contrôle ? Les technologies produites seraient-elles différentes de celles que nous connaissons aujourd'hui ? À quoi l'histoire de la fin du XX^e^ siècle ressemblerait-elle si les technologies d'aujourd'hui avaient été disponibles à l'époque réformiste et idéaliste des années 1960 ?

L'exemple, bien réel celui-là, de l'exploration automatisée de données (*data mining*) pour dépister les comportements criminels ou terroristes peut aussi illustrer cette question de neutralité. Les logiciels d'exploration de données, bien qu'objectivement incapables de discrimination, doivent tout de même être *conçus et programmés* par des personnes qui font des choix sur les types de comportement constituant des menaces et de combien de tels éléments on doit disposer pour supposer la culpabilité d'un individu (Brodeur et Leman-Langlois, sous presse). Ces choix reflètent bien sûr un certain nombre d'observations empiriques, mais également les valeurs des individus et de leurs institutions au sujet de ce qui doit et peut être mesuré. L'aspect mécanique, scientifique de la technologie escamote facilement ces choix culturellement localisés puisque c'est le processus de production, plutôt que le contenu, qui donne une apparence de vérité objective. Une série de techno-sophismes en découlent, incluant celui de la neutralité, celui des « faits qui parlent

d'eux-mêmes », celui du « système à protection totale » (*fail-safe*) et celui du « coup imparable » (Marx, 2003).

Conclusion

Lorsqu'on considère l'observation au sens large, au-delà de la vision oculaire, beaucoup des phénomènes sous-tendant la thèse panoptique sont en augmentation (Marx, 2005). Combinés aux changements législatifs et culturels qui ont suivi les événements du 11 septembre 2001, les moyens de collecte, d'archivage, d'analyse et de communication des données sont de plus en plus sophistiqués, rapides, étendus, intégrés (à la fois quant aux types de données et aux banques de données), puissants, accessibles à distance, faciles à mettre en application et à des coûts de plus en plus modiques.

Côté informatique, jusqu'au début du XXIe siècle le nombre de transistors par microprocesseur, suivant la fameuse loi de Moore, a doublé à tous les 18 mois, la quantité de mémoire des ordinateurs doublant tous les ans (National Academy of Sciences, sous presse). Il est désormais moins coûteux de conserver l'information que de nettoyer les mémoires, ainsi la quantité de données conservées est en augmentation exponentielle. Cela produit l'impression d'en savoir toujours plus, à la fois sur le passé et sur l'avenir, comme l'exploration de données et l'analyse statistique sont de plus en plus décisives dans l'adoption de politiques gouvernementales et de stratégies industrielles. Il est à noter que de plus en plus de ces nouvelles techniques de surveillance sont perfectionnées, adoptées ou distribuées par les forces militaires (utilisation de robots, reconnaissance du visage, exploration de données, système de positionnement GPS, analyse à distance). En octobre 2004, la Food and Drug Administration des États-Unis, qui autorise la mise sur le marché des médicaments et des dispositifs de type médical, approuvait l'utilisation de puces sous-cutanées permettant l'identification à distance des humains, technologie jusqu'alors réservée au bétail. Tout comme les frontières nationales, les frontières internes ont également été renforcées ; on le voit dans la prolifération de communautés à accès restreint, dans la problématisation de l'entrée dans les édifices publics et privés et dans l'omniprésence de la caméra à circuit fermé.

La surveillance continue d'augmenter à la fois dans son intensité et dans son étendue. L'*observation* est de plus en plus généralisée et catégorielle, actuarielle, tout en permettant l'isolement des individus et leur

description minutieuse. Sa puissance nette permet à la fois l'agrégation massive et le détail microscopique. Ces deux facettes sont vouées à l'amplification sans limite puisqu'elles suivent le progrès constant et la pénétration de l'informatique dans nos activités quotidiennes. Les puces d'identification et de localisation seront présentes dans un nombre croissant d'appareils électroniques, mais également dans une masse d'autres produits de consommation, à partir des emballages de lames de rasoirs aux sous-vêtements, en passant par les livres et les disques. Les dispositifs permettant leur détection seront installés dans les murs, trottoirs, routes, portes, etc. En intégrant toutes ces informations, on produira une valeur ajoutée massive permettant la mise sur pied de nouveaux modèles d'analyse et de prédiction du comportement.

