Pour une éthique des nouvelles (et anciennes) techniques de contrôle et de surveillance[1]

Le respect de l'ordre public fait aujourd'hui figure de priorité dans nos démocraties occidentales. Au nom de ce respect, le déploiement d'outils de contrôle et de surveillance ne cesse de se renforcer. De la vidéosurveillance dans les lieux publics jusqu'aux fuites de données personnelles sur Internet, ce contrôle social se fait parfois au détriment des libertés individuelles et du respect de la vie privée des citoyens.
Gary Marx, professeur émérite de sociologie au MIT (*Massachussetts Institute of Technology*), se saisit de cet enjeu pour proposer une éthique de la surveillance, qui concerne tant les outils employés que le comportement des agents chargés de ce contrôle. Sans tomber dans la démonologie consistant à présenter ces agents comme guidés par de mauvaises intentions, l'auteur suggère des questions élémentaires que les acteurs de la surveillance doivent se poser avant de déployer une procédure. Ces questions concernent les conditions préalables de cette procédure, les moyens déployés, les buts recherchés, l'adéquation entre ces moyens et ces buts, les modalités de recueil et d'analyse des données et l'appréhension des conséquences néfastes des techniques de contrôle.
Gary Marx livre ici une analyse opérationnelle qui aura valeur de guide pratique pour bon nombre de managers amenés à mettre en place des procédures de contrôle, et pour le citoyen en général.

Si ça ne sent pas bon, c'est que ce n'est pas éthique (expression populaire).

J'étudie l'informatique. Parce qu'un jour je veux être certain de ne pas me tromper (un étudiant du M.I.T.).

Il y a longtemps que les aspects sociaux, politiques et culturels des nouvelles technologies de contrôle social m'intéressent. Plusieurs de mes enquêtes (certaines en français) sont disponibles sur www.garymarx.net.[2] Elles portent à la fois sur le fonctionnement étatique, la consommation, les jeux, la famille..., ce qui m'a permis d'identifier les éléments du contrôle social, ses procédés et structures, ses buts, les données qu'il recueille et son historique

[1] *Cet article est inspiré du nouvel ouvrage de G.T. Marx, Windows Into the Soul : Surveillance and Society in an Age of High Technology, University of Chicago Press, à paraître, 2011.*

[2] *Des exemples des problématiques citées seront trouvés in Marx, 1988a ; Lianos, 2001 ; Lyons 2007 ; Norris and Wilson, 2006.*

culturel. Dans ce travail, j'ai tenté de rester objectif en suggérant des catégories de questionnement sans prétendre pour autant à la neutralité. La recherche est en fait obligatoirement entrelacée de préoccupations morales. Une pratique sociale est-elle en effet bonne ou mauvaise en soi, souhaitable ou non ? Ces questions sont au cœur du contrôle social d'aujourd'hui. Des expressions populaires comme « si ça ne sent pas bon, c'est que ce n'est pas éthique » ou « on ne traite pas les gens comme cela » semblent indiquer que l'éthique est enracinée dans la culture populaire. La collecte de données personnelles et les efforts de protection qu'on y attache indiquent des soucis d'éthique non clairement formulés. Dans ce qui suit, il est suggéré un cadre éthique pour penser le contrôle social des individus, que ce soit par les nouvelles ou anciennes méthodes (comme les écoutes ou le recueil d'informations privilégiées). D'une façon générale, il y a des attentes dans les pays occidentaux et industrialisés-capitalistes (et peut-être au-delà) dont la violation sous-tend le malaise, l'ambivalence perçue à l'occasion du franchissement des barrières de la vie privée. Cet article suggère des questions élémentaires qui peuvent aider les acteurs principaux dans ce domaine à juger le contrôle social projeté comme acceptable ou non, ou du moins à savoir le mettre en cause en général ou en particulier. Le tableau suivant récapitule les questions que l'on peut se poser à ce sujet, et qui seront ensuite traitées individuellement dans l'article.

Prérequis pour juger de la validité d'une technique de surveillance :

CONDITIONS PREALABLES
- Procédure officielle et consultation du public sur le projet / Inversion des rôles
- Possibilité de restauration de l'ordre antérieur / Conséquences imprévues de la mesure
- Signification symbolique de la mesure / Réversibilité en cas d'échec
- Compétence et budget du service chargé de l'application de la mesure

MOYENS
- Validité / Valeur du projet / Contrôle humain des procédures mises en place / Moyens alternatifs

BUTS
- Buts appropriés et non déviés / Clarté des buts fixés / Usage unique des données

RELATIONS ENTRE MOYENS ET BUTS
- Juste adéquation entre moyens et buts / L'inaction comme solution / Proportionnalité

RECUEIL ET ANALYSE DES DONNEES
- Critère de sélection de l'échantillon / Principe de retenue / Violations du droit à l'intimité
- Violation des principes de base

CONSEQUENCES NEFASTES DES TECHNIQUES DE CONTROLE
- Torts et dommages causés au moment de la collecte des informations
- Désavantage structurel d'une des parties / Avantage stratégique déloyal
- Avantage par manipulation / Dommage créé à la réputation d'un sujet
- Trahison de la confiance ou violation de la confiance donnée
- Intrusions dans la vie privée par abus de faiblesse

Les questions qu'on peut poser

L'analyse s'intéressera plus aux « contrôleurs » qu'aux « contrôlés ». Elle évite de porter tort à quiconque se penche sur les individus plutôt que sur les groupes, le court terme plus que le long, et les pratiques de contrôle les plus courantes et les plus acceptées plutôt que les cas d'urgence et d'exception. Toutefois beaucoup des idées exprimées ici peuvent trouver une application plus générale.

Les questions sont organisées selon les catégories suivantes : a/ conditions préalables, b/ moyens, c/ buts, d/ relations entre buts et moyens, e/ collecte de données et analyse, f/ conséquences néfastes pour les sujets et les autres, g/ protection des données et suivi de celles-ci.

a) Conditions préalables : politiques, procédures et potentialités

Procédure officielle et apport du public dans la décision à prendre : est-ce que la décision de mettre en œuvre une technique sensible résulte d'une étude préalable précise dans laquelle les parties concernées (dans ou en dehors de l'organisation) sont consultées ?

