Un rapport sur la société de la surveillance

A l'intention du commissaire à l'information

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

Rapport de synthèse

Septembre 2006

Rédaction :

Kirstie Ball et David Murakami Wood

Matériel de recherche :

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

Introduction

En juin 2006, le Surveillance Studies Network a été chargé par le commissaire à l'information britannique de rédiger un rapport sur la société de la surveillance. Le présent document est une synthèse de ce rapport. Il se divise en trois chapitres qui reprennent les principaux points couverts par le rapport. Le premier d'entre eux illustre dans les grandes lignes le contexte de la société de la surveillance : ses définitions, ses problèmes et ses conséquences. Le deuxième indique le mode d'opération de la société de surveillance. Quant au troisième, il étudie certains des défis réglementaires posés par la société de la surveillance.

1. Société de la surveillance : synthèse, histoire et définitions

Nous vivons au sein d'une société de la surveillance. Inutile de parler de société de la surveillance au futur. Dans tous les pays riches du monde, le quotidien est envahi par la surveillance, pas simplement de l'aube au crépuscule, mais bien 24 heures sur 24 et 7 jours sur 7. Le problème ne réside pas simplement dans le fait que nous soyons filmés plusieurs centaines de fois par jour par des caméras de télévision à circuit fermé (CCTV) en réseaux de surveillance, ou que l'on nous demande notre carte de fidélité en passant à la caisse du supermarché. Il vient du fait que ces dispositifs représentent une infrastructure fondamentale et complexe qui part du principe que la collecte et le traitement des données personnelles sont désormais des activités essentielles à la vie contemporaine.

Certaines formes de surveillance ont toujours existé : on s'observe pour prendre soin les uns des autres, pour se donner une caution morale et découvrir secrètement des informations. Cependant, il y a environ 400 ans, des méthodes « rationnelles » ont commencé d'être appliquées à des pratiques organisationnelles qui ont progressivement éliminé la nécessité de recourir aux réseaux et aux contrôles sociaux informels sur lesquels s'appuyaient au quotidien le commerce et les activités gouvernementales. On a fait en sorte que les relations sociales ordinaires soient jugées désuètes, afin d'empêcher les liens familiaux et les identités personnelles d'entraver le bon déroulement de ces nouvelles organisations, appelées « bureaucraties ». Mais, point positif, les citoyens et, par la suite, les travailleurs, ont pu espérer un plus grand respect de leurs droits, se sentant protégés par des données précises ainsi que par la loi. Les pratiques impersonnelles et centrées sur des règlements se sont multipliées dans le domaine de la surveillance. De nouvelles technologies de l'information ont révolutionné l'administration bureaucratique de l'après-guerre, améliorant ainsi vitesse, niveau de contrôle et coordination. Ce phénomène, associé à une amélioration des techniques d'identification et de localisation mises au point dans les secteurs militaire et du maintien de l'ordre, constitue le principal message de ce rapport. La surveillance se développe dans le contexte de la modernité.

Inconvénients de la société de la surveillance

Comprendre la société de la surveillance en tant que produit de la modernité nous évite de tomber dans les deux pièges suivants : envisager la surveillance comme un malin complot ourdi par une puissance diabolique, et estimer que la surveillance est uniquement le produit des nouvelles technologies (ces deux pièges ne faisant bien sûr qu'un pour les plus paranoïaques d'entre nous). Mais le fait de replacer la surveillance dans son contexte n'implique pas que tout va bien, mais seulement que nous devons être prudents lorsque nous cherchons à identifier les problèmes clés, et vigilants lorsque nous souhaitons les mettre en évidence.

La surveillance est un concept à double face, et il convient d'en reconnaître les bénéfices. Cependant, il est également vrai que tout système à grande échelle s'accompagne toujours de risques et de dangers et, bien évidemment, que le pouvoir corrompt ou tout du moins trouble la vision de ceux qui l'exercent. Les infrastructures technologiques de grande ampleur sont prédisposées à engendrer des problèmes d'une ampleur tout aussi importante. Le fait d'appuyer par inadvertance ou par imprudence sur la mauvaise touche peut facilement faire des ravages. Prenons l'exemple de la publication par AOL, à des fins d'« étude », de vingt millions de données de recherche en ligne effectuées par des gens ordinaires en août 2006. Officiellement dépouillées d'identificateurs, il n'a fallu que quelques instants pour parvenir à rapprocher ces données de recherche des noms des individus qui les avaient formulées.[1]

Il convient également de réfléchir à la corruption et aux visions déformées du pouvoir. Encore une fois, pour pouvoir comprendre le problème, inutile de s'imaginer un tyran en train d'essayer d'accéder aux clés des bases de données de la sécurité sociale ou à des dossiers médicaux. La corruption du pouvoir concerne des dirigeants qui invoquent de bonnes intentions (par exemple gagner la guerre) pour justifier des tactiques inhabituelles ou extraordinaires. Aux Etats-Unis, pendant la Seconde Guerre mondiale, les Américains d'origine japonaise ont été identifiés puis internés à l'aide des données de recensement – pratique normalement illégale. Pour citer un exemple plus récent, de nombreux Américains musulmans se voient refuser le droit de voyager parce que leur nom est inscrit sur des listes d'interdiction aérienne, ou bien font l'objet d'un profilage racial, une pratique condamnée dans d'autres contextes pour son injustice manifeste.[2]

Dans l'univers de la haute technologie et du commerce mondial, les exemples de conséquences involontaires d'actions pourtant bien intentionnées sont très nombreux. Ainsi, pour rester compétitives, les entreprises « connaissent leurs clients », nous explique-t-on, ce qui leur permet de cibler leurs campagnes de publicité et même de localiser leurs usines et leurs magasins au bon endroit. Personne n'irait penser que le responsable d'un magasin qui souhaite n'attirer que les clients les plus solvables affiche en réalité un comportement sournois en recourant aux services d'Experian pour vérifier leur solvabilité. Cela part tout simplement du bon sens, dans l'intérêt d'une meilleure rentabilité. Mais le résultat – la conséquence involontaire – d'une démarche consistant à passer des données au peigne fin pour se forger une clientèle rentable est que certains groupes obtiennent alors un traitement préférentiel basé sur leurs capacités financières, et que d'autres se retrouvent exclus.[3]

Fait plus inquiétant, l'ensemble des processus et pratiques de surveillance actuels témoignent d'un monde dont nous savons qu'il ne nous fait pas vraiment confiance. La surveillance engendre la suspicion.[4] Les employeurs qui équipent leurs stations de travail d'un enregistreur de frappes au clavier ou leurs véhicules de service de systèmes GPS déclarent ne pas faire confiance à leurs employés. L'employé du service des prestations sociales qui recherche les preuves de cumul d'allocations ou interroge les voisins pour savoir si l'assuré fraude, affiche son manque de confiance à l'égard de ce dernier. Et les parents qui utilisent des webcams et des systèmes GPS

---

[1] Voir : Barbaro, A. et Zeller, T. « A face is exposed for AOL searcher no. 4417749 », New York Times, 9 août 2006. http://select.nytimes.com/gst/abstract.html?res=F10612FC345B0C7A8CDDA10894DE404482/

[2] Voir : Amnesty International USA (2004) Threat and Humiliation: Racial Profiling, Domestic Security and Human Rights in the USA, New York : Amnesty International USA, http://www.amnestyusa.org/racial_profiling/report/rp_report.pdf

[3] Lace, S (2005) The Glass Consumer, Bristol, Royaume-Uni : Policy Press ; Danna, A. et Gandy, O. (2002) « All that glitters is not gold: Digging beneath the surface of data-mining » Journal of Business Ethics, 40: 373-386; Lyon, D. (éd.) (2003) Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination, Londres et New York : Routledge.

[4] Question dont il est débattu dans : Lyon, D. (2003) Surveillance after September 11, Cambridge R.-U. : Polity Press, 45-48, 142ff

pour surveiller les activités de leurs enfants avouent en fait qu'ils ne leur font pas confiance non plus. Peut-être êtes-vous d'avis que certains de ces comportements sont de simples mesures de prudence. Mais jusqu'où peut-on aller ? Les relations sociales dépendent de la confiance accordée à autrui, et le fait que nous nous permettions de saper ainsi cette confiance fait penser à un suicide social à petit feu.

Définition de la surveillance ; parcours de la société de la surveillance

La société de la surveillance est une société dont l'organisation et la structure reposent sur l'utilisation de techniques de surveillance. Etre sous surveillance signifie que les données relatives à nos déplacements et activités personnels sont enregistrées par des technologies pour le compte des organisations et des gouvernements qui structurent notre société. Ces informations sont ensuite triées, passées au crible et classées, pour servir de base à des décisions qui affectent nos chances de vie. Ces décisions touchent au droit et l'accès aux prestations sociales, au travail, aux produits, aux services et à la justice pénale ainsi qu'à la santé, au bien-être et à nos mouvements dans les lieux publics et privés. La surveillance quotidienne revêt notamment les formes suivantes :

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

Chaque fois que nos détails personnels font l'objet d'une attention déterminée, routinière,

systématique et ciblée, à des fins de contrôle, de vérification des droits, de gestion, d'influence ou de protection, nous sommes en présence d'un phénomène de surveillance, qui se compose des éléments suivants :

- L'attention est *déterminée* ; celui qui nous observe est à même de justifier sa démarche – nécessité de contrôler, de vérifier un droit, ou quelque objectif publiquement convenu.
- Puis vient la *routine* ; une surveillance a lieu alors même que nous menons nos activités quotidiennes en toute insouciance.
- La surveillance est aussi *systématique* ; elle s'effectue selon un programme rationnel, et pas simplement aléatoire.
- Enfin, elle est *ciblée*. Une grande partie de la surveillance concerne des personnes identifiables, dont les données sont collectées, stockées, transmises, extraites, comparées, exploitées et vendues.

Les détails personnels en question peuvent être de tous types : images collectées par un réseau CCTV, données biométriques (empreintes digitales ou image de l'iris), données relatives à nos communications et à leur contenu, ou, plus communément, données numériques ou catégoriques. Comme un très grand nombre de données font partie de cette dernière catégorie et se rapportent à des transactions, des échanges, des statuts, des comptes et ainsi de suite, Roger Clarke appelle ceci « dataveillance ».[5]
La dataveillance revient à surveiller ou à vérifier les activités ou communications d'individus de manière automatisée à l'aide de technologies de l'information. Son coût est bien inférieur à celui de la surveillance électronique directe ou spécifique, et par conséquent, la dataveillance confère des avantages qui peuvent parfois inciter à un élargissement du système même si les données ainsi récoltées ne sont pas strictement requises pour les raisons prévues à l'origine.

Perspectives relatives à la société de la surveillance 1 : Processus

Dressons maintenant un inventaire des processus et des questions se rapportant à la société de la surveillance telle qu'elle vient d'être décrite. L'objectif est ici de fournir une liste des aspects qu'il importe de prendre en considération lors de tout débat portant sur la société de la surveillance. Il convient de noter que même si ces aspects varient en fonction de l'époque et du lieu, ils sont d'une manière ou d'une autre extrêmement significatifs si l'on souhaite comprendre les grandes lignes de la société de la surveillance.

