Surveillance totale ou servitude volontaire ?

< Hélène Jeannin >

Département de sociologie et d'économie, Orange Labs
140 avenue de la République, Châtillon 92320, France
helene.jeannin@orange.com

DOI:10.3166/RIN.4.491-508

< RÉSUMÉ >

L'accroissement des capacités technologiques contribue à une collecte massive et de plus en plus systématisée de données en capacité de parler des individus, y compris dans ce qu'ils ont de plus intime. Dans un premier temps, nous identifions la multiplicité des sources qui constituent autant d'instruments de surveillance potentielle. Puis nous élargissons la réflexion à la manière dont les pratiques sociales s'en emparent, portées par des acteurs privés, des pouvoirs publics ou des individus. Le rôle significatif de ces derniers en tant qu'artisans de leur propre surveillance, amène à s'interroger sur la notion de servitude volontaire.

< ABSTRACT >

The increase in technological capacities contributes towards a massive and much more systematized data collection, able to speak about individuals, including their innermost thoughts and privacy. First, we identify the multiplicity of sources as key instruments of surveillance. Then we extend our thinking to the way social practices deal with them, whatever their origin: private actors, public authorities, or individuals. The meaningful role of the latter as builders of their own surveillance makes us question the notion of voluntary servitude.

< MOTS-CLÉS >

Surveillance, dataveillance, contrôle, servitude volontaire.

< KEYWORDS >

Surveillance, dataveillance, control, voluntary servitude.

1. Introduction

La société de surveillance évoque une menace omniprésente, à la fois proche et lointaine (Berthoud, 2002), invisible ou visible, panoplie d'un attirail sécuritaire sans cesse perfectionné (Forest, 2009), dans lequel réseaux et bases de données occupent une place de plus en plus prépondérante.

Or, nos actions de la vie quotidienne : achats au supermarché, retraits de carte bancaire, déplacements, … sont de plus en plus enregistrées et converties en données. C'est d'après l'utilisation de ces bases de données à des fins de surveillance qu'a été forgé le terme de « dataveillance » (Clarke, 1988). Nous dresserons ici certains de ses contours.

La concentration de données dans de gigantesques bases fait débat : techniquement, la vulnérabilité de tels systèmes est décriée. Surtout, face à l'asymétrie de pouvoir qu'engendrent de tels agrégats et aux nouveaux types de gouvernements par les chiffres qu'elle induit (Marzouki, 2010), les appréhensions concernant le risque de fichage, la centralisation excessive, la rétention d'information, la manipulation indétectable suscitent beaucoup de remous. Si certaines des technologies de l'information et de la communication offrent des possibilités de mise en relation jusque-là inégalées, elles suscitent aussi nombre de controverses quant à leurs potentielles utilisations. Se dirigerait-on vers un excès de surveillance ? L'accroissement des capacités de contrôle représente-t-il l'opportunité d'un surcroît de sécurité ? Nous appréhenderons ces problématiques par le point de vue des acteurs dans un deuxième temps, avant de questionner la notion de servitude volontaire.

2. Les multiples facettes de la dataveillance

La surveillance se caractérise par : la finalité (un objectif défini) ; la routine (elle intervient à des intervalles réguliers) ; la systématicité (elle obéit à un agenda rationnel) ; la focalisation : l'attention est concentrée sur un point particulier, pouvant regrouper plusieurs individus (surveillance de masse) et non un seul (Ball et Wood, 2006). La langue

française ne fait pas la distinction que permet l'anglais entre surveillance et monitoring (D'Urso, 2006)[1].

Placer des personnes ou des groupes sous surveillance implique de disposer de l'information enregistrée sur leurs mouvements. Cette information est ensuite traitée, analysée, utilisée à des fins qui les affecteront directement ou indirectement, dans l'immédiat ou en différé, et parfois jamais.

Pas un aspect de notre vie, perçu comme présentant le moindre intérêt en termes d'information, qui ne puisse aujourd'hui être transformé en un format numériquement quantifié. Ce phénomène est amplifié par les grands axes de convergence technologique : entre le monde des télécommunications et celui de l'informatique, entre des familles d'outils, et en raison des capacités accrues de stockage des données sur les disques durs et les serveurs, transformant les *data centers* en véritables actifs stratégiques. Plus qu'un simple rapprochement entre deux technologies, l'industrie parle de convergence lorsque plusieurs technologies fusionnent pour ne plus donner que la simple addition des composants. La convergence nécessite du matériel, des infrastructures et des protocoles de communications nouveaux pour faire transiter les flux de données sur le réseau.