En prenant la décision d'adopter ou non la mesure, la procédure doit prêter attention à des questions impliquant la possible inversion des rôles, la restauration du *statu quo ante*, les conséquences imprévues de la mesure appliquée, les significations symboliques de celle-ci et la réversibilité des choses. Ces facteurs élargis sont à part des spécificités de la tactique en cause ou encore de son efficacité.

Inversion des rôles : est-ce que les responsables du contrôle (responsables de la décision d'appliquer la mesure et de sa mise en œuvre proprement dite) seraient d'accord pour être soumis à leur tour à ces règles de surveillance si les rôles contrôleur/contrôlé étaient inversés ? Ne penseraient-ils pas alors à des moyens de neutralisation de la mesure envisagée ? C'est un aspect de la règle d'or, limitée ici à l'inversion de rôle dans une organisation, qui fait écho au principe de réciprocité ou de cohérence de Kant : que se passerait-il si tout le monde avait la possibilité d'appliquer une mesure quelconque en tant que sujet/acteur à la fois ou alternativement et non plus en tant qu'objet de cette mesure ? La question reflète un aspect du principe d'égalité (chacun son tour) mais elle peut aussi avoir une qualité instrumentale puisque les acteurs vont modérer leur propre comportement de peur de recevoir le même traitement en cas d'inversion des rôles.

Que se passerait-il si tout le monde avait la possibilité d'appliquer une mesure quelconque en tant que sujet/acteur à la fois ou alternativement et non plus en tant qu'objet de cette mesure ?

Restauration : la technique envisagée rompt-elle radicalement avec les garanties traditionnelles de protection des données personnelles ? Est-ce que ces protections pourraient au besoin être réinstaurées par d'autres moyens (légaux ou techniques) ? Réfléchissons par exemple à l'apparition systématique de l'appelant qui supprime l'anonymat de l'appel ou aux infrarouges ou rayons x qui permettent de voir à travers les murs, les vêtements, la peau.

Un aspect important de l'encadrement du contrôle social repose donc sur la manière de rétablir, si besoin est, des conditions de contrôle raisonnables dignes d'être protégées/sauvegardées avant la mise en place d'un nouvel outil. Reste à s'entendre sur ce que veut dire « raisonnable ».

Aux Etats-Unis par exemple, la Cour Suprême a donné sa version de ce qui lui paraissait raisonnable en matière de standard de protection de la vie personnelle dans la décision Katz en 1967.
Dans certaines conditions, cette restauration du *statu quo ante* peut ne pas être souhaitable ou simplement possible et il faut alors que les avocats de la mesure envisagée expliquent pourquoi il devient indispensable de rendre la mesure antérieure inopérante ou pourquoi il faut carrément la détruire.

Conséquences imprévues de la mesure : est-ce que la technique envisagée peut créer des précédents qui conduiront à ce qu'elle soit utilisée dans des secteurs indésirables ? Quelles conséquences imprévues aura-t-elle alors pour les gens qui y seront soumis, les agents chargés de sa mise en œuvre, les tierces parties et la société en général ? Même si une nouvelle tactique est censée être efficace, il importe de la penser dans le long terme pour voir ce qui peut en découler[3]. En quoi les libertés traditionnelles et les valeurs démocratiques de base pourraient-elles en être affectées ? Est-ce que la nouvelle technique amènera des opposants à en faire usage ? Est-ce que les agents chargés de l'appliquer feront face à de nouveaux risques ? Il est plus facile de juger *a posteriori* que de prévoir les conséquences inattendues d'une décision qui ne sont souvent perceptibles qu'après un certain temps. D'où l'intérêt de s'intéresser à l'expérience des autres acteurs ou d'autres pays.

Des pratiques peuvent apparaître moralement condamnables parce qu'elles violent un principe fondamental comme le respect de la dignité des personnes.

Signification et valeur symbolique de la mesure : est-ce que l'outil projeté et la façon dont il va être appliqué prend en compte la perception de citoyens possédant des droits dignes d'une démocratie ? Ou est-ce que l'individu est réduit à un simple sujet sans droits qui doit se soumettre aux intérêts et pouvoir coercitif d'une organisation capable d'appliquer à tous sans exception des mesures violant voire dégradant leur vie privée ? Les moyens d'évaluer la communication symbolique sont plus subjectifs que pour la plupart des autres questions ; mais on peut toujours commencer par se demander si « cela a l'air bien ». Des pratiques peuvent apparaître moralement condamnables parce qu'elles violent un principe fondamental comme le respect de la dignité des personnes.

Réversibilité : si une mesure mise en œuvre se révèle dans la pratique indésirable, sera-t-il néanmoins aisé de l'abroger malgré les investissements consentis et les intérêts plaidant en faveur du nouveau *statu quo* ?
Si les réponses aux questions ci-dessus plaident en faveur de l'adoption d'une nouvelle technique, il faut ensuite songer à mettre en place les procédures, ressources et politiques nécessaires pour la gérer, en particulier pour garantir l'intégrité, la juste application et l'efficacité du système. Les politiques définiront qui sont les agents et les sujets, leurs droits et responsabilités, comment et quand les données seront recueillies, fusionnées, changées, analysées, interprétées, évaluées, utilisées, communiquées, protégées, mises à niveau ou expurgées et qui y aura accès de l'intérieur ou de l'extérieur.