Le tri social est endémique au sein de la société de la surveillance. L'Etat et le secteur privé analysent et catégorisent d'importantes bases de données personnelles afin de définir les marchés cibles et les populations à risque.[6] Une fois classé, il est difficile de sortir du moule. Depuis les attentats du 11 septembre 2001, il est possible que ce tri ait contribué à augmenter la sécurité des compagnies aériennes (nous ne le saurons jamais), mais il a certainement entraîné un profilage grossier de certains groupes, surtout des musulmans, qui a débouché sur des inconvénients, des privations et parfois même des cas de torture. Le tri social définit de plus en plus la société de la surveillance. Il offre différentes opportunités à différents groupes et revient souvent à organiser nos sociétés de manière subtile et parfois involontaire, sans véritable débat démocratique.

Flux de données: Les données recueillies par les technologies de surveillance circulent entre les

---

[5] Clarke, R. (2006[1997]) « Introduction to dataveillance and information privacy », http://www.anu.edu.au/people/Roger.Clarke/DV/Intro.html#DV

[6] Voir l'étude de référence dans ce domaine : Gandy, O. (1993) The Panoptic Sort: A Political Economy of Personal Information, Boulder CO : Westview Press.

réseaux informatiques. Bon nombre d'entre nous peuvent certes accepter de fournir des informations dans un contexte précis, mais que se passe-t-il si ces données sont transférées ailleurs ? Pour protéger les enfants des abus, ou réduire la fraude dans les services publics, des appels sont souvent lancés en faveur d'une plus grande diversification de l'exploitation des bases de données. Le public et les agences de partage des données ne savent cependant généralement pas grand-chose de la destination finale de ces données. L'idée selon laquelle les interventions politiques découlent de «renseignements intelligents » est désormais bien ancrée et ce phénomène, ainsi que le potentiel de mise en réseau et de comparaison des données offert par les infrastructures numériques actuelles, font que la surveillance semble fonctionner selon une logique qui lui est propre. Cette logique doit être remise en question, examinée et vérifiée, surtout lorsque les données circulent d'un site à un autre.

Un détournement de l'utilisation se produit lorsque les données personnelles collectées et utilisées dans un but unique et pour remplir une seule fonction, sont réutilisées ailleurs, ce qui engendre une surveillance et des invasions de la vie privée accrues au-delà de ce qui avait été compris à l'origine et de ce qui est considéré comme socialement, éthiquement et juridiquement acceptable. Dans le cas des cartes de transport Oyster à Londres, les données récoltées dans le domaine commercial des transports en commun sont de plus en plus utilisées par les services de police dans le cadre de leurs enquêtes.[7] Le détournement de l'utilisation se produit généralement discrètement, la commodité administrative servant de bon prétexte. En effet, étant donné que ces nouvelles technologies permettent un échange de données de plus en plus important et que l'efficacité organisationnelle est fréquemment considérée comme une priorité absolue, les conséquences humaines du détournement de l'utilisation sont trop souvent inconnues, ignorées ou minimisées.

Technologies: la surveillance dépend fondamentalement des technologies, mais il convient de rappeler deux points : premièrement, la « surveillance humaine » directe, sans technologie, existe toujours et est souvent complétée par d'autres méthodes plus technologiques. Deuxièmement, les systèmes technologiques à proprement parler ne sont ni la cause ni la somme de tout ce que représente aujourd'hui la surveillance. Il est impossible de connaître les conséquences qu'imposent les capacités de chaque nouveau système. Pour bien comprendre la société de la surveillance, nous devons comprendre le fonctionnement des technologies, leur mode d'utilisation (il s'agit là d'une démarche interactive à laquelle doivent participer les personnels des entreprises ainsi que les consultants en technologie et les techniciens), et la façon dont elles influencent le mode de fonctionnement de l'organisation. Qui plus est, nous devons suffisamment bien comprendre ces questions pour pouvoir influer sur la politique et les pratiques, comme nous le suggérons ci-dessous dans notre discussion concernant les évaluations de leur impact.

L'autre question soulevée par les technologies est que beaucoup d'entre nous estimons (à tort, comme nous le verrons) qu'il est possible de venir à bout des angoisses suscitées par la société de la surveillance en déployant des moyens techniques. Certes, l'usage de certaines technologies dites de protection de la vie privée (PET), qui permettent de limiter ou de modérer la surveillance, doit être encouragé le cas échéant. Mais ces technologies n'offrent dans le meilleur des cas qu'une solution partielle. Nous faisons bien de nous méfier de toute suggestion visant à apporter une solution purement technique aux soi-disant problèmes techniques. Comme nous allons le voir, la réalité de la société de la surveillance est bien trop complexe pour se limiter à des réponses aussi superficielles.

---

[7] Voir :Oyster data use rises in crime clamp-down » The Guardian, 13 mars 2006, http://politics.guardian.co.uk/foi/story/0,,1730771,00.html

Perspectives sur la société de la surveillance 2 : Problèmes

Vie privée, déontologie, droits de l'Homme: depuis les années 1970, la question de la surveillance suscite une réflexion profonde et un débat portant sur ses aspects juridiques, qui ont conduit à l'introduction de lois en matière de protection des données et de la vie privée en Europe et ailleurs. Les réglementations de ce type s'appuient sur une interprétation spécifique du concept de vie privée. Bien que les « pratiques équitables de traitement de l'information » (FIP – Fair Information Principles)[8] aient évolué, il s'avère difficile de persuader les décideurs politiques de l'importance des dimensions *sociales* de la vie privée,[9] sans même évoquer la nécessité de lutter contre les problèmes associés à la société de la surveillance proprement dits. La société de la surveillance engendre des dilemmes d'ordre déontologique et associés aux droits de l'Homme qui transcendent le domaine de la vie privée. Il est anormal d'attendre du citoyen ordinaire qui fait l'objet d'une surveillance, quel que soit son niveau de connaissances, qu'il puisse se protéger lui-même. Trois questions clés ressortent de cette discussion :

Exclusion sociale, discrimination: L'intensité de la surveillance varie à la fois en fonction du lieu, de la classe sociale, du groupe ethnique et du sexe. La surveillance, l'invasion et la protection de la vie privée varient d'un groupe à un autre, au profit de certains et au détriment d'autres. Le système de santé et de protection sociale du commencement à la fin de notre existence, autrefois fière promesse des gouvernements sociaux-démocrates, en est aujourd'hui réduit à la simple gestion des risques qui demandent une parfaite connaissance de la situation – et c'est à ce niveau qu'intervient la société de la surveillance. Les données personnelles sont donc essentielles pour déterminer l'attribution des ressources.[10]

Choix, pouvoir et autonomisation: Le citoyen ordinaire peut influencer (et influence) les débats, notamment en insistant pour que la réglementation soit respectée, en remettant en cause le système ou en refusant que ses données soient utilisées à des fins pour lesquelles il ne dispose que d'informations partielles ou qui lui semblent suspectes. Mais jusqu'à quel point les citoyens ou les groupes peuvent-ils choisir d'être exposés à cette surveillance et limiter les informations personnelles qui sont collectées et utilisées ? Lorsque le système de surveillance est de nature infrastructurelle, et que son mode de fonctionnement est enveloppé de la mystique technique, il est véritablement très difficile de changer le cours des choses de manière significative. Par exemple, ce n'est que lorsqu'un scandale concernant un vol d'identité éclate que les consommateurs prennent conscience de l'ampleur des opérations de profilage individuel effectuées par les grandes entreprises,[11] et l'encore, le débat a tendance à se concentrer sur les questions de sécurité – comment empêcher d'autres cas de fraude similaires – plutôt que sur la limitation des capacités des sociétés privées et des organismes publics à traiter à grande échelle et sans discernement un si grand nombre de données. En matière de contrôle de l'impact de la surveillance, le citoyen est fortement désavantagé.

Transparence, responsabilité: Les citoyens et les groupes ont du mal à savoir ce que deviennent leurs informations personnelles, qui les manipule, à quel moment et à quelles fins. Pourtant, peu à peu, ces données personnelles sont utilisées pour façonner leurs opportunités futures et orienter leurs choix. Cependant, étant donné le pouvoir dont jouissent les grandes entreprises aux capacités de surveillance sophistiquées, il semblerait juste que les citoyens ordinaires aient le

---

[8] Les « FIP sont l'équivalent nord-américain des « principes de protection des données » européens.

[9] Voir l'excellent rapport traitant de la socialité de la vie privée dans : Regan, P. (1005) Legislating Privacy: Technology, Social Values, and Public Policy, Chapel Hill : University of North Carolina Press.

[10] Ericson, R. et Haggerty, K. (1997) Policing the Risk Society, Toronto : University of Toronto Press.

[11] Voir l'editorial du New York Times « The data-fleecing of America », 21 juin 2005.

droit de s'exprimer, même si ce n'est qu'au niveau du principe. Une telle démarche peut être entreprise non seulement par le biais d'agences spécialisées, mais également par celui des groupes de défense et des médias.

Les organisations doivent assumer leurs responsabilités, en particulier lorsque des opérations de surveillance intense, dont les conséquences sont potentiellement négatives, se déroulent au quotidien. Bien que la surveillance du lieu de travail offre des exemples flagrants de mauvaises pratiques, il est intéressant de noter qu'au moins dans certains cas, les syndicats ont réussi à intervenir énergiquement pour contraindre les employeurs à mettre un frein à leur politique de contrôle abusive. Par ailleurs, d'importants progrès peuvent être accomplis si les employeurs adoptent un processus transparent consistant à expliquer la teneur du contrôle et à obtenir le consentement négocié des employés à cet égard. Cependant, dans le domaine de la surveillance des consommateurs, aucune démarche analogue n'existe, et pourtant la puissance considérable des données détenues par des entités telles que Tesco ou Walmart est pratiquement inégalée. Aujourd'hui, l'émergence de la société de la surveillance demande à ce que nous passions de l'autoprotection de la vie privée à la responsabilisation des manipulateurs de données, celle-ci venant s'ajouter au travail des instances réglementaires officielles chargées d'appliquer les mesures de contrôle et d'encourager la minimisation de la surveillance.

2. Enquête sur la société de la surveillance

Le Surveillance Studies Network a commandité plusieurs rapports d'experts couvrant les thèmes suivants : santé et médecine, consommation, travail et emploi, services publics, citoyenneté, crime et justice, communications, cadre bâti et infrastructure ainsi que frontières. De ces rapports sont ressortis plusieurs thèmes clés qui peuvent être regroupés en quatre domaines : contexte de la société de la surveillance, technologies de la surveillance, modes de fonctionnement et de mise en œuvre de la surveillance, et enfin impacts de la surveillance sur les individus et les différents groupes de la société. Bien évidemment, de nombreux aspects se recoupent d'un domaine à l'autre, et ces considérations ne sont pas exhaustives.

Contexte de la société de la surveillance

Indiquons tout d'abord les grandes lignes de plusieurs tendances fondamentales qui caractérisent les sociétés occidentales et entraînent l'émergence d'une société de la surveillance, à savoir : risque et sécurité, militarisation de la surveillance, économie politique de la surveillance, et enfin, économie croissante des données personnelles.

Risque et sécurité: Notre société est obsédée par le risque. Les techniques de gestion du risque applicables aux menaces externes et internes constituent désormais un élément clé des activités organisationnelles. Il en résulte une approche *préemptive* par opposition à une démarche *préventive* du risque.[12] Point significatif, l'utilisation de l'exploitation des données et du profilage visant l'identification du risque oriente les pratiques de la surveillance de plus en plus vers l'examen des actions et des transactions de la population en général.[13] Cet examen permet alors de cibler des interventions destinées à des individus ou des groupes d'individus considérés comme vulnérables ou posant un risque à autrui. La collecte et l'analyse de l'information, y compris des données relatives aux individus identifiables, sont primordiales. Ces pratiques

[12] Ewald, F. (2002) « The return of Descartes' malicious demon: an outline of a philosophy of precaution », dans Baker, T. et Simon, J. (éd.), Embracing Risk: The Changing Culture of Insurance and Responsibility, Chicago : University of Chicago Press.