Cependant, les tendances opposées deviennent elles aussi de plus en plus puissantes ; par exemple, on publie de plus en plus rapidement sur Internet les caractéristiques de systèmes de surveillance, afin d'en révéler les failles. Aucun observateur de la société ne se surprendra de constater que toutes ces épées ont deux tranchants, que tout outil possède des usages multiples, que tout ordinateur mis sous surveillance peut être utilisé pour crypter des données. Dans un environnement où se multiplient les objectifs plus ou moins conflictuels et où des humains, avec toutes leurs failles, doivent tenter de tirer leur épingle du jeu, il ne peut qu'y avoir un différentiel entre les buts visés et les résultats réels. Sur les eaux vives du conflit, ceux qui surveillent peuvent souvent avoir l'impression d'être toujours en glissement, sans jamais arriver au point visé sur l'autre rive. Les ironies inhérentes et les talons d'Achille du contrôle par la surveillance ne réduisent pas à l'effort (souvent on ne réussit qu'à les exacerber). Comme je l'ai noté plus haut, il faut également tenir compte des préoccupations du public, du désir de transparence, d'imputabilité, de nouvelles garanties juridiques et de l'usage de technologies antisurveillance.

Foucault (1975) a bien montré comment l'accent sur l'aspect spectaculaire de la sanction pénale a disparu, le détenu moderne étant désormais puni hors de la vue du public. Et pourtant, l'apparition et le déploiement des médias d'information et, avec eux, le concept de *droit à l'information* semble au contraire faire retourner certains aspects du système de justice au statut de spectacle (ou de cirque, dans certains cas). Les bulletins de nouvelles, par exemple, font grand usage d'enregistrements vidéo montrant le déroulement de crimes variés ou la poursuite effrénée de suspects sur l'autoroute, visibles en direct de l'*hélicoptère des nouvelles*.

Dans ce dernier cas, le même mécanisme est employé pour surveiller et pour communiquer, comme c'est le cas des conférences vidéo où les employés informent et sont évalués tout à la fois. La faim insatiable des médias pour les images de la déviance et de la criminalité vient à son tour modifier la perception qu'ont les consommateurs des nouvelles de la criminalité, de son contrôle et de ceux qui sont responsables de l'un ou de l'autre, convainquant le citoyen de la nécessité de surveiller davantage, ce qui produit à son tour plus d'images médiatiques. Il y a là un cercle sans fin où l'appétit pour les images de surveillance s'autogénère (Mathiesen, 1997 ; Altheide, 2002). La présence des produits de la surveillance dans les médias de masse sert également à normaliser le comportement, à l'aide de moralités sans cesse jouées par des acteurs involontaires capturés par les lentilles panoptiques.

Cela dit, cette intégration de la surveillance et de la communication pourrait bien contrer certains des excès possibles de la surveillance. Au lieu des élites *benthamiennes* observant les masses, ce sont les masses de téléspectateurs qui pourraient voir des détenteurs d'autorité humiliés devant les caméras. La même logique de surveillance produirait l'imputabilité des élites. Sur Internet, où les usagers peuvent faire l'objet de formes particulièrement intenses de surveillance, chacun est également un éditeur en puissance capable de publier ce qu'il veut dans une presque totale liberté, à peu de frais (en supposant que l'information nécessaire puisse être glanée quelque part).

Bref, le pessimisme et l'optimisme sont prématurés puisque nous ne possédons toujours pas les connaissances empiriques comparatives nécessaires à une évaluation satisfaisante des variations de la surveillance et du contrôle. L'observation rigoureuse des phénomènes dont j'ai fait ici une classification préliminaire est aussi indispensable à une distinction entre les énoncés factuels, la rhétorique pro ou antitechnologie et les professions de foi.

Pourtant, à force de prêcher l'humilité scientifique et d'exhorter à une meilleure prise en compte des complexités des phénomènes en question, il y a danger de devenir des eunuques intellectuels ou des laquais du statu quo. On dit un jour de l'Irlande qu'il s'y trouvait trop de catholiques, trop de protestants et pas assez de chrétiens. Au pays de la surveillance, on trouve encore trop d'idéologues, trop de commentateurs et pas assez de chercheurs.

Références

Altheide, D. (2002). *Creating Fear : News and the Construction of Crisis*. New York : Aldine de Gruyter.

Bennett, C. & Raab, C. (2003). *The Governance of Privacy*. Brookfield, VT : Ashgate.

Brin, D. (1999). *The Transparent Society*. Reading, Massachusetts : Perseus Books.

Brodeur, J.-P. & Leman-Langlois, S. (sous presse). Surveillance-Fiction : High and Low Policing Revisited. In R. V. Ericson & K. Haggerty, The New Politics of Surveillance and Visibility. Toronto : Toronto University Press.

Chan, J. (2003). Police and New Technologies. In T. Newburn (ed.), *Handbook of Policing* (655-679). Cullompton, Devon : Willan Publishing.