La question de la compétence et des moyens des organisations concernées se posera alors : ont-elles les budgets, les savoirs et la motivation pour appliquer avec succès comme il

[3] *Les agents chargés du contrôle peuvent fort bien se montrer mesurés dans un premier temps d'accoutumance, avant d'élargir ensuite abusivement leurs procédés sans le dire. Ce qui pose la question d'un contrôle nécessaire pour éviter des ajouts à une mesure initiale lui faisant perdre son caractère d'acceptabilité.*

convient la mesure et en interpréter les résultats ? Est-ce qu'elles sauront s'auto-évaluer par une réflexion critique sur l'usage de pratiques sensibles ? Par exemple, dans le cas de pratiques d'infiltration policière (qui peuvent être redoutablement efficaces), le problème n'est pas la valeur en soi de la tactique mais plutôt les risques qu'elle fait courir à la police, auquel cas il faudra savoir si elle disposera des moyens requis pour les gérer. Un autre exemple peut être donné avec l'USTSA (administration chargée des contrôles aéroportuaires aux Etats-Unis) : les critiques qu'on lui adresse ne portent pas sur les technologies employées mais sur la capacité et la formation des individus qui ont vocation à les utiliser au quotidien.

b) Moyens

> « Chaque façon de voir est aussi une façon de ne pas voir... »

Adéquation et validité : est-ce que la mesure est appliquée de manière valide au regard de son potentiel global ? Une tactique valide peut en effet être mal appliquée ou encore ne pas être fiable dans tous les cas. Quel est alors le consensus entre spécialistes à propos d'une tactique donnée et ses mérites ? La validité est un concept social fluctuant. Le philosophe Alfred Whitehead faisait un jour l'observation suivante : « *Chaque façon de voir est aussi une façon de ne pas voir...* ». Cela pose la question de la légitimité des avis donnés : qui a le pouvoir de dire ce qui est valide/juste/équitable ? Quel niveau de certitude est requis pour qu'une mesure soit admise au vu de ses résultats ? Comment définit-on la ligne entre ce qu'on pensera être acceptable comme niveau de preuve et ce qui ne l'est pas ?

Contrôle humain : existe-t-il des dispositifs permettant de vérifier les résultats et de contrôler à intervalles réguliers l'outil lui-même ? Y a-t-il une forme de vérification humaine des résultats produits par les machines : à la fois des données de base et éventuellement des recommandations d'action automatisées ? Les machines sont aussi faillibles que ceux qui les construisent. Le contrôle humain des résultats et préconisations automatisées reste essentiel dans beaucoup de configurations vu les ratés tant des supports matériels informatiques que des logiciels. Cela est particulièrement sensible quand une décision vitale doit être prise. Un individu est souvent mieux à même d'apprécier les nuances de situations propres à l'humain que ne le sont les ordinateurs, souvent faillibles malgré leur prix.

Solutions alternatives : le moyen mis en œuvre est-il le mieux adapté ? Comment se compare-t-il avec d'autres en ce qui concerne sa facilité d'application, sa validité, son coût, ses risques et ses incertitudes de mesure des résultats ? Est-on plus enclin à compter (dans les deux sens) ce qui peut être quantitativement mesuré facilement et à faible coût plutôt que de s'intéresser à ce qui est directement lié au but fixé ?

c) Buts

Légitimité des buts : les buts de la collecte de données sont-ils justifiés et en phase avec les bénéfices qu'on en attend ? La logique surveillance/contrôle mérite-t-elle qu'on s'y attarde dans un environnement donné ? Des buts clairs et non polémiques comme la santé publique et la sécurité sont plus faciles à reconnaître que d'autres qui seront alors, à cause de leur nature douteuse, probablement camouflés en buts acceptables pour se faire accepter.

Un recueil de données acceptable pour un but donné dans un contexte précis peut devenir inacceptable dans un autre. Prenons des exemples :

- dépistages d'usage de stupéfiants sur les chauffeurs de bus scolaires et dépistages sur

des jeunes qui veulent s'inscrire à l'orchestre de leur école (comme on l'a vu aux Etats-Unis) ;

- un gynécologue demandant à ses patientes leur passé clinique en matière de contraception et d'avortement et une compagnie aérienne (américaine) posant à toutes ses employées la même question sans préciser en quoi cette information était nécessaire...

Même quand le but d'une mesure est acceptable, il y a fort à parier que si les résultats recueillis étaient utilisés dans un autre cadre, la controverse en jaillirait. Par exemple, est-il légitime d'utiliser les résultats d'un test de capacité pulmonaire pour apprécier si les salariés se conforment ou non à la politique anti-tabac de l'entreprise ? On dit aux salariés que c'est une mesure indispensable pour leur santé, bonne en soi à la fois pour eux et l'entreprise, et qui vise à faire des économies. Mais des salariés peuvent parfaitement percevoir cette démarche comme mauvaise et malsaine parce qu'elle tend à contrôler leur comportement en dehors du travail, dans leur vie privée.

Transparence des buts fixés : les buts fixés sont-ils bien transparents et hiérarchisés ? Quand la confidentialité s'impose et que les buts n'ont reçu aucune publicité, est-on certain qu'ils ont au moins été bien définis au sein de l'organisation qui les met en place ?

Agréger des données de diverses sources de profilage, de rapprochement etc., peut aboutir à des informations dont la somme excède de loin les éléments individuels.

Usage unique : les données sont-elles utilisées pour le seul usage qui a justifié leur recueil, en ligne avec la compréhension qu'en avaient les sujets et leur accord spécifique ? Est-ce que les données restent contrôlées par le responsable du traitement ou migrent ailleurs ? Est-ce par manque de fiabilité ou de sécurité du système ?
Aux Etats-Unis, beaucoup plus qu'en Europe, il est fréquent que de nombreux utilisateurs de données soient interconnectés entre eux. Or agréger des données de diverses sources de profilage, de rapprochement etc., peut aboutir à des informations dont la somme excède de loin les éléments individuels.

d) Relations entre buts et moyens

L'adéquation entre les moyens et le but : y a-t-il un lien clair entre l'information recherchée/recueillie et le but à atteindre ? Comme déjà noté, un test de dépistage d'alcool ou de stupéfiant ou une vérification des kilomètres effectués ou encore du lieu de résidence (moyens) peuvent avoir d'autres buts que ceux visés par les résultats de l'enquête, laquelle peut fort bien être valide[4] dans ses affirmations brutes mais sans rapport avec le but réel non avoué.
Plus nous nous éloignons des résultats directs d'une mesure légitime et fiable au regard de son but (exemple d'une mesure de chaleur ou de localisation grâce à des sondes) pour aller vers des buts basés sur des inférences de probabilité portant sur des comportements futurs, comme cela se pratique dans le profilage, plus l'utilité des données recueillies diminue. Un profilage comme celui utilisé pour prédire qui peut se livrer à des détournements d'avion (des jeunes gens achetant un seul ticket aller avec du liquide) implique le recueil d'informations très précises mais une faible corrélation avec tous les cas ultérieurs.