[13] Valverde, M. et Mopas, M. (2004) « Insecurity and the Dream of Targeted Governance », dans Larner, W. et Walters, W. (éd.) Global Governmentality: Governing International Spaces, Londres : Routledge.

peuvent en effet apporter des bénéfices personnels et sociaux, mais, par ailleurs, la conception de la sécurité a des implications importantes au niveau de la liberté, de la vie privée et d'autres valeurs sociales, ainsi que de l'innovation et du changement.

Plusieurs exemples permettent d'illustrer cette tendance à l'évaluation du risque et à la préemption:

- L'épidémiologie et la modélisation dans le secteur de la surveillance médicale,[14] qui permettent d'identifier les cas individuels, d'enregistrer les occurrences à des fins d'analyse statistique et de faire ressortir des catégories de la population vulnérables à des maladies particulières
- L'évaluation des risques auxquels sont exposés des individus, des familles et des quartiers en matière de protection de l'enfant, de santé mentale et de justice pénale
- La catégorisation du risque que posent les voyageurs à la sécurité nationale, en recourant à des listes nominatives des passagers et à l'analyse des transactions financières
- L'estimation de la valeur relative des consommateurs individuels et de leurs profils géodémographiques.

Militarisation de la surveillance: La surveillance militaire est l'un des rares phénomènes dont on puisse dire qu'il est déjà réellement mondial, à une époque où tout est censé être en voie de mondialisation. Notre planète est encerclée d'une multitude de satellites de surveillance militaire et les systèmes de communication transnationaux sont totalement infiltrés par ceux de la surveillance militaire. Le GPS (Système de positionnement mondial) et Internet étant deux exemples contemporains de technologies conçues avec des capacités militaires intégrées, il est possible de faire remonter toute l'histoire de la surveillance moderne à ses premiers balbutiements, les systèmes C3I (Command Communications, Control and Intelligence) de la Seconde Guerre mondiale et de la Guerre froide, dont l'objectif était de faire de la planète un lieu entièrement défendable et sûre.[15] Cette interaction se manifeste non seulement au niveau du gouvernement et des composants technologiques, mais également dans la façon toujours plus militaire d'évoquer la sécurité au quotidien : les Etats et les médias parlent de l' «evaluation de la menace », de la « lutte contre la drogue » de « lutte contre la criminalité » et même de la « guerre contre le terrorisme », de la fermeté de la loi, de « tolérance zéro », et ainsi de suite. La « guerre de l'information » est sortie de la pénombre des opérations militaires secrètes pour être mise bien en évidence en plein cœur du monde des affaires, où l'espionnage d'entreprise et la pénétration des ordinateurs font rage et où les spécialistes de la sécurité sont rebaptisés « guerriers de la connaissance ». De nombreuses sociétés spécialisées dans les technologies de surveillance sont intimement liées au secteur militaire et, pourtant, elles vendent également leurs produits aux usagers civils. Par exemple, TRW, un important partenaire de la société américaine chargée des contrats de défense, est devenu l'un des chefs de file de la biométrie civile ; la société française Sagem fabrique des produits allant des téléphones mobiles à des algorithmes de surveillance, en passant par des systèmes de reconnaissance aérienne automatisés.

Economie politique de la surveillance: Ces nouvelles entreprises, avec les sociétés de sécurité traditionnelles et les gros fournisseurs militaires, font partie de ce que l'on pourrait globalement appeler l'« industrie de la sécurité ». D'autres secteurs industriels jouent également un rôle clé

[14] Concernant la montée en puissance de l'économie de la santé, un domaine qui applique des techniques et résultats de l'épidémiologie à l'évaluation des technologies médicales, voir par exemple : Ashmore, M., Mulkay, M.J. et Pinch, T.J. (1989) Health and Efficiency: A Sociology of Health Economics, Buckingham : Open University Press.

[15] de Landa, M. (1991) War in the Age of Intelligent Machines, Cambridge MA : MIT Press; Edwards, P. (1997) Computers and the Politics of Discourse in Cold War America, Cambridge MA : MIT Press.

dans la croissance du secteur de la surveillance, notamment ceux des télécommunications et de l'informatique, ainsi que de la banque et de l'assurance. L'industrie de la sécurité s'est considérablement développée ces dernières années. D'après l'indice des 100 entreprises répertoriées par le cabinet de conseil américain Security Stock Watch,[16] la croissance de l'industrie dans son ensemble a régulièrement surpassé l'indice du Dow Jones et les valeurs de haute technologie du NASDAQ.[17] Ainsi, à la fin de l'exercice financier 2005-6, l'indice avait plus que doublé en trois ans, avec une capitalisation boursière pour les 100 entreprises composant l'indice estimée à plus de 400 milliards de dollars US.

Economies de l'information personnelle: Les Etats et les organisations ne sont pas les seuls à mener une surveillance – les gens ordinaires se livrent également à cette activité. Après les attentats de 2005 à Londres, les chaînes de télévision et la police ont encouragé les gens à photographier avec leur téléphone portable les individus au comportement suspect. Par ailleurs, un nombre croissant d'individus, surtout des enfants et des jeunes, affichent leur vie en public, et observent à leur tour la vie d'autres individus, au moyen de Webcams en ligne[18] et de sites de réseaux sociaux tels que MySpace et Bebo. En outre, les individus disposant d'un accès accru aux ressources de la connaissance commencent à l'heure actuelle à gérer les « doubles informationnels » qui se trouvent par exemple dans les bases de données d'agences d'évaluation du crédit telles qu'Experian ou Equifax. Ces agences donnent aux individus un accès en ligne à leurs dossiers de crédits, leur permettant ainsi de contester ou de corriger des données trompeuses. Cette ouverture volontaire des entreprises mêlée à l'auto-éducation des individus ne peut toutefois être considérée comme un mode de régulation, même s'il est envisageable qu'une nouvelle génération de jeunes puissent se transformer en citoyens habitués à surveiller, à faire l'objet de surveillance ou à prendre des mesures à l'égard de celle-ci.

Technologies de la surveillance

Bien qu'il soit primordial de ne pas perdre de vue l'importance de la surveillance non technologique (par exemple écoutes de conversation, espionnage et surveillance impliquant une appréciation humaine directe), ce chapitre est consacré aux technologies de la surveillance. Nous nous concentrerons tout d'abord sur des avancées réalisées dans quatre domaines (qui se recouvrent partiellement) : les télécommunications, la vidéosurveillance, les bases de données, la biométrie et les technologies du positionnement, du suivi et du repérage. Nous réfléchirons ensuite aux relations qu'entretiennent les différentes technologies et la tendance qu'ont les technologies de la surveillance à disparaître et à se propager tout à la fois. Nous conclurons en envisageant les limites du développement technologique.

Développement technologique: Il est indéniable que les nouvelles technologies contribuent à modifier la nature de la surveillance. Ces dispositifs technologiques ne comprennent pas de composantes intrinsèques « bonnes » ou « mauvaises ». Des bases de données nationales efficaces peuvent aussi bien servir à fournir des soins de santé ciblés qu'à persécuter des opposants politiques. Mais tout ne dépend pas simplement de la façon dont l'on s'en sert. Toutes les technologies sont développées par des organisations particulières aux objectifs et intérêts qui leur sont propres. Nous examinerons plusieurs de ces technologies particulières et leurs capacités.

---

[16] Cet indice comprend les industries des secteurs suivants : « biodéfense », « sécurité environnementale », « prévention de la fraude », « défense militaire », « sécurité des réseaux de télécommunications » et « sécurité physique » (obstacles physiques, vidéosurveillance, etc.).

[17] SecurityStockWatch.com 100 Index, août 2006, http://www.securitystockwatch.com/

[18] Koskela, H. (2004) « Webcams, TV Shows and Mobile phones: Empowering Exhibitionism », Surveillance & Society, CCTV Special (éd. Norris, McCahill et Wood), 2(2/3): 199-215, http://www.surveillance-and-society.org/cctv.htm

Télécommunications: la surveillance dans le domaine des télécommunications concerne la capacité d'individus, d'organisations ou de personnes morales à contrôler, trier et stocker des renseignements sur l'occurrence et le contenu des échanges, à la fois entre plusieurs appareils technologiques, et entre des appareils technologiques et des individus. Depuis que l'Etat se livre à des « écoutes téléphoniques », le développement technologique a abouti sur des technologies plus diversifiées applicables aux télécommunications, ainsi qu'à une capacité de surveillance accrue. Par exemple, l'emplacement d'un appareil portable peut être identifié en procédant à un simple traitement croisé (triangulation) du signal de l'appareil et de sa réception par plusieurs relais différents au fur et à mesure que les signaux « se déplacent » d'un émetteur à un autre – cette information peut être stockée en vue d'une exploitation de données ultérieure. Le système ECHELON, le réseau de surveillance global de la NSA (American National Security Agency), possède un vaste centre à Menwith Hill, dans le comté anglais du North Yorkshire : ce centre filtre automatiquement et régulièrement l'ensemble du trafic de télécommunications du Royaume-Uni à la recherche de mots ou expressions clés, et fait de plus en plus souvent appel à des algorithmes de reconnaissance verbale et sémantique toujours plus sophistiqués.[19]

Vidéosurveillance: La surveillance photographique existe depuis la fin du XIXème siècle. Conséquence d'une forte propagation des réseaux CCTV à partir du début des années 1990, dans le but d'enrayer le déclin des centres commerciaux urbains et d'apaiser les craintes face au terrorisme et à la criminalité, on estime désormais à près de 4,2 millions le nombre de caméras CCTV en Grande-Bretagne, soit une pour 14 habitants,[20] et chaque personne peut être filmée par plus de 300 caméras par jour.[21] Pendant les années 1990, le ministère de l'intérieur (Home Office) a consacré à l'installation de télévisions en circuit fermé 78 % du budget[22] alloué à la prévention de la criminalité, et, d'après certaines estimations, 500 millions de livres sterling de fonds publics ont été investies dans cette infrastructure au cours des dix dernières années.[23] Cependant, une étude réalisée par le Home Office est a conclu que « les programmes de CCTV évalués n'ont eu qu'un effet global marginal sur les taux de criminalité ».[24] La numérisation s'est traduite par une utilisation accrue des systèmes de CCTV automatisés, essentiellement le long des routes. Ainsi, les plaques minéralogiques des véhicules permettent d'identifier leurs propriétaires officiels. Les contrôles par caméra de l'application des limites de vitesse sont passés d'un peu plus de 300 000 en 1996 à plus de deux millions en 2004, et quelque 113 millions de livres sterling d'amendes sont recueillies chaque année.[25] Cette surveillance étatique accrue a mauvaise presse,[26] et ce, bien que les caméras de surveillance de la vitesse, à la différence des caméras CCTV installées dans les rues, contribuent réellement à diminuer le nombre des accidents de la route graves ou

---

[19] Campbell, D. (1999) Development of Surveillance Technology and Risk of Abuse of Economic Information (An appraisal of technologies of political control) Volume 2/5: Interception Capabilities 2000, Luxembourg : Parlement européen, Direction générale de la recherche, Direction A, Programme STOA ; Wood, D (2001) The Hidden Geography of Transnational Surveillance, thèse de doctorat non publiée, université de Newcastle (Royaume-Uni).