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

Coser, R. L. (1961). Insulation from Observability and Types of Social Conformity. *American Sociological Review*, *26*, 28-39.

Curry, M. (1997). *Digital Places : Living With Geographic Information Systems*. London : Routledge.

Ericson, R. & Haggerty, K. (1997). *Policing the Risk Society*. Toronto : University of Toronto Press.

Ewick P., & Silbey, S. (1998). *The Commonplace Law : Stories from Everyday Life*. Chicago : University of Chicago Press.

Foucault, M. (1975). *Surveiller et punir*. Paris : Gallimard.

Gandy, O. (1993). *The Panoptic Sort*. Boulder : Westview.

Gilliom, J. (2001). *Overseers of the Poor*. Chicago : University of Chicago Press.

Goffman, E. (1961). *Asylums : Essays on the Social Situation of Mental Patients and Other Inmates*. Chicago : Aldine.

Handler, J. (1992). Postmodernism, Protest, and the New Social Movements. *Law and Society Review, 26*, 697-732.

Leman-Langlois, S. (2005). Theft in the Information Age : Music, Technology, Crime and Claims-Making. *Knowledge, Technology and Policy*, *17* (3-4), 140-163.

Leman-Langlois, S. (2002). The Myopic Panopticon : The Social Consequences of Policing Through the Lens. *Policing and Society, 13*, 43-58.

Lyon, D. (2003). *Surveillance after September 11th*. Cambridge : Polity Press.

Mann, S., Nolan, J. & Wellman, B. (2003). Sousveillance : Inventing and Using Wearable Computing Devices for Data Collection in Surveillance Environments. *Surveillance and Society, 1*, 331-355.

Manning, P. K. (1992). Information Technologies and the Police. In M. Tonry & N. Morris. *Modern Policing : Crime and Justice, A Review of Research*, *15*, 349-98.

Marx, G. (1981). Ironies of Social Control : Authorities as Contributors to Deviance through Escalation, No Enforcement and Covert Facilitation. *Social Problems*, *28* (3), 221-246. (Pas cité dans le texte.)

Marx, G. (2003). Some Information Age Techno-Fallacies. *Journal of Contingencies and Crisis Management, 11* (1), 25-31.

Marx, G. (2005). Seeing Hazily (But Not Darkly) Through the Lens : Some Recent Empirical Studies of Surveillance Technologies. *Law and Social Inquiry, 30* (2), 339-399.

McCahill, M. (2002). *The Surveillance Web*. Devon : Wilan Publishing.

McCahill, M. (sous presse). *Windows into the Soul : Surveillance and Society in an Age of High Technology*. Chicago : University of Chicago Press. (Pas cité dans le texte.)

Mathiesen, T. (1997). The Viewer Society : Michel Foucault's 'Panopticon' Revisited. *Theoretical Criminology*, *1*, 215-234.

McCann, M. & March, T. (1995). Law and Everyday Forms of Resistance. *Studies in Law, Politics, and Society, 15,* 207-236.

Meehan, A. J. (1998). The Impact of Mobile Data Terminal (MDT) Information Technology on Police Subculture through the Introduction of Information Technology. *Qualitative Sociology*, *21*, 225-254.

Merton, R. (1959). Control, Departion and Opportunity Structures. *American Sociological Review*, *24*, 177-188.

Monmonier, M. (2002). *Spying With Maps*. Chicago : University of Chicago Press.

National Academy of Sciences (sous presse). *Privacy in the Information Age*.

Norris, C. & Armstrong, G. (1999). *The Maximum Surveillance Society*. Oxford : Berg.

Norris, C., Moran, J. & Armstrong, G. (1998). *Surveillance, Closed Circuit Television and Social Control*. Aldershot : Ashgate.

Nelkin, D. & Tancredi, L. (1994). *The Social Power of Biological Information*. Chicago : University of Chicago Press.

Newburn, T. & Hayman, S. (2002). *Policing, Surveillance and Social Control*. Devon : Willan Publishing.

Regan, P. (1995). *Legislating Privacy : Technology, Social Values, and Public Policy*. Chapel Hill : University of North Carolina Press.

Rule, J. (1973). *Private Lives and Public Surveillance*. London : Allen Lane.

Scott, J. (1985). *Weapons of the Weak : Everyday Forms of Peasant Resistance*. New Haven : Yale University Press.

Smith, J. (1994). *Managing Privacy*. Chapel Hill : University of North Carolina.

Tunnell, K. (2004). *Pissing on Demand*. New York : New York University Press.