[4] *Une mesure peut être efficace mais non valide à cause des mécanismes mis en place, comme dans le cas du détecteur de mensonge qui « marche » quand les gens disent la vérité parce qu'ils ont peur que leurs mensonges soient détectés.*

Inaction/action : quand le seul outil disponible est trop cher et/ou trop risqué ou encore trop peu en lien avec le but recherché parce que ce qu'il faut détecter est trop difficile à trouver ou statistiquement improbable, a-t-on aussi réfléchi à ne rien faire tout simplement, ou encore à redéfinir le but ? C'est l'exemple de la décriminalisation de l'usage de marijuana étant donné l'échec des efforts de la poursuite pénale et les conséquences indirectes non souhaitées de cette poursuite.

Proportionnalité : est-ce que les moyens et les fins sont proportionnellement adaptés ? Cela demande de faire attention à la fois aux problèmes et aux avantages amenés par la taille des moyens mis en œuvre par rapport au niveau d'importance du but. Un marteau pilon n'est pas nécessaire pour casser une noix. Inversement, un tuyau d'arrosage n'éteindra pas un incendie de maison. Il faut toujours limiter la mesure à son but et en vérifier l'efficacité.

Il existe un réel contraste entre la vérification systématique de tous les passagers sur un vol et le contrôle aléatoire mais très poussé d'un nombre réduit de voyageurs au passage d'une frontière.

e) Recueil et analyse des données

Critères de sélection de l'échantillon : est-ce qu'on retient des critères aboutissant à une systématisation du recueil et des mesures appliquées à tous les sujets ? Le cas échéant, ces sujets sont-ils pour autant tous soumis aux mesures de surveillance/contrôle ? Reste à vérifier qu'ils aient tous une probabilité égale d'être visés par les mesures arrêtées même si tous ne le seront pas ? A titre d'illustration, il existe un réel contraste entre la vérification systématique de tous les passagers sur un vol et le contrôle aléatoire mais très poussé d'un nombre réduit de voyageurs au passage d'une frontière. Quand il n'existe pas d'indication précise de ce qu'il faut chercher, un contrôle superficiel préliminaire de tout le monde peut également permettre de détecter qui doit subir un contrôle plus approfondi.
Si une technique invasive de libertés ou de vie privée est appliquée au nom d'un bien public et qu'il n'y a pas lieu d'établir une différenciation des sujets, l'équité voudrait que tous soient effectivement soumis à cette mesure ou du moins que tous puissent également être visés. Mais en pratique, des budgets limités peuvent très bien ne pas le permettre. La stratification sociale peut aussi aboutir à ce que certaines classes privilégiées soient exclues des mesures en cause. Exemple : les dirigeants d'une entreprise donnée sont-ils soumis aux mêmes mesures de détection d'usage de stupéfiants et aux mêmes restrictions d'usage des outils de communication de l'entreprise que leurs salariés ?

Principe de retenue : fait-on un effort pour minimiser le caractère invasif de la technique envisagée et l'étendue de la communication de l'information personnelle directe ou indirecte collectée ? Ceci recoupe d'autres questions sur les moyens alternatifs, les buts, la spécificité du choix des sujets, la collecte des données et la protection de celles-ci pour éviter qu'elles soient utilisables par d'autres. Les méthodes les moins invasives doivent donc toujours être préférées, seules les informations personnelles directement liées au but recherché doivent être recueillies, et pas davantage que nécessaire.
Un aspect important du principe de retenue est de savoir si les données recueillies sont directement liées à une personne qui peut être située géographiquement, à une personne identifiée individuellement ou si les données sont anonymisées. Pour de nombreuses transactions, tout ce qui est requis est la preuve que le sujet potentiel

est dans une catégorie qui lui donne droit à bénéficier de biens ou de services. Nul besoin d'en savoir davantage sur lui. Exemple : l'accès aux autoroutes payantes ou aux outils payants de communication ne nécessite rien de plus que de savoir que le service a bien été payé, pas de connaître l'identité de l'utilisateur.

Intrusion dans la vie privée : la technique passe-t-elle la frontière de la vie privée à un endroit sensible sans autorisation ni permission (soit coercitivement, soit frauduleusement), ou encore une frontière physique, relationnelle, spatiale ou symbolique ? Le consentement éventuellement donné est-il sincère?

Irrespect des conditions préalables : la technique en cause viole-t-elle les conditions posées pour la collecte des données personnelles ? Ceci peut impliquer des normes, souvent tacites, ou des attentes culturelles sur la qualité réelle des personnes qui posent les questions, sur la croyance que des informations réputées confidentielles le resteront ou qu'il n'y aura pas de liste noire gouvernementale. Cela peut aussi impliquer le non-respect de politiques explicites ou de promesses telles que la destruction ultérieure des données collectées[5].

Préjudices infligés lors de la collecte des données : est-ce que le recueil des données peut entraîner un trouble physique ou psychologique ? Des tactiques de questionnement (opposées au recueil passif de données) sont par exemple basées sur des outils de pression comme la peur ou la menace d'infliger des préjudices ou torts importants. La torture en est l'exemple extrême. Mais un interrogatoire n'a pas forcément besoin d'être assorti d'une menace de violences physiques pour se révéler stressant ou problématique sur le plan éthique.