[20] McCahill, M. et Norris, C. (2003), « Estimating the extent, sophistication and legality of CCTV in London », dans M. Gill (ed.) CCTV, Perpetuity Press

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

[22] *ibid.*: 54

[23] Norris, C. (2006) « Closed Circuit Television: a review of its development and its implications for privacy », rapport élaboré pour la réunion trimestrielle du comité consultatif du Department of Homeland Security Data Privacy and Integrity Advisory Committee quartely meeting (ministère de la sécurité intérieure, de la confidentialité des données et de l'intégrité), 7 juin, San Francisco CA

[24] Gill, M. et Spriggs, A. (2005). Assessing the impact of CCTV. Londres, Home Office Research, Development and Statistics Directorate, 43, 60-61

[25] Wilkins, G. et Additcott, C. (1998) Motoring Offences England and Wales 1996, Home Office Statistical Bulletin, Londres : ministère de l'intérieur ; Ransford, F., Perry, D. Murray, L. (2005) Motoring Offences and Breath Test Statistics: England and Wales 2003, Home Office Statistical Bulletin, Londres : ministère de l'intérieur

[26] McCahill et Norris, 2003 op cit. n.44

mortels.[27] Le centre national de données ANPR (Reconnaissance automatique des plaques minéralogiques) envisage de faire passer ses capacités actuelles de 35 millions de lectures par jour à 50 millions d'ici 2008.

Bases de données: Des données multiples peuvent désormais être recueillies, tabulées et référencées avec une plus grande précision et bien plus rapidement qu'avec les anciens dossiers sur papier qui caractérisaient autrefois la bureaucratie moderne. La surveillance par bases de données peut être appelée « dataveillance ». Les bases de données associées à d'autres systèmes de surveillance permettent également une surveillance algorithmique, qui consiste à utiliser des logiciels pour travailler sur les images ou les données capturées et les comparer à celles qui figurent dans la base de données. Cet aspect a joué un rôle essentiel dans le développement de la biométrie. La dataveillance se retrouve de plus en plus dans les secteurs du marketing, de la médecine, du maintien de l'ordre et du contrôle des frontières.

Par exemple, dans le domaine du *marketing*, alors que baissait le coût des bases des données, de nombreuses entreprises du secteur privé ont souhaité recueillir autant de données que possible sur leurs clients et mieux cibler leurs méthodes de marketing. Les données transactionnelles (utilisation des cartes de crédit, des appels sur téléphones portables, etc.) que l'on peut lier directement à une personne sont associées à des données supplémentaires de sources diverses : les programmes de cartes de fidélité, les enquêtes de consommation, les groupes de discussion, les concours promotionnels, les demandes d'informations de produits, les contacts avec les centres d'appels, les « cookies » informatiques, les forums permettant aux consommateurs de donner leur avis et les transactions de crédit. A ces données *internes* et souvent propriétaires se superposent fréquemment des données *externes* provenant de sources publiques (par exemple, les statistiques nationales), d'organisations à but non lucratif ou de sociétés spécialisées dans la collecte de données. Ces données sont dans la plupart des cas reliées à des codes postaux, et certaines rues « profilées » reçoivent les appellations comme « retraités prudents », « secteur des crèches peu développé » ou « bonne aptitude à faire face aux crises ».[28] Aux simples techniques de mise en correspondance et de profilage géodémographique viennent désormais s'ajouter des processus (d'apprentissage) « heuristiques » plus sophistiqués destinés à l'exploitation des données, telles que la «Knowledge Discovery in Databases» (KDD), une méthodologie de création de nouveaux savoirs à partir de bases de données. Cette technique contribue à l'identification de relations jusque là *inconnues ou cachées* au sein des jeux d'informations.[29] Le « produit » de ces systèmes est surtout le plus évident dans les systèmes de personnalisation Web, tels que ceux qu'utilise la société Amazon.com, qui recourt à une multiplicité de sources de données pour prédire les préférences probables de ses clients.[30]

---

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

[28] La première de ces catégories provient du système de classification d'ACORN mis au point par une société connue sous le nom de CACI, et les deux autres sont des classifications MOSAIC créées par Experian. Pour tout renseignement complémentaire sur ces produits, consulter http://www.caci.co.uk/acorn/ and http://www.business-strategies.co.uk/Content.asp?ArticleID=629 Voir également : Burrows, R. et Gane, N. (à paraître) « Geodemographics, software and class. » Sociology

[29] Pour en savoir davantage sur les différences entre KDD et l'exploitation de données, voir Tavani, H.T. (1999) « KDD, data mining, and the challenge for normative privacy ». Ethics and Information Technology 1: 265-273. De nombreuses sources envisagent l'exploitation de données comme représentant le processus global consistant à travailler sur des données en vue de réaliser les objectifs décrits dans le présent rapport. Voir Rygielski, C., Wang, J-C et Yen, D.C. (2002) « Data mining techniques for Customer Relationship Management ». Technology in Society 24: 483-502, Danna et Gandy (2002) op cit. n.6. Dans l'intérêt d'une plus grande clarté, le terme KDD désigne ici le processus technique faisant ressortir des affinités particulières (évidentes ou non) parmi des séries de données, et l'exploitation de données, la démarche consistant à accumuler des données critiques en vue de les analyser ultérieurement

[30] Fink, J. et Kosba, A. (2000) « A review and analysis of commercial user modeling servers for personalization on the World Wide Web ». User Modeling and User-Adapted Interaction 10: 209-249

Biométrie: La quasi-totalité des nouveaux systèmes d'identité a recours à la biométrie : images numériques des empreintes digitales, de l'iris, de la topographie faciale et du contour de la main font partie intégrante des différents systèmes de passeports et de cartes d'identité. L'attrait de la biométrie réside dans le fait qu'elle semble « ancrer » l'identité au corps humain, auquel des données et des informations peuvent être attachées. L'identificateur biométrique devient alors la passerelle d'accès aux données détenues. Cette technique consiste à faire converger l'exploitation des données et l'intégration de l'information avec les identificateurs biométriques. L'idée est le taux de précision n'en sera que meilleur et que la fraude diminuera. Les codes et mots de passe peuvent s'oublier ou se perdre, mais le corps offre un lien direct et constant entre les archives et la personne. La « guerre contre le terrorisme » a engendré une hausse considérable du financement de la recherche dédiée à la mise en œuvre de la biométrie. Suite aux attentats du 11 septembre 2001 aux Etats-Unis, les techniques de biométrie déjà utilisées à des fins commerciales ou sur le point d'être lancées ont connu un développement accéléré et elles ont été jugées comme la solution par excellence pour remporter ce nouveau type de guerre.[31] Le US Patriot Act (loi américaine sur le patriotisme), a mis en œuvre, dans un cadre dont les implications dépassent largement le territoire américain, une série de pratiques destinées aux applications biométriques qui permettait leur utilisation quasi-illimitée au titre des procédures d'enquêtes et d'identification de l'activité terroriste. Au Royaume-Uni, l'expansion progressive des réseaux de surveillance avec télévision en circuit fermé évoquée ci-dessus a donné lieu à des études plus poussées sur les possibilités de déploiement de réseaux CCTV biométriques et de la reconnaissance des visages, suite aux premières expériences menées à Newham, à Birmingham et dans d'autres villes.

Positionnement, suivi et repérage: Les pratiques en matière de surveillance sont de plus en plus référencées, organisées et localisées au moyen de systèmes d'information géographique (GIS).[32] Nombre de ces systèmes effectuent le suivi des mouvements géographiques d'individus, de véhicules ou de marchandises à l'aide de puces RFID (radio-identification), de systèmes de positionnement mondial (GPS), de cartes d'identité intelligentes, de transpondeurs ou de signaux radio émis par les téléphones ou les ordinateurs portables. Par exemple, dans le cadre de *l'application des lois*, en 2004/5 quelque 631 adultes et 5 751 adolescents, certains à peine âgés de 12 ans, ont été munis de bracelets électroniques qui leur permettent d'attendre leur procès chez eux plutôt qu'en détention provisoire.[33] Les delinquants libérés font de plus en plus souvent l'objet d'une surveillance électronique, en échange d'une sortie de prison anticipée dans le cadre du programme avec couvre-feu et détention à domicile (Home Detention Curfew Scheme),[34] ou d'une libération conditionnelle.[35] Dans le domaine de *la gestion des frontières* aux Etats-Unis, des cartes RFID à puce frontalières intelligentes font actuellement l'objet d'essais à la frontière américano-mexicaine. L'industrie de la RFID souhaite attirer l'attention sur le potentiel que représente cette technologie en insistant sur les possibilités de suivi ou de repérage des travailleurs migrants qui traversent la frontière pour une période limitée. Après les animaux, c'est au tour des êtres humains de se faire implanter une puce RFID. Aux Etats-Unis, 70 personnes atteintes de maladies cérébrales dégénératives se sont ainsi vu implanter une puce pour pouvoir

---

[31] Amoore, L. (2006) « Biometric borders: governing mobilities in the war on terror », Political Geography 25: 2: 336-351; Gates, K. (2005) « Biometrics and post-9/11 technostalgia », Social Text 23(2): 35-53. Irma Van der Ploeg, « Biometrics and the body as information », dans Lyon, D. (éd.) (2003) op cit. n.3

[32] Institute for the Future (2004) Infrastructure for the New Geography, Menlo Park, CA : IFTF

[33] NPS (National Probation Service) (2006) Electronic Monitoring 6
http://www.probation.homeoffice.gov.uk/output/Page137.asp#Current%20Programmes

[34] Le programme HDC permet aux personnes condamnées entre 3 mois à quatre ans de prison d'être libérées avec une anticipation variant entre 2 semaines et quatre mois et demi sous réserve d'un couvre-feu assuré par une surveillance électronique. En 2004/5, 19 096 personnes ont été libérées plus tôt dans le cadre de ce programme (ibid.: 6)

[35] NPS op cit

être plus facilement localisées,[36] de même que deux employés d'une société soucieuse de veiller au contrôle de l'accès au *lieu de travail*.[37] Des developpements permanents dans le domaine de l'application des données géographiques en temps réel aux profils des consommateurs ne manqueront pas de conférer une couche de données supplémentaire pour aider les entreprises à cibler des consommateurs particuliers lors de leurs campagnes de marketing. Il s'agit donc de technologies dont les fonctions ont de très fortes chances d'être « détournées ».

Synergie technologique et détournement de l'usage: Si les capacités des technologies et systèmes individuels sont importantes, on constate également une hausse de la synergie technologique, ou convergence des technologies de surveillance. Il s'agit là d'une tendance à long terme des systèmes informatiques qui est aussi motivée par le désir de créer des économies d'échelle. Un nombre croissant de systèmes sont conçus dans une optique d'interopérabilité. Cela signifie également que de nouveaux produits peuvent naître de technologies plus anciennes, qui avaient au départ été comprises et gérées par des organismes de réglementation, et qui convergent les unes vers les autres pour engendrer une fonction totalement imprévue et déréglementée. Par exemple:

- Systèmes d'identification à usages multiples – passage des frontières, lutte contre la fraude, accès aux informations gouvernementales voir même commerciales (locations de vidéos) et semi-commerciales (bibliothèques). Alors que des agendas tels que la « guerre contre le terrorisme », la limitation des flux de migration de groupes indésirables et même la recherche de solutions pour combattre la fraude par carte de crédit, façonnent l'évolution des systèmes d'identification, les valeurs « impersonnelles » de la bureaucratie dans le sens classique du terme semblent fragilisées.
- A Londres, le système de reconnaissance ANPR, au départ créé à des fins militaires pour contribuer à l'identification des terroristes de l'IRA, joue aujourd'hui un rôle dans la gestion de la circulation, la génération de recettes pour les autorités locales et la sécurité face à une nouvelle génération de terroristes.

Vers une surveillance omniprésente: Les technologies ne sont jamais aussi importantes que lorsqu'elles sont omniprésentes, acceptées de tous et en grande partie invisibles. L'informatique omniprésente (Ubicomp), également connue sous le nom d'« intelligence ambiante » (Ambient Intelligence – AmI), instaure les conditions nécessaires à la mise en place d'une surveillance omniprésente en se fondant simultanément dans l'environnement physique et virtuel.[38] Les services et domaines électroniques sont relativement faciles à contrôler comparé aux rues de nos villes, mais de nombreux points de passage urbains associent désormais étroitement des éléments électroniques et physiques. La conjugaison de technologies à base de CCTV, de biométrie, de bases de données et de suivi peut être considérée comme s'inscrivant dans le cadre d'une exploration bien plus étendue – souvent financée avec le soutien des Etats-Unis et du Royaume-Uni au titre de la « guerre contre le terrorisme » – de l'utilisation de systèmes « intelligents » interconnectés servant à suivre les mouvements et comportements dans le temps et dans l'espace de millions de citoyens. Pour employer un terme propre à l'industrie, il s'agit là d'un suivi spatiotemporel multi-échelle.[39]

---

[36] La société en question est la Verichip Corporation. http://www.verichipcorp.com/

[37] Waters, R. (2006) « US group implants electronic tags in workers », Financial Times, 12 février. http://www.ft.com/cms/s/ec414700-9bf4-11da-8baa-0000779e2340.html

[38] Kang, R. et Cuff, D. (2005) « Pervasive Computing: Embedding the Public Sphere », Washington and Lee Law Review 62(1): 93-146. Cuff, D. (2002) Immanent domain: Pervasive computing and the public realm, Journal of Architectural Education, 57: 43-49

[39] Hampapur, A. et al. (2005), « Smart video surveillance », IEEE Signal Processing Magazine, mars : 38-51

Limites de la technologie: Bien évidemment, les technologies ne tiennent jamais entièrement leurs promesses. Les ambitions technologiques du programme biométrique USVISIT, par exemple, ont été revues à la baisse pour des raisons logistiques, la lecture des empreintes digitales ayant remplacé l'identification par lecture de l'iris initialement envisagée. Sont également jugées préoccupantes les questions liées à la fiabilité,[40] au défaut des caractéristiques (FTE, pour « Failure to Enrol », qui signifie que les données biométriques ne peuvent être saisies) et aux fausses reconnaissances (la lecture ne correspond plus aux données biométriques de l'individu). Malgré cela, des décisions de mise en œuvre majeures sont souvent prises avant la réalisation d'essais complets. Par exemple, en ce qui concerne le système d'identification que le Royaume-Uni se propose de mettre en place, il est estimé qu'une personne sur six ne pourra peut-être pas se servir de sa carte d'identité à cause de problèmes de type FTE.[41] Des problèmes propres à des technologies utilisées dans le domaine de l'application de la loi, telles que la reconnaissance des visages et le système ANPR, ont aussi été identifiés.

Verrouillage technologique et décalage réglementaire: Les technologies de surveillance sont souvent qualifiées de « réponse » indéniable à de multiples menaces, et, récemment, à la menace du terrorisme. Cependant, plus nous dépendons des technologies de la surveillance, plus il se produit, d'une part, un « verrouillage technologique » qui empêche la prise en compte d'autres options, et, d'autre part, un écart de compréhension qui accroît notre dépendance à l'égard d'une expertise non soumise au contrôle démocratique. Les organismes de réglementation sont constamment en retard par rapport aux innovations technologiques et incapables de comprendre « leur fonctionnement ». Dans cette course effrénée, il convient de se demander si les autorités disposent des outils nécessaires pour mettre en place une réglementation significative des pratiques de surveillance complexes. Une question que l'on retrouve souvent dans le contexte du développement technologique est de savoir s'il est possible de forcer « le génie à rentrer dans sa bouteille ». Or les titulaires de brevets et les fournisseurs tendent à ne pas se prononcer sur la réversibilité des dispositifs et des systèmes.

Les processus de surveillance

L'importance de l'évaluation préventive des risques, et la prescription de la surveillance comme solution à toutes sortes de problèmes, ont donné naissance à divers processus et phénomènes uniques. Le tri social, les conséquences imprévues, le partage des informations et le flou entre le public et le privé en sont quatre exemples.

Tri social, catégorisation et ciblage. Le tri social, le classement de la population en différentes catégories de risque, droit ou valeur, se retrouve dans de nombreux domaines:

- Les consommateurs fournissent continuellement leurs données de transaction aux entreprises et font partie d'une boucle de réaction évolutive qui relie les comportements de consommation à la collecte de données et à la génération de profils.[42] Les centres d'appel classent maintenant les comptes client en fonction de leurs dépenses relatives, et adaptent leur niveau de service en conséquence. De même, l'industrie des télécoms enregistre des données de trafic pour identifier les meilleures voies de pénétration du marché (par exemple, le marketing par SMS).
- Les employés des centres d'appel sont évalués vis à vis de facteurs sociaux et de style de

[40] Voir : Zureik, E. with Hindle, K. (2004) « Governance, security and technology: the case of biometrics » Studies in Political Economy, 73: 113-137

[41] Voir : Grayling, A.C. (2005) In Freedom's Name: The Case Against Identity Cards, Londres : Liberty

[42] Détaillé dans : Elmer, G. (2004). Profiling Machines: Mapping the Personal Information Economy. Cambridge, MA: The MIT Press

vie qui correspondent à ceux du segment de marché pour lequel ils travaillent.

- Ainsi, à de nombreux points d'entrée sur terre, mer et air, il est maintenant courant de voir des voies « express » pour accélérer le passage, comme le système « Privium » de l'aéroport de Schiphol aux Pays-Bas, qui utilise un balayage de l'iris pour remplacer des longues files d'attente pour le contrôle des passeports.

Contrôle involontaire: Il ne faut pas confondre la surveillance et le contrôle social direct.[43] L'intention de la surveillance se résume souvent à gérer des flux efficaces et rapides de produits, de gens et d'informations.[44] Cependant, ce qu'une personne appellera « efficacité », signifiera « contrôle social » pour une autre, et ceci est particulièrement vrai pour les systèmes fortement personnalisés comme la récupération de registres d'identification, qui exploite des identificateurs cohérents et uniques pour chaque citoyen.[45]

Partage des informations: Pour permettre le tri social, les données doivent être précises et facilement disponibles. Dans de nombreux pays, y compris la Grande-Bretagne, on observe une tendance vers des services publics plus intégrés et « décloisonnés », souvent facilitée par un partenariat et un travail d'équipe impliquant plusieurs organismes. Il arrive de plus en plus que divers contrats d'association locaux rassemblent une variété d'organismes et de professions permettant de mieux cibler leurs compétences sur la fourniture plus intégrée de services aux individus.[46] L'une des conséquences de cet important développement est que les frontières qui étaient jadis considérées comme procurant certaines protections, même fragiles, de la vie privée ainsi que les limites de la surveillance sont maintenant remises en question, ce qui déroute souvent le public et les fournisseurs de service qui se demandent comment les informations personnelles sont, et devraient être gérées.[47] C'est notamment le cas dans le domaine des services publics, de l'application de la loi, de la gestion des frontières et du marketing. Ainsi, plus de 50% de la population britannique possède une carte de fidélité Nectar, administrée par Loyalty Management UK ; 216 sociétés de catalogue au Royaume-Uni font partie du consortium de partage des données Abacus, qui gère des données recueillies sur 26 millions de consommateurs individuels et valorisées par le « Lifestyle Universe » de Claritas. Ces données couvrent le revenu, le mode de vie ainsi que des informations de stade de vie à un niveau individuel pour chacun de ces clients.[48]

Le flou entre les frontières public/privé: les frontières entre les intérêts du secteur public et privé commencent à s'estomper du fait que, les secteurs public et privé se partageant les données, un nombre croissant tâches gouvernementales sont accomplies par la combinaison parfois complexe

---

[43] Lianos, M. (2001) Le Nouveau Contrôle Social: toile institutionnelle, normativité et lien social. Paris : L'Harmattan Logiques Sociales

[44] Graham, S. et Wood, D. (2003) « Digitising surveillance: categorisation, space and inequality, » Critical Social Policy, 23: 227-248

[45] Pour l'avis critique d'un informaticien, voir : Clarke, R. (2006) « National identity cards? Bust the myth of 'security über alles'! », http://www.anu.edu.au/people/Roger.Clarke/DV/NatID-BC-0602.html

[46] 6, P., Raab, C. et Bellamy, C. (2005) « Joined-up government and privacy in the United Kingdom: Managing tensions between data protection and social policy, Part I ». Public Administration 83 (1): 111-133; Bellamy, C., 6, P., and Raab, C. (2005) « Joined-up government and privacy in the United Kingdom: Managing tensions between data protection and social policy, Part II ». Public Administration 83 (2): 393-415

[47] Un récent document de consultation du Home Office, réclame des pouvoirs supplémentaires contre le crime organisé et financier, et déplore que le « partage des données avec d'autres parties du secteur public est très inégal, alors que les tentatives de partage entre le public et le privé sont extrêmement rares ».Il demande une amélioration de ces flux d'information, avec notamment – vis à vis des rapports sur les activités douteuses – la mise en correspondance des données entre la nouvelle agence SOCA (Serious Organised Crime Agency, agence contre le grand banditisme) et la base de données d'une quantité d'organismes gouvernementaux, y compris le service des douanes et du revenu du gouvernement britannique, l'agence des permis et immatriculations des véhicules(DVLA - Driver and Vehicle Licensing Agency), la DWP, et le service des passeports. Il existe maintenant de nouvelles initiatives dont notamment le nouveau Comité ministériel sur le partage des données, MISC 31, qui s'est vu confier la « mise au point d'une stratégie gouvernementale sur le partage des données dans l'ensemble du secteur public »

[48] Evans, M. (2005) « The data-informed marketing model and its social responsibility. » dans Lace, S (2005) op cit., n.3

des mécanismes des secteurs public, privé, bénévole et commercial. Il arrive de plus en plus que divers contrats d'association locaux rassemblent une variété d'organismes et de professions permettant de mieux cibler leurs compétences sur la fourniture plus intégrée de services aux individus.[49] Quand des informations d'Etat sont disponibles pour usage privé, comme certains l'ont suggéré avec le Registre national de l'identité, il convient de s'interroger sur les limites au consentement des gens en tant que citoyens et en tant que consommateurs, et sur la place de ces frontières. Des questions continueront à se poser avec la privatisation des télécommunications, la gestion des frontières (projet Semaphore d'IBM, le programme e-borders du Royaume-Uni (frontières électroniques) et la sécurité locale (comme les Citizen Corps aux Etats-Unis qui « guettent des activités inhabituelles »).

Les conséquences sociales de la surveillance

Nous allons à présent nous intéresser plus ouvertement aux conséquences sociales des technologies et processus de surveillance que nous venons d'aborder. Les critiques de la surveillance se bornent souvent aux termes du respect de la vie privée et, bien que ceci représente indéniablement un aspect essentiel, nous souhaitons l'aborder comme l'un des éléments de l'autonomie individuelle. Nous aimerions également souligner les effets rarement discutés du choix et du consentement, et plus important encore, ceux des processus de tri, catégorisation et ciblage sur les chances de vie des individus et des groupes ou communautés entières, leur mobilité relative et l'accès aux opportunités.