Un interrogatoire n'a pas forcément besoin d'être assorti d'une menace de violences physiques pour se révéler stressant ou problématique sur le plan éthique.

Interrogatoires, tests psychologiques, dépistages de stupéfiant et fouilles peuvent être utilisés pour augmenter ou réduire un sentiment de malaise. Se faire interroger sur des sujets sensibles et voir des données personnelles recueillies peut évidemment procurer de la gêne, de la honte, un sentiment de malaise ou d'impuissance et/ou ramener le souvenir de faits douloureux. Les méthodes de l'agent collecteur et les conditions du moment peuvent aussi contribuer à exacerber ces désagréments. L'agent peut aller plus loin que nécessaire dans ses questions ou au-delà de ce à quoi il s'était initialement engagé. Regardons par exemple les conséquences psychologiques de la prise de sang pour les tests obligatoires HIV dans les prisons ou à l'armée, ou encore le stress supplémentaire que l'on peut exercer dans l'usage du détecteur de mensonge (en resserrant les menottes par exemple).

f) Conséquences néfastes des techniques de contrôle

Torts causés aux personnes : les résultats du recueil de données ou de la surveillance causent-ils un tort ou un inconvénient imprévus aux personnes concernées, à l'agent, à une tierce personne ? On pourrait en parler longtemps, surtout savoir si cela devrait être défini en termes objectifs ou subjectifs et/ou si l'intention de l'agent devrait être considérée en dehors des conséquences mesurables.
Quelques formes de torts parfois rencontrées :

[5] *Le cas est probable avec des données recueillies par un gouvernement. Exemple de la Grèce (Samatras, 2004) où on s'est aperçu que des données n'avaient pas été détruites comme le gouvernement l'avait prétendu, mais transférées vers des opérateurs privés. Le fait de ne pas enregistrer ou documenter le recueil de données quand la loi le demande présente le problème inverse.*

- avantage stratégique illégitime : exemple du dévoilement d'une information que le sujet aurait aimé protéger en la gardant pour lui à cause d'un conflit d'intérêts légitime. Pensons à l'espionnage industriel ou par exemple à un hall d'exposition de voitures d'occasion piégé avec des caméras : le vendeur pourra apprendre les goûts de son client et combien il est prêt à mettre ;
- avantage déloyal : quand on persuade ou influence un sujet dans ses choix par ces méthodes, soit pour des objets de consommation courante, soit en politique. Le cas extrême est le chantage et l'intimidation. Mais pensons aussi à l'exemple plus bénin d'une société de sucreries qui enverrait une publicité avec ristourne spéciale à une liste de gens faisant un régime alimentaire et ce, grâce à une liste nominative achetée à un fournisseur quelconque ;

Croire que l'on est surveillé en permanence peut inhiber l'innovation et l'expérimentation et tuer la prise de risques.

- limitation des droits dans la société civile courante : traitement inéquitable de sujets au regard d'informations non valables, inappropriées, non contextuelles ou encore discriminatoires. Les exemples abondent dans le secteur de la banque, assurance, logement, emploi et même dans la consommation courante. Oscar Gandy (1993) a montré comment la recherche sur les attitudes des acheteurs dans le secteur de la consommation pouvait se retourner contre les intérêts des moins privilégiés ;
- dommage causé à la réputation à cause d'une publication non contractuelle d'information personnelle : il peut en résulter gêne, honte, humiliation, ou cela peut encore présenter une personne sous un jour défavorable[6] ;
- au-delà de leur capacité à nuire, les détournements de procédures et les plaintes exagérées des victimes (visant à créer le mythe orwellien de la surveillance absolue) peuvent conduire au sentiment généralisé de trahison de la confiance et à la croyance systématique aux procédés déloyaux (même à tort). La confiance est un élément central de spontanéité, de sociabilité et de savoir vivre ensemble. Son absence rend la coopération difficile dans un groupe donné. Croire que l'on est surveillé en permanence peut inhiber l'innovation et l'expérimentation et tuer la prise de risques ;
- les données issues des techniques de surveillance (à la fois le recueil et l'utilisation) peuvent induire un isolement non souhaité puisque des individus peuvent perdre le contrôle de leur vie privée au profit d'acteurs extérieurs. Le fait de collecter des données peut perturber le sens de l'espace personnel et de sécurité. L'utilisation extensive de résultats spécifiques peut aboutir à un démarchage ciblé *via* l'usage non souhaité des moyens de communication de la cible (fax, téléphone, ordinateur).
  Des sollicitations automatiques peuvent en plus ressasser un souvenir que l'on voudrait oublier. Pensons au tort que ferait un courrier circulaire pseudo-personnalisé qui commencerait par des félicitations à des personnes censées être les parents d'un enfant pour son premier anniversaire, courrier renouvelé tous les ans. Le but est de vendre quelque chose à un enfant d'un an. Les données ont été achetées

[6] *Le tort fait à quelqu'un qui n'a rien à se reprocher est rarement étudié : cas des alarmes de portiques qui se déclenchent à tort, ou encore rejet d'une carte de crédit parfaitement valide et approvisionnée.*

à un prestataire de santé. Comment un couple qui a aurait eu le malheur de voir la grossesse s'achever en fausse-couche non répertoriée dans la *data-base* réagirait-il à la réception de ce courrier ? Ce cas réel d'un courrier de masse peut créer un mal considérable[7]. Ou encore imaginons un courrier circulaire à de jeunes retraités vantant les mérites de la crémation sur l'inhumation classique...

- non participation à la richesse créée : le bénéfice ou le profit qu'une compagnie va tirer de la vente d'une liste de données personnelles sera-t-il partagé avec les individus concernés ? La personne a-t-elle donné l'autorisation de la réutilisation de son nom ? Des magazines, conscients de cette problématique offrent par exemple un mois d'abonnement en échange d'une telle permission.

g) Les budgets et les droits des personnes concernées affectent les conséquences des techniques qui leur sont imposées

> Il ne devrait y avoir aucune base de données secrète en démocratie.

Droit d'inspection : est-ce que les sujets sont au courant des résultats d'enquête et de la manière avec laquelle ils ont été trouvés ? Des aspects fondamentaux de la procédure judiciaire impliquent le droit de connaître et de remettre en cause les éléments personnels détenus par des administrations opaques et kafkaïennes. Dans le cas de la puissance étatique, le droit pour un citoyen d'accéder à son dossier est lié à un principe plus large selon lequel, en l'absence de conditions spéciales, il ne devrait y avoir aucune base de données secrète en démocratie.

Droit de consultation et de rectification : existe-t-il des procédures pour regarder avec un esprit critique les résultats et pour corriger les données recueillies ou les interpréter ?

Rectifications et sanctions : si un tort a été fait à quelqu'un, comment le voir et le détecter et, au besoin, rectifier ou détruire la donnée erronée ? Comment diminuer ou supprimer ces cas ? Existe-t-il des audits et des sanctions pour le responsable du fichier et des solutions justes et équitables à ces conflits ?
A l'inverse de l'Europe et du Canada, où des autorités de contrôle peuvent veiller à la conformité des données et de leur recueil, aux Etats-Unis, c'est en général aux individus de se défendre seuls. Pour que cela soit possible, ils doivent d'abord savoir qu'il y a eu un problème et que celui-ci obéit à des règles[8]. Des agents spécialisés (inspecteur général de contentieux, auditeurs ou encore groupements de veille d'intérêt public) représentent d'autres façons de traiter le problème. Le développement de « correspondants protection des données personnelles » dans les organisations est un instrument d'inspection plus récent. Mais peuvent-ils être vraiment indépendants et efficaces si leur rôle remet en cause l'organisation elle-même ?

Egal accès aux outils de surveillance : dans des systèmes théoriquement réciproques, est-ce que les moyens de surveillance sont en priorité ou proportionnellement accessibles aux puissants ou aux experts ? Comparons la possibilité d'utiliser les images satellites avec les photos faites par un téléphone. Demandons-nous si les médecins

[7] *Le mauvais ciblage fait ici allusion à des catégorisations qui sont valables dans l'ensemble mais pas forcément dans les cas particuliers. C'est l'éternelle question des profilages et des généralisations qui balancent entre efficience de la mesure globale et cas particuliers, source de conflits incessants.*

[8] *Problème de la découverte accidentelle ou non de données illégales, Marx (1984).*

doivent/peuvent dévoiler des informations personnelles (dans des investigations faites par un panel de professionnels par exemple) sur des patients, comme si, dans le même temps, les patients avaient la possibilité d'entreprendre des recherches sur les médecins pour savoir s'ils ont déjà été eux-mêmes poursuivis par des tribunaux ? A l'inverse, peut-on imaginer qu'un médecin demande à un patient quelles sont ses attitudes face aux drogues ou au sexe dans un environnement clinique sans que le patient puisse poser la même question au docteur (possibilité ou non du principe d'inversion des rôles).

Egal accès aux outils de neutralisation : dans les systèmes où la neutralisation des informations est légitime (soit parce que les règles l'autorisent, soit parce que le comportement des agents est sujet à caution et le justifie), est-ce que les moyens pour y parvenir sont plus accessibles aux plus privilégiés, puissants ou technologiquement capables ? Les moyens de maintenir un contrôle sur des données personnelles comme de donner un faux nom ou adresse quand la demande de les fournir n'est pas légitime (comme si on payait avec du liquide dans un magasin) ou avec les services gratuits de transmission d'e-mails, sont-ils facilement accessibles à tous ? Car protéger les données peut requérir des compétences techniques ou coûter de l'argent comme c'est le cas avec un broyeur de papier, une liste rouge ou encore acheter un plus grand degré de confidentialité.

Conséquences pour les agents et les tierces parties

Torts faits aux agents du contrôle : est-ce que la pratique en cause fait ou non du tort aux agents qui la mettent en œuvre ? Y a-t-il des impacts sur les valeurs et la personnalité de ceux-ci ? S'il y a des risques, peut-on les réduire ou y porter remède ? Exemple : le super tueur électronique Harry Caul dans le film « La conversation ». Au cours de sa carrière, Caul devient paranoïde, sans personnalité et insensible aux aspects éthiques de son travail. Les agents infiltrés font face eux aussi à une variété de risques de cette nature, depuis l'agression jusqu'aux tentations de devenir criminels au détriment de leur équilibre psychique et familial. Il y a des présomptions que les policiers qui utilisent les radars contre les excès de vitesse aient plus de cancers que les autres policiers.

Fuites vers des personnes non concernées : comment s'assurer que la pratique retenue reste limitée aux seuls sujets concernés ? Peut-on éviter des effets indirects indésirables ? La mesure est-elle bien ciblée et restreinte ? Des enregistrements audio et vidéo de sujets visés par la mesure, de leur famille et amis peuvent se trouver en circulation ; des analyses d'ADN peuvent donner des renseignements sur des membres de la famille dont l'ADN n'a pas été recueilli.

h) Protection des données et suivi dans le temps

Contrôle périodique : est-ce que le système est régulièrement révisé pour s'assurer de son efficacité, de sa justesse et de son fonctionnement conforme aux politiques initiales ? Et si non, faut-il les revoir ? Faire des audits ? Des inspections suivies d'effets ?

Suivi dans le temps : des règles sur la rétention ou destruction des données existent-elles et sont-elles respectées?