Autonomie : anonymat et confidentialité: La surveillance affecte l'autonomie dans le sens qu'elle compromet l'anonymat individuel et la confidentialité. A bien des égards, une condition générale d'anonymat donne à l'individu la possibilité d'établir sa propre identité par ses actions et ses relations. L'une des premières victimes de la surveillance omniprésente, et en particulier des systèmes d'identification, est l'anonymat qui permettait aux gens d'échapper aux intenses règles de surveillance humaine des petites communautés. La confidentialité des personnes vulnérables ou marginalisées est en régression constante. Dans les prisons britanniques, tous les détenus sont soumis à une surveillance pratiquement permanente. En outre, même quand ils sortent de prison, ils sont de plus en plus assujettis à une surveillance électronique, soit comme condition d'une mise en liberté anticipée dans le cadre du programme de détention à domicile et couvre-feu (Home Detention Curfew Scheme),[50] soit comme condition d'une libération provisoire.[51] La capacité des employeurs à fouiner dans les vies privées de leurs employés doit être examinée sans relâche. La couverture de multiples bases de données par les systèmes d'identification nationaux, en particulier ceux qui portent sur les secteurs public et privé, est un sujet de préoccupation clé. De même, fin 2002, la BBC signalait que des organismes d'application de la loi avaient émis plus de 400,000 demandes de données de trafic auprès des opérateurs de réseau mobile.[52] Comme indiqué par l'ACLU dans leur étude sur un nouveau réseau de surveillance, les entreprises et les citoyens sont « enrôlés de force dans la construction d'une société de surveillance ».[53]

Choix et consentement: Le choix a joué un rôle crucial dans les débats sur la surveillance et la protection des données en Amérique du Nord. Cependant, au Royaume-Uni, son profil est resté

---

[49] 6 et al. 2005 op cit. n.24; Bellamy et al., 2005 op cit. n.46

[50] Le programme HDC permet aux personnes condamnées entre 3 mois à quatre ans de prison d'être libérées avec une anticipation variant entre 2 semaines et quatre mois et demi sous réserve d'un couvre-feu assuré par une surveillance électronique. En 2004/5, 19 096 personnes ont été libérées plus tôt dans le cadre de ce programme. Voir : NPS (2006) op cit. n. 82

[51] ibid.

[52] « Phone firms « flooded » by crime checks ». BBC News, 20 décembre 2002, http://news.bbc.co.uk/1/low/uk/2592707.stm

[53] Stanley, J. (2004) The Surveillance-Industrial Complex, Washington DC: ACLU. http://www.aclu.org/FilesPDFs/surveillance_report.pdf

quelque peu discret par rapport aux autres moyens de protection. Quelqu'un peut-il choisir d'être surveillé ou pas tout en continuant à mener une vie normale ? Comment est-il encore possible d'affirmer que nous avons accepté la surveillance ? La question du choix est évidente dans tout le système de justice pénale. Nous ne choisissons pas d'être surveillé par CCTV quand nous passons par des espaces publics et personne n'a consenti à l'enregistrement des déplacements de son véhicule par le système ANPR de l'ACPO. Les inculpés ne choisissent pas, et ne sont pas contraints, à donner des empreintes ou des échantillons d'ADN qui seront conservés indéfiniment dans la base de données nationale de la police, même s'ils sont libérés sans inculpation. Et, bien qu'une personne ne puisse pas être forcée à donner un échantillon d'urine pour le dépistage de drogues, elle n'a pas vraiment le choix étant donné qu'un refus pourrait entraîner une amende, une peine d'emprisonnement ou les deux. Il est pratiquement impossible pour une personne de savoir comment les informations sont utilisées et comment elles peuvent insidieusement affecter sa vie, en augmentant par exemple les chances d'avoir son véhicule arrêté par la police, ou d'avoir à payer à l'avance pour des biens ou des services. Une solution possible serait de rendre les interactions de surveillance étatique avec les citoyens non obligatoires quand c'est possible, ce qui a été proposé dans le cas des cartes d'identité en Grande-Bretagne. Cependant, cette réponse est en grande partie illusoire car une fois rendue nécessaire pour un éventail d'accès à des services, elle deviendra obligatoire de fait. De plus, les identificateurs existants correspondent à des rôles uniques, comme les chauffeurs, les consommateurs ou les touristes alors que le système de carte d'identité donne au gouvernement le pouvoir de surveiller les activités de tout un ensemble de rôles qui comprennent non seulement ces derniers mais aussi celui de citoyen.

Discrimination : vitesse, accès et exclusion sociale: La discrimination, sous la forme de différentiation dans la vitesse, la facilité d'accès et divers degrés d'exclusion sociale est une conséquence majeure des processus de tri engendrés par la surveillance. La logique gouvernementale a changé. Alors que les interprétations plus anciennes de la citoyenneté du vingtième siècle insistaient sur *l'inclusion* de toutes les personnes recevables dans les systèmes de santé, aide sociale et protection juridique, les pratiques de citoyenneté plus récentes, y compris les systèmes d'identification, semblent mettre l'accent sur *l'exclusion* des éléments indésirables.[54] Ceux qui ont accès aux ressources sont extrêmement mobiles – hommes d'affaires internationaux, touristes etc – et leurs systèmes d'identification (des cartes de crédit aux cartes de grands voyageurs) ont tendance à accélérer leur facilité de déplacement. Mais pour les autres qui travaillent (ou pire, au chômage), comme les immigrés, les réfugiés ou les demandeurs d'asile, sans parler de ceux dont les noms sont distinctement « musulmans » ou « arabes », ces systèmes ont tendance à gêner leurs déplacements, que ce soit à l'intérieur du pays ou delà des frontières.

La surveillance intensifiée de la vie urbaine implique aussi des processus puissants d'exclusion sociale, qui se caractérisent par la création de déconnexions pour les personnes et endroits considérés d'une certaine manière comme non rentables ou risqués. Ainsi, les nouvelles technologies de surveillance peuvent résolument *ralentir* la vie de certaines personnes, et la rendre plus, et non pas moins, difficile du point de vue logistique. Mais une fois introduits, l'accès et le blocage sont de plus en plus surveillés automatiquement,[55] entrant ainsi un danger de verrouillage technologique qui diviserait plus franchement les sociétés contemporaines en classes haute vitesse, haute mobilité et connectées et basse vitesse, basse mobilité et déconnectées. L'exclusion se retrouve aussi dans les structures de tarif pour les produits. Amazon.com étant déjà connu pour changer le prix de ses DVD en fonction du client, on peut se demander si une

[54] Bigo, D. (2004) « Globalized in-security: the field of the professionals of unease management and the ban-opticon, » Traces, 4

[55] Lianos, M. (2001) op cit . n.109; Lianos, M. (2003) « Social control after Foucault, » Surveillance & Society 1(3): 412-430. http://www.surveillance-and-society.org/articles1(3)/AfterFoucault.pdf

intervention réglementaire ne serait pas nécessaire pour empêcher une fixation des prix au niveau commercial de masse. Et bien qu'il soit difficile de tirer des conclusions sur la surveillance et l'exclusion sociale au travail, principalement en raison des facteurs déterminants structurels, sociaux et professionnels préexistants des marchés du travail, un domaine commence à stratifier les opportunités d'emploi : le recrutement électronique. Faire le tri dans d'importants volumes de CV et rechercher des candidats possibles soulève la question de la discrimination de deux façons. D'abord parce que le recrutement électronique est sujet à la partialité et à des procédés empiriques qui se manifestent par les termes choisis par les professionnels dans les recherches par mot clé, [56] [57] et ensuite parce que certains groupes sociaux, économiques et ethniques n'ont pas facilement accès à Internet.

Ceci peut s'enfoncer profondément dans l'infrastructure même de la société. Le discernement humain étant éliminé et remplacé par du code et l'identité culturelle et nationale étant devenue une dimension tellement contestée de la vie, avec son lourd bagage de chances d'épanouissement, de choix, de souvenirs et d'espoirs, il est ironique de constater que des efforts parallèles sont déployés pour réduire ce discernement à des formules et des algorithmes exploitables par une machine afin de faciliter la bureaucratie, la surveillance et l'administration intégrée.

Démocratie, responsabilisation et transparence: De nombreuses questions se posent : quelles sont les limites de l'examen public ? Comment réglementer la frontière entre les bases de données commerciales et la sécurité du public et de l'Etat ? Comment responsabiliser les entreprises privées vis à vis des erreurs et des fausses réponses positives (« hits ») dans leurs systèmes de base de données ? Ainsi, les citoyens qui se retrouvent sur la liste de surveillance d'une « frontière intelligente » ont actuellement un accès extrêmement limité. Alors que de nombreux organismes et autorités peuvent accéder au système ou placer des informations sur le système, il est plus difficile d'effacer ou de corriger les données. Enfin, des questions importantes se posent sur la responsabilisation des gouvernements élus vis à vis de leurs citoyens et sur la nature « extraterritoriale » de nombreux entrepreneurs privés pour leurs systèmes de surveillance actuels. Dans la pratique, les banques de données commerciales comme les transactions de carte de crédit ou les relevés de téléphone portable qui sont détenus par des corporations multinationales peuvent être « extraterritoriales » et hors de portée directe d'une juridiction politique. Les exemples récents de multinationales extradant des informations vont créer des problèmes particuliers pour l'examen et la réglementation publics, notamment quand une entreprise détient les données commerciales *et* possède un contrat pour les fonctions de surveillance.

Sous la législation de nombreux pays, les citoyens ont le droit de savoir quelles informations sont détenues à leur propos, et comment elles sont utilisées, bien qu'il y ait des exceptions à la règle. Ce droit exige qu'un « contrôleur de données » fournisse à chaque individu des informations sur toutes les données qu'il détient sur lui ainsi que les détails de tous les traitements auxquels elles ont été soumises. Ceci permet de corriger l'asymétrie du pouvoir du « belvédère » de la surveillance, en particulier quand le consentement d'utiliser nos données personnelles était implicite, au lieu d'être accordé de façon positive. Cependant, de nombreuses personnes ne connaissent pas leurs droits, ne les exercent pas et reçoivent très peu d'assistance pour le faire.

La dataveillance intensive s'inscrit de plus en plus dans les caractéristiques normales de l'Etat moderne, et peut, en elle-même, être justifiable – et justifiée par ceux qui la défendent – dans l'intérêt du public. Ces activités peuvent souvent être explicitement autorisées par le parlement.

---

[56] Tversky, A. et Kahneman, D (1974) « Judgement under uncertainty: heuristics and biases, » Science 185(4157) : 1124-1131

[57] Mohamed, A.A., Orife, J. and Wibowo, K. (2002) « The legality of key word search as a personnel selection tool, » Employee Relations 24(5)

Ce qui les rend problématiques est leur manipulation de grandes quantités de données personnelles par des voies qui peuvent dépasser le repère établi par les principes et les lois de protection des données (à nouveau le parlement), et par d'autres contraintes et directives sur la façon dont les informations doivent être recueillies, triées et communiquées. Nous nous habituons peut-être sans nous en rendre compte à être surveillés, et au suivi et aussi à l'anticipation de nos activités et de nos mouvements, tout ceci (en particulier dans les services publics) sans la possibilité d'accepter ou refuser, ou de comprendre vraiment ce qui arrive à nos données. Nous pouvons très bien considérer comme « raisonnables » des limitations de la confidentialité que nous refuserions autrement si nous réfléchissions à ce que signifie vraiment d'être citoyen. Il n'est pas du tout certain que la situation politique va en définitive permettre aux droits à la vie privée de s'opposer fermement aux revendications des organisations gouvernementales présentées dans « l'intérêt du public », même si l'intérêt du public semble clair et plus important. Si la surveillance est sensée être « proportionnelle », beaucoup dépend de la façon dont ce terme est interprété, et sur qui l'interprète. Beaucoup dépend aussi des mesures de protection qui accompagnent les nouveaux développements intrusifs.