Questions sur les questions

Comme on l'a suggéré plus haut, plus ces questions sont présentes dans les réponses apportées, plus la situation dans laquelle on se trouvera sera probablement éthique. Ce qui n'empêche pas de s'interroger sur les valeurs sous-jacentes.
Y a-t-il des procédures et des politiques couvrant les sujets de base ? Sont-elles bonnes en subs-

tance ? Sont-elles mises en pratique ? L'organisation fait-elle régulièrement des autocontrôles à travers des audits et des inspections ? Le public sera-t-il au courant si des politiques échouent ?
S'inquiéter de savoir si les politiques sont suivies et respectées peut se vérifier à travers toutes les applications ou par une sélection de celles-ci. Exemple : la validité et les conséquences d'un dépistage de drogue comme classe d'objet.
Des distinctions sont aussi parfois nécessaires : entre rejeter, limiter ou revoir une tactique comme le détecteur de mensonge à cause des doutes sur son efficacité, mais également pour faire la distinction entre le rejet d'une application particulièrement défectueuse alors que la pratique et la tactique sont bonnes.
Quand des manquements/échecs sont identifiés, il est crucial de savoir s'ils sont idiosyncrasiques et apparemment aléatoires ou systématiques. D'où vient le problème ? Combien de fois des problèmes particuliers doivent-ils apparaître avant qu'on en conclut à la mise en cause du système plutôt qu'à une occurrence malheureuse mais tolérable ? Si c'est le système, peut-on le réparer ?

a) Tout dépend du contexte

L'analyse a au moins démontré un élément essentiel. La surveillance publique n'est pas bonne ou mauvaise en soi, tout dépend du contexte dans lequel elle est pratiquée (au moins dans la majorité des cas). La grande variation des méthodes de surveillance, leurs buts, systèmes, relations, applications dans le temps et spécificités illustrent l'importance d'établir des distinctions – que ce soit pour l'intérêt de la science sociale ou pour le raisonnement. Une approche éthique est toujours préférable à une approche sur la technicité des systèmes ou à une intellectualisation ou encore des *a priori* rigides sur ceux-ci.
Le livre dont cet article est inspiré (cf. note 1) propose des exemples pris dans des industries de haute technologie, une association de protection de l'enfance, chez un *free lance* curieux de tout et un leader du secteur privé de la surveillance du public. Toutes les histoires rapportées sont remplies d'humour et illustrent bien l'incompréhension entre les comportements des « surveillants » et des « surveillés » qui se posent des questions sur la légitimité des techniques mises en place (travail-maison ; relations personnelles-anonymes ; Etat-société civile). Un facteur clé est la compréhension du positionnement des frontières entre tous ces éléments comme on le voit entre règles, attentes du public, système appliqué et comportement des gens soumis à la mesure.
En écrivant sur le respect à la vie privée, Helen Nissenbaum (2010) développe de façon intéressante des idées de contexte d'intégrité. Cette perspective peut être appliquée plus généralement, du respect de la vie privée au concept plus large de la surveillance[9].
En étudiant des pratiques policières d'infiltration, j'ai souligné l'importance des règles et des attentes moins formelles dans des contextes spécifiques, opposées aux éléments intrinsèques d'un outil pour atteindre des résultats (Marx, 1988). Cette méthode est tout aussi valable pour d'autres formes de surveillance.
Le fait d'avoir une technique moralement acceptable est objectivement insuffisant pour en justifier l'emploi, de même qu'un but satisfaisant n'est pas une justification pour utiliser un moyen douteux ou inutilement risqué ou dangereux. Mais même avec une technique et un but moralement justifiés, des préoccupations éthiques peuvent aussi survenir ensuite, comme avec la collecte des données, l'analyse, la protection des données et leur durée de rétention. Le statut éthique peut varier de cas où les moyens, buts et conditions d'emploi sont mauvais ou même odieux, à des cas où les moyens sont acceptables, voire souhaitables en des combinaisons variées. Une analyse plus précise et riche est possible

[9] *Un bon résumé de la position aux Etats-Unis sur la protection des données personnelles se trouve dans un rapport de Waldo (2007) à l'Académie Nationale Scientifique.*

quand des jugements sont liés à de telles distinctions.

> **Comparé au nombre étonnant de techniques de surveillance utilisées chaque jour, l'usage avoué de tactiques exécrables ou de dernière extrémité n'est pas très fréquent.**

Il existe à coup sûr des moyens de collecter des informations personnelles qui frappent les observateurs comme erronés ou à tout le moins troublants, sans parler des raisons pour lesquelles ils sont faits, et même de savoir s'ils sont valides et efficaces. La torture en est le cas le plus évident. Blesser ou menacer de quelque chose des amis innocents ou des membres de la famille en est un autre. D'autres moyens de surveillance comme le mensonge, la tromperie et la manipulation (comme dans l'infiltration policière), bien que parfois nécessairement pris en considération, sont rarement choisis dès le début. Comme Sissela Bok (1978) le fait remarquer à propos du mensonge, on ne devrait les utiliser que dans des circonstances limitées et quand il n'y a pas possibilité de faire autrement, parce que ces moyens présentent toujours un dilemme moral.
Malgré tout, comparé au nombre étonnant de techniques de surveillance utilisées chaque jour, l'usage avoué de tactiques exécrables ou de dernière extrémité n'est pas très fréquent[10].

b) Traiter la complexité, oui ; s'abstenir d'agir, non.

Dans le meilleur des mondes possible, le philosophe a besoin qu'une théorie soit fondée sur un raisonnement normatif formel offrant des justifications aux principes énoncés, indiquant leurs implications logiques et aboutissant à des conclusions claires. Un tel raisonnement anticipe et permet de répondre aux objections probables sur les systèmes mis en place. De surcroît, il est cohérent avec plusieurs types de justifications (par exemple, il ne confond pas des arguments basés sur des principes premiers absolus avec ceux basés sur des conséquences empiriques).
Comme un kaléidoscope disposant d'une unique source de lumière, une théorie éthique globale se doit d'éclairer et de lier entre elles toutes les formes du contrôle social. Ce serait bien sûr formidable si le monde avait été créé de telle sorte qu'une simple pierre de Rosette soit suffisante pour apprécier toutes les formes éthiques de contrôle. Mais un tel principe nécessiterait d'être si général qu'il en deviendrait inopérant et inintéressant (« faites le bien, évitez de faire le mal »).
L'alternative offerte par cet article est une approche inductive qui s'interroge sur le côté éthique des dispositifs et comportements multiples mis en place. Certes, la prise en considération complète des myriades de facteurs qui peuvent faire qu'une technique soit acceptable ou non pourrait effrayer l'observateur. La réflexion dans toute son étendue et sa finesse crée le risque d'être sans portée, de sembler irréaliste, voire de ne pas être lue. Ce qui peut déboucher sur la recherche de solutions faciles qui ignoreraient la complexité des conflits moraux. On court le risque de mésestimer les données du problème de l'inspecteur « Dirty Harry » (incarné par Clint Eastwood au cinéma) où les moyens employés ne peuvent qu'avoir des coûts chaque fois qu'on les mobilise (Klockars, 1980). On court également le risque de se contenter d'une quantification fallacieuse aboutissant à des décisions soi-disant « éthiques » mais en fait bureaucratiques et automatiques, fondées sur des statistiques, par exemple en comptabilisant les oui et les non apportés aux questions du tableau n° 1 et en appliquant la mesure qui recueille une simple majorité de oui.
J'ai recherché une position intermédiaire, en

[10] *Le fait que ce soit rare ne justifie pas les quelques exemples relevés ; c'est un facteur de prise en considération.*

jetant un filet assez grand pour attraper les formes les plus variées de contrôle et en les filtrant à travers certaines valeurs de base. L'insistance de cet article sur les agents chargés du contrôle reflète surtout le souci de s'intéresser aux abus susceptibles d'être commis dans les secteurs privé, public, ou dans de grandes organisations comme l'industrie ou encore à travers l'insuffisance d'accès aux outils de surveillance. Dans le même temps doivent être évités la démonologie qui consisterait à présenter les agents de la collecte des données comme systématiquement mauvais ; ou, à l'inverse, l'irénisme, qui consiste à voir parmi les sujets de la collecte de données des victimes systématiquement impuissantes dont les droits seraient toujours bafoués.

Nous jouons des rôles multiples et sommes tantôt des agents du contrôle et tantôt des cibles de celui-ci. Les organisations publiques et privées et tous ceux qui ont du pouvoir sont plus enclins à mettre l'accent sur leurs droits de collecter des informations personnelles que sur leurs devoirs ou sur les droits des gens soumis aux contrôles. Lesquels, de leur côté, montrent évidemment plus d'intérêt à protéger leur propre information qu'à reconnaître les droits qu'auraient certains à détenir des données sur eux-mêmes. La plupart des gens sont d'ailleurs relativement ignorants ou peu intéressés aux raisons et à l'utilité du recueil des données.

Dans des conditions satisfaisantes, on peut avoir le droit et même l'obligation de surveiller/contrôler. Mais il y a en parallèle l'obligation de le faire avec responsabilité et d'en rendre compte. Réciproquement, ceux qui sont visés par ces mesures ont également des obligations (comme celles de fournir des informations fiables et de ne pas menacer les agents), même s'ils ont, dans certains cas, le droit de ne pas être soumis à certaines formes de surveillance.

En dépit de tous les facteurs exposés ci-dessus qui plaident contre des généralisations trop larges de l'éthique de la surveillance, il faut souligner que ce qui sous-tend la réflexion consiste en la réaffirmation d'un ensemble de valeurs. Valeurs désirables en soi : honnêteté, équité. Mais également valeurs pouvant être des moyens utiles pour atteindre des buts plus collectifs (un minimum de légitimité démocratique dans les pratiques électives, de droit à la vie privée ou de transparence et de confiance entre gouvernants et gouvernés)

Dans les sociétés démocratiques, la question la plus importante, primordiale même, reste bien l'idée kantienne du respect de la dignité de la personne doublée du respect des conditions du droit, deux valeurs qui permettent de poursuivre la vie en commun. ■

Gary T. Marx,
professeur émérite de sociologie au M.I.T.
Massachussetts Institute of Technology

Bibliographie

S. Bok, Lying : Moral Choice in Private and Public Life, Pantheon, New York, 1978.

O. Gandy, The Panoptic Sort, Westview Press, Colorado, 1993.

C. Klockars, « The Dirty Harry Problem », The Annals 452 (Nov.), 1980, pp. 33-47.

M. Lianos, Le Nouveau Contrôle, L'harmattan, Paris, 2001.

D. Lyons, Surveillance Studies : an Overview, Polity Press, Cambridge, 2007.

G.T. Marx and N. Reichman, « Routinizing the Discovery of Secrets : Computers as Informants », American Behavioral Scientist, Vol. 27, no. 4, March/April, 1984.

G.T. Marx, « Notes on the discovery, collection, and assessment of hidden and dirty data », In Studies in the Sociology of Social Problems, ed. J. Schneider and J. Kitsuse, Norwood, NJ, Ablex, 1984.

G.T. Marx, « La Société de sécurité maximale », Déviance et société, vol. 12, no. 2, 1988a.

G.T. Marx, Undercover : Police Surveillance in America, Univ. of California Press, Berkeley, CA., 1988b.

G.T. Marx, « What's New About the 'New Surveillance' ? : Classifying for Change and Continuity. », Surveillance and Society, vol. 1, no. 1, 2002.

G.T. Marx, « Mots et Mondes de Surveillance, Contrôle et Contre-Contrôle à l'Ère Informatique », Criminologie, vol. 39, no. 1, 2006.

H. Nissenbaum, Privacy in Context : Technology, Policy, and the Integrity of Social Life, Stanford University Press, Palo Alto, CA, 2010.

C. Norris and D. Wilson, Surveillance, Crime and Social Control, Aldershot, Ashgate, 2006.

M. Samatras, Surveillance in Greece, Pella Press, Pellas, N.Y., 2004.

J. Waldo and al., Engaging Privacy and Information Technology in a Digital Age : Issues and Insights, National Academies Press, Washington D.C., 2007.

E. Zureik and al. (eds.), Privacy, Surveillance and the Globalization of Personal Information : International Comparisons, McGill-Queen's University Press, Montreal, 2010.