4. Réglementation de la société de surveillance

La surveillance a besoin d'être réglementée. Par « réglementée », nous n'entendons pas seulement les dispositifs légaux pour contrôler les systèmes et les pratiques, mais aussi toutes les techniques qui ont un effet régulateur,[58] c'est-à-dire qui appliquent des règles à la surveillance et au traitement des données en fixant des limites et des contrôles. La plupart des systèmes de contrôle du traitement des données personnelles ont été mis au point dans le contexte de la protection des données, avec l'objectif de protéger la *confidentialité*. Nos remarques dans cette section portent principalement sur ces stratégies. Mais réglementer la *surveillance* peut être aussi autre chose. On pourrait argumenter que la protection contre la surveillance doit être établie pour elle-même, car ses effets indésirables sont ceux qui touchent à la violation de la vie privée et de plus, la première ligne de défense, bien que non négligeable, est vulnérable. Dans cette section du Rapport, nous examinons l'historique de la réglementation et évaluons la pertinence de ces efforts. Nous suggérons également des possibilités d'amélioration.

Qu'est-ce qui ne va pas dans la Réglementation?

La réglementation de la vie privée et de la surveillance a souffert d'inconvénients courants. Nous sommes en mesure d'identifier au moins six domaines de difficulté:

- La réglementation a été plutôt réactive : une réponse a été faite au développement technologique, à la mise en œuvre et à la pratique, après coup.
- La réglementation s'est essentiellement focalisée sur la technique et la gestion, en fonction de codes de pratique, du respect de prescriptions juridiques standard et de l'application de technologies protégeant la confidentialité, laissant peu de place à l'anticipation.
- La plupart des règlements reposent sur une conception étroite de la vie privée personnelle et de sa valeur pour les individus, ce qui représente (forcément) la réflexion actuelle des décideurs qui ont souvent une vue restreinte de ce qui est dans l'intérêt du public.
- La réglementation a été largement discutée et mise en œuvre sans consulter le public. Le débat s'est tenu dans les communautés expertes, comme pour le mode de protection des

[58] Baldwin, R. et Cave, M. (1999) Understanding Regulation: Theory, Strategy and Practice. Oxford : Oxford University Press

données ou l'application de la loi. Ceci s'est traduit par une participation minimale des gens ordinaires à des enjeux qui font pourtant partie des plus importants de notre époque.
- La réglementation est souvent considérée, en termes politiques, comme un fardeau injustement placé sur les affaires ainsi que sur l'Etat, et qui inhibe les initiatives, la prise de risque et la productivité. En Grande-Bretagne, on a pu observer une tentative marquée de déréglementation ou de « meilleure réglementation » visant à alléger la charge. La reconnaissance que les entreprises et le gouvernement peuvent bénéficier de la confiance du public et des gains en efficacité que pourrait apporter la réglementation est très inégale dans la pratique, mais plus évidente en rhétorique.
- La discussion des médias se consacre essentiellement aux « histoires d'horreur » sur les incidents de violation de la vie privée et représente aussi des vues utopiques et orwelliennes des technologies de surveillance. Les histoires dignes d'être publiées dans les nouvelles sont importantes, mais il arrive trop souvent que les enjeux éthiques et sociaux complexes encadrant la surveillance soient tout simplement ignorés. Quand la surveillance est discutée, c'est bien souvent en termes de cause à effet (« la CCTV empêchera les activités criminelles ») ou de peur (« nous serons tous contrôlés »). De même, d'autres vues sont contrées par l'argument fallacieux et dangereux selon lequel « si vous n'avez rien à cacher, vous n'avez rien à craindre ».

L'état actuel de la réglementation

Lors des trente-cinq dernières années au moins, la protection de la vie privée s'est étendue au monde entier. Cette évolution s'est appuyée sur certains principes totémiques selon lesquels une organisation:

- doit être *responsable* de toutes les informations personnelles en sa possession;
- doit *identifier les finalités* du traitement des informations quand elles sont rassemblées ou avant;
- ne peut pas recueillir d'informations personnelles à l'insu et sans le *consentement* de l'individu (sauf cas spéciaux);
- doit *limiter la collecte* des informations personnelles à celles qui sont nécessaires à la poursuite des finalités identifiées;
- ne doit pas utiliser ou divulguer des informations personnelles à des fins autres que celles identifiées, sauf avec le consentement de l'individu (le principe de *finalité*);
- doit seulement *conserver* les informations aussi longtemps que nécessaire;
- doit s'assurer que les informations personnelles restent *exactes, complètes et à jour*;
- doit protéger les informations personnelles en utilisant les *mécanismes de sécurité* appropriés;
- doit être *ouverte* à propos de ses politiques et pratiques et ne pas utiliser de système d'information secret;
- doit permettre aux sujets des données *l'accès* à leurs informations personnelles, avec la possibilité de les modifier si elles sont inexactes, incomplètes ou obsolètes.[59]

Animé de cet ensemble de « principes de gestion équitable de l'information » (Fair Information Principles ou FIP) ou de principes similaires, le monde réglementaire régissant la violation de la vie privée et la surveillance a été alimenté par des lois générales couvrant certains secteurs (par exemple, les télécommunications) ou pratiques (par exemple, la comparaison des données), ainsi que par des documents et déclarations internationales au niveau mondial et régional. Le plus

[59] Bennett, C. et Raab, C. (2006) The Governance of Privacy: Policy Instruments in Global Perspective, Cambridge MA: MIT Press, 12

connu est peut-être la Directive européenne 95/46/EC sur la protection des données, qui se retrouve aussi dans la Directive sur la vie privée et la communication électronique (2002/58/EC). Des autorités de réglementation, comme les commissaires à l'information, ont été établies aux niveaux national, infranational et même régional. De plus, les sociétés privées, les associations professionnelles et les pouvoirs publics ont formulé leurs propres codes de pratiques et protocoles, et les commerçants en ligne ont adopté leurs propres déclarations ou politiques de confidentialité. Des pénalités et sanctions ont été appliquées aux transgresseurs sous les diverses formes de la réglementation juridique. Ces dernières années, des solutions technologiques – technologies d'amélioration de la confidentialité, ou PET (Privacy Enhancing Technologies) – ont rejoint la cause de la réduction de la collecte, de l'assurance de l'anonymat et aussi de la limitation du potentiel de la surveillance de la technologie elle-même. Les défenseurs de la confidentialité ont été prolixes et actifs pour prévenir des dangers, dénoncer les pratiques et sensibiliser le public à la façon dont la surveillance et la violation de la vie privée peuvent affecter leur vie. Les médias ont souvent répondu aux menaces de la surveillance, même quand les médias eux-mêmes trouvent un intérêt à violer la vie privée des célébrités mais aussi des citoyens « ordinaires ».

Pour beaucoup, établir un système pratique de contrôle de la surveillance sur les bases fragiles de la protection de la confidentialité des informations semble malavisé. Cependant, pour d'autres,[60] la vie privée et sa protection peuvent être étendues pour couvrir d'autres situations, physiquement intrusives, qui donnent lieu à une asymétrie entre l'individu et les surveillants, comme dans la surveillance vidéo. Les nouvelles pratiques de surveillance entraînent cependant des discriminations et d'autres conséquences sociales fâcheuses par des voies qui ont des effets puissants et injustes sur les chances de la vie au-delà du domaine des violations de la vie privée elles-mêmes, qui touchent principalement les individus. On peut donc soutenir que les régimes de réglementation pour la surveillance et la confidentialité doivent être réexaminés et tout au moins modifiés pour être en mesure d'affecter la conception, la mise en œuvre et les effets des nouvelles technologies de surveillance, plus intensives et extensives. Mais la nouvelle surveillance ne se limite pas seulement aux technologies. On peut argumenter que le « problème » pour les régimes de réglementation ne se résume pas à la façon de maîtriser les technologies, mais porte aussi sur le moyen d'influencer les politiques et les finalités de ceux qui les développent et les déploient, et d'influencer les sociétés et les populations qui y sont soumises.

Instruments de réglementation: le pour et le contre

Le répertoire existant des instruments de politique qui ont été mis au service de la protection des données et de la confidentialité, et qui par conséquent s'appliquent aussi à d'importants domaines de surveillance, est détaillé ci-dessous:[61]

Instruments internationaux: La Convention européenne des droits de l'Homme, ainsi que d'autres déclarations internationales, confèrent une force légale et morale à la protection de la vie privée qui pourrait jouer un rôle significatif dans la maîtrise des excès de la surveillance. Avec des documents connexes, cette convention a institué une activité législative et de mise en œuvre spécifique dans un grand nombre de pays et juridictions secondaires. Les interventions au niveau international sont depuis longtemps largement responsables de la prééminence de l'ensemble de principes qui ont régi la protection des données, et par extension, la surveillance.

Lois: La diffusion globale de la législation pour contrôler le traitement des informations

[60] Par ex. : Dubbeld, L. (2004) The Regulation of the Observing Gaze: Privacy Implications of Camera Surveillance. Enschede: Ipskamp Printpartners

[61] Pour une typologie et une discussion plus détaillées, voir op cit. n. 59: chs. 4-7

personnelles s'est rapidement poursuivie des années 70 à nos jours. De nombreux pays ont adopté des lois sectorielles et générales pour la protection des données, et la plupart ont établi des formes d'application et de moyens de contrôle spécifiques. Ces moyens, sous la forme de commissaires à la protection de la vie privée, sont essentiels à l'effort complet de protection de la confidentialité. Les Etats-Unis restent en-dehors du « club » des pays possédant une législation exhaustive de ce type, ce qui gêne les efforts globaux de réglementation de la surveillance, qui reste fragmentée et au coup par coup. La faiblesse de nombreuses lois et de leur mécanisme d'application dans le domaine du traitement des informations personnelles est depuis longtemps un sujet de plainte. Les solutions juridiques qui pourraient légitimer la surveillance au lieu de la réglementer peuvent expliquer l'impatience des critiques.[62] De plus, les lois sur la protection de la vie privée et des données ne réglementent pas facilement un large éventail de pratiques de surveillance, comme celles qui font partie intrinsèque des télécommunications modernes, et ne peuvent pas être simplement et clairement interprétées pour le faire. En outre, le tort que la surveillance est susceptible de causer aux individus, groupes et sociétés dans leur ensemble ne fait pas partie de l'ensemble des impacts que ces lois individuelles fondées sur les droits sont censées remédier ou prévenir.

Auto-réglementation: Divers codes de conduite ou de pratiques ont été développés par des industries ou des sociétés, des organismes spécialisés et des Etats pour réglementer la surveillance dans de nombreux domaines d'activité. Il existe aussi des moyens d'auto-réglementation en ligne par les commerçants travaillant sur Internet, sous la forme de déclarations de confidentialité en ligne, soutenues par des organisations qui s'en portent garant. L'auto-réglementation est parfois écrite dans les lois, comme les codes de pratique dans la loi britannique sur la protection des données de 1998 (Data Protection Act 1998) et la Directive européenne sur la protection des données de 1995 (95/46/EC). L'auto-réglementation est de plus en plus considérée comme une meilleure façon de réglementer, qu'il est jugé préférable d'encourager étant donné « l'imperfection » des lois et le climat commercial moins réglementé.[63] Il est cependant difficile d'imaginer l'existence des codes et autres sans l'existence préalable et parallèle des lois ou instruments internationaux à l'origine des normes et directives traduites dans ces codes.

Technologies d'amélioration de la confidentialité: Depuis le début des années 90, la réalisation du fait que les technologies elles-mêmes peuvent fournir des contrôles puissants sur la surveillance ou la violation de la vie privée représente un important développement. Ainsi, les potentiels de surveillance ou de non-surveillance de technologies spécifiques dépendent de la façon dont elles sont conçues et déployées. Le cryptage des données personnelles quand elles sont stockées ou circulent entre les domaines et au-delà d'autres frontières, peut aller du non existant au très robuste, et la conception du réseau ainsi que le « code » logiciel peuvent avoir un effet réglementaire profond.[64] Le cryptage, l'exploration anonyme du web, les dispositifs de filtrage, les agents intelligents, les outils de préférence de confidentialité, et ainsi de suite, peuvent jouer le rôle d'instruments qui habilitent les individus. Il reste à savoir si, seules, ces solutions aux pratiques de surveillance en ligne sont suffisamment robustes.

Initiative personnelle: Il s'agit d'une autre grande catégorie de réglementation. Ici, l'individu contrôle sa propre divulgation des renseignements, soit par le biais de PET, soit en acceptant ou en refusant certaines procédures de traitement de l'information, soit encore grâce à ses

---

[62] Flaherty, D. (1989) Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States. Chapel Hill NC : University of North Carolina Press

[63] US Department of Commerce, National Telecommunications and Information Administration (NTIA) (1997) Privacy and Self Regulation in the Information Age. Washington DC : Department of Commerce, NTIA

[64] Lessig, L. (1999) Code and Other Laws of Cyberspace. New York NY: Basic Books.

connaissances, sa sensibilisation et sa vigilance vis à vis des pratiques de surveillance et des menaces de confidentialité. Tout ceci donne grand cas à l'intérêt porté par l'individu à la protection et au « capital culturel » – la capacité et les moyens de comprendre ce qui se passe, et de faire valoir ses droits lui-même pour contrôler les incursions ou demander réparation une fois ces menaces matérialisées. Aux Etats-Unis, en l'absence d'organismes de réglementation ou de surveillance, l'initiative personnelle, y compris la poursuite d'actions en justice, représente le principal moyen de réglementer la vie privée et les critiques de cette approche font légion. D'autres systèmes de protection des données reposent dans une certaine mesure sur le fait que les individus déposent des plaintes auprès des organismes de réglementation et font office d'informateurs de première ligne sur les pratiques douteuses.

Nous aimerions aussi souligner l'importance des activités des groupes suivants:

- les groupes de pression pour la confidentialité et contre la surveillance, qui, avec le soutien de certains secteurs des médias, sensibilisent le public aux enjeux et dangers, surveillent les situations et exercent une pression sur les gouvernements et les entreprises qui font appel à la surveillance ;
- les technologues, qui conçoivent les systèmes de surveillance et d'information, et dont l'éducation, la formation et le respect des codes de pratique peuvent affecter la sensibilisation de leurs employés et influencer les produits ;
- les chercheurs, dont le travail peut mettre au jour ce qui se passe, expliquer pourquoi, et mettre au point et tester des théories sur la place et la légitimité de la surveillance dans les sociétés du passé, du présent et du futur ; tout ceci permettant de développer des connaissances utiles pour alimenter le débat public.

Problèmes généraux concernant les Instruments

Trois des plus importants problèmes concernant les méthodes de réglementation existantes ont trait à la *fragmentation* et à la *faible coordination*. L'un des problèmes porte sur les *instruments* principaux ; l'autre concerne la multiplicité de *niveaux* juridiques auxquels la réglementation est censée s'appliquer. Dans les deux cas, la difficulté provient du fait que la surveillance risque de présenter à la réglementation un défi plus unifié et plus global, vu la persistance probable des tendances. Dans les deux cas, la question est de savoir comment on peut améliorer les choses. Autrement dit, peut-on lutter contre l'incendie avec le feu ? Si les forces visant à étendre la surveillance sont de plus en plus intégrées et « unifiées », que ce soit dans un pays donné ou au niveau international, dans quelle mesure les instruments et les niveaux des activités de protection compensatoires sont-ils intégrés ? Le troisième problème est celui de l'application de ces instruments aux effets sociaux de la surveillance – et peut-être en particulier de la « nouvelle surveillance » – au-delà la violation de la vie privée ou de la conception de nouveaux outils. Pour les trois, il y a matière à repenser la panoplie de la réglementation pour voir comment elle pourrait devenir plus cohérente et efficace. Il serait également intéressant de considérer les possibilités d'application d'une évaluation de l'impact de la confidentialité et de la surveillance à tous les niveaux et dans tous domaines ou secteurs d'application. Une fois de plus, on ne peut qu'aborder ce problème ici.

Options pour la réglementation future

Evaluation des facteurs relatifs à la vie privée: Nous pensons qu'il peut être extrêmement intéressant d'adopter l'approche de l'évaluation des facteurs relatifs à la vie privée (EFPV) dans

les méthodes de réglementation des juridictions à tous les niveaux pertinents.[65] On peut décrire une EFPV comme un instrument utilisable par ceux qui proposent des systèmes nouveaux ou modifiés de traitement de données pour limiter les effets des facteurs relatifs à la vie privée potentiellement néfastes sur les sujets des données. Une EPFV peut aider à montrer comment la protection de la confidentialité peut être accommodée dans un programme de partage des informations comme une exigence éthique et légale essentielle qui pourrait contribuer à des objectifs sociaux et politiques importants, comme une meilleure fonction publique ou une sécurité améliorée, davantage orientée vers les citoyens, au lieu de les gêner.

De l'Evaluation des facteurs relatifs à la vie privée à l'Evaluation des impacts de la surveillance: Pour inclure les effets potentiellement néfastes de la surveillance dans un cadre plus général que celui de la protection de la confidentialité, nous suggérons la nécessité de pousser plus loin la configuration des outils EFPV actuels, et de développer ce que l'on pourrait appeler une *Evaluation des impacts de la surveillance* (ou EIS). Ceci donne évidemment lieu à une modification de la signification, car si l'EPFV évalue les impacts du *traitement de l'information sur la vie privée*, l'EIS évalue quant à elle les impacts de la *surveillance sur un ensemble de valeurs*, ce qui pourrait inclure, mais aussi dépasser, la vie privée elle-même.

Comme l'EPFV a été innovée comme un outil permettant d'examiner *la vie privée*, appréhendée en termes de droits individuels, elle n'est pour le moment pas la plus apte à couvrir les ramifications supplémentaires de la surveillance en termes d'un ensemble d'autres impacts sociaux et personnels. Le faire nécessiterait un changement de paradigme pour ne plus seulement tenir compte de l'effet sur les *individus*, comme la politique de confidentialité a tendance à le faire, mais aussi considérer la valeur de la protection de la vie privée et de la limitation de la surveillance en termes *sociétaux*.[66] La vie privée n'est pas seulement une valeur individuelle, elle joue également un rôle important pour la société en tant que fondation pour l'intérêt général et pour des valeurs communes comme la démocratie, la confiance, la sociabilité et une société libre et équitable. Comme la valeur de la vie privée dépasse les individus, nous avons tous un intérêt dans le droit, et la capacité, de tout individu à la protection de sa vie privée. C'est une valeur collective dans le sens qu'il s'agit d'un intérêt commun qui ne peut pas être divisé, qu'aucun individu ne peut être exclu de sa protection et qu'elle ne peut être efficacement fournie par le marché.[67] C'est pourquoi l'EIS pourrait jouer un rôle important en incorporant l'EPFV mais en la complétant avec un ensemble de demandes de renseignements visant à évaluer l'impact de la surveillance ou de la violation de la vie privée sur la société elle-même et sur les autres intérêts de nature non privée de différents individus, catégories et groupes.

Les questions soulevées dans une EIS peuvent notamment comprendre:[68]

- La technique entraîne-t-elle un préjudice physique ou psychologique ?
- La technique franchit-elle une frontière personnelle sans permission (qu'elle mette en jeu une coercition, une tromperie ou une frontière corporelle, relationnelle ou spatiale) ?
- La technique viole-t-elle des hypothèses faites sur la façon dont les informations personnelles vont être traitées, comme les enregistrements non secrets ?

---

[65] Stewart, B. (1999) « Privacy impact assessment: towards a better informed process for evaluating privacy issues arising from new technologies, » Privacy Law & Policy Reporter 5 (8): 147-149 ; une discussion descriptive de l'EPFV est donnée dans Raab, C., 6, P., Birch, A. et Copping, M. (2004) Information Sharing for Children at Risk: Impacts on Privacy. Edinburgh : Scottish Executive

[66] Regan (1995) op cit. n.9, ch. 8

[67] ibid

[68] Gary T. Marx, « Ethics for a the New Surveillance », The Information Society, 14, 3, 1998: 174

Autres options: Si l'EIS prend appui sur l'EPFV, d'autres options prennent également appui sur le présent.

- Etablir une masse de ressources de connaissances et de sensibilisation à la technologie pour aider les organismes de réglementation à suivre les progrès de la technologie
- Conseiller les managers et les technologues sur la façon de concevoir et implémenter des techniques de surveillance de façon responsable, en portant une attention particulière à la stratégie, au changement organisationnel, à la formation du personnel et à la responsabilité sociale
- Reconceptualiser la confidentialité comme une valeur sociale collective et non pas une valeur individuelle
- Encourager un débat public sur la surveillance de manière participative et non condescendante
- Mener des évaluations indépendantes des coûts de la confidentialité, de la réglementation de la surveillance et de la conformité à la réglementation. Estimer s'ils sont excessifs, et s'ils inhibent l'innovation. Examiner si ceci équilibre les avantages de la confiance du public et de l'efficacité, en sachant que le test « d'équilibre » est loin d'être approprié et devrait être lui-même remis en cause.
- Monter le ton des média au-delà des clichés, du sensationnalisme et de l'alarmisme

Il faut enfin mentionner la façon dont la réglementation gagnerait à être améliorée en considérant l'adéquation des relations et de l'interdépendance des tâches : entre les systèmes de réglementation à différents niveaux jusqu'au niveau global, et entre les différents types de participants, y compris les organismes de réglementation et les groupes de société civile. Il reste à discuter dans quelle mesure, par exemple, les relations coopératives qui ont été indiquées dans la Directive européenne 95/46/EC ont non seulement rempli un rôle d'application et de conformité, mais de collecte de renseignements et de sensibilisation aux enjeux dans le cadre plus large des pratiques et des technologies de surveillance. Pour un autre exemple, dans quelle mesure existe-t-il une relation mutuellement productive entre les organismes de réglementation et les groupes de société civile qui assistent ces organismes quand ces groupes attirent leur attention sur des questions et des informations ou connaissances utiles, et font office de mouche du coche quand les réglementations semblent hésiter ou quand le gouvernement et les pratiques commerciales semblent étendre la surveillance. Qu'il y ait matière à d'autres innovations sur les rôles indépendants dans le système de réglementation, hormis les organismes de réglementation engagés et les défenseurs invétérés de l'anti-surveillance, est une autre question à discuter en dehors de ce rapport, qui permet peut-être de montrer un type d'illustration.