Si certains dispositifs ont pour fonction première de surveiller, d'autres ont adjoint une finalité de surveillance à une fonction initiale : ainsi les cartes de paiement permettent désormais, grâce au développement des bases de données et à l'interconnexion des fichiers, de déterminer à partir des historiques d'achat les préférences alimentaires, ou de retracer les dates et les lieux d'achat…

1. « Bien que les deux termes « monitoring » et « surveillance » soient souvent utilisés de manière interchangeable, et que la distinction entre les deux reste floue lorsque le motif de leur utilisation est inconnu, ce sont en réalité deux concepts distincts. Le monitoring est un terme bien plus bénin qui peut être appliqué à une variété de situations où les données sont collectées pour un nombre de raisons acceptables ou nécessaires. La surveillance, cependant, induit souvent une connotation de suspicion car l'information collectée a le potentiel d'imposer des conséquences négatives, telles que d'entraver certains comportements de la part des individus ciblés ».

Appartenant à la première catégorie, les caméras vidéo se sont banalisées au cours des dernières années. Caméras de surveillance jusque dans les distributeurs de billets, les parkings et les ascenseurs, webcams, mais aussi téléphones-appareils photos constituent la « société des écrans » (Lipovetsky et Serroy, 2007). Les justifications sont multiples et surtout les applications se diversifient : détection de mouvements suspects dans le métro, substitut de pointeuse sur des chantiers, vérification de l'identité de chômeurs...

Les défenseurs des libertés publiques s'alarment de cette prolifération subie et de ses effets comportementaux induits. Même du point de vue de ceux qui sont prêts au compromis avec les libertés publiques au nom de la sécurité publique et de la préservation de l'ordre social, les caméras de surveillance montrent leurs limites. Elles sont, par exemple, inefficaces quand il s'agit de prévenir des crimes, des émeutes en temps réel ou de disperser des foules ; tout juste servent-elles à apporter la preuve, après l'événement, de la responsabilité des faits aux personnes impliquées dans les incidents. Si un rapport du Parlement européen fait état de la difficulté d'assurer sur du long terme une stabilité de l'ordre public dans un cadre démocratique, il recommande toutefois de bien mettre en balance les systèmes de supervision de masse conduisant à une surveillance totale et de limiter leur extension (European Parliament, 2000).

Les puces RFID (*radio frequency identification*), ou dispositifs communicants équivalents, illustrent la seconde catégorie. Développées à l'origine pour la gestion logistique des marchandises, leurs usages se diversifient, deviennent ludiques (chronométrage de sportifs pendant une course), sécuritaires (suivi de délinquants, de documents ou marchandises pour éviter le vol) ou motivés par un souci d'efficacité gestionnaire (vérification du recyclage dans les poubelles). Avec la montée en puissance de l'Internet des objets et la miniaturisation des dispositifs grâce aux nanotechnologies, elles sont en train de se répandre massivement dans l'espace privé et public. Elles commencent aussi à pénétrer le corps humain pour du suivi médical.

Le drone, quant à lui, se déploie aux deux bouts de la chaîne. Objet volant miniature et ludique pour les bricoleurs du dimanche, il est en

train de changer radicalement la manière dont la guerre se conçoit et se mène. Dans un marché en plein essor, il devient un élément clé de la chaîne de la mort, la « kill chain » d'une guerre transférée chaque jour davantage aux mains d'organisations privées ; il raccourcit la boucle de décision entre la détection de la cible et la frappe. Il laisse envisager une guerre prenant la forme d'un « télétravail accompli par des employés de bureau » (Schwartzbrod, 2013), moderne et connectée (Singer et Deville-Fradin, 2013), privilégiant la capacité à travailler en réseau, utilisant la maîtrise totale de l'information associée à des systèmes d'attaque de précision.

Dans l'échelle de l'infiniment petit, les poussières intelligentes ou communicantes forment une nuée de micropuces capables de capter, traiter, ou transmettre des données grâce à leur dissémination dans l'atmosphère.

La biométrie se répand de plus en plus dans les systèmes de sécurité publics et privés, les biens de consommation électroniques, les terminaux de points de vente, tout en se sophistiquant. Elle s'appuie sur des parties du corps pour répondre au besoin croissant d'identification, souvent au motif d'un gain de temps et d'une évolution vers la simplification. Les recherches s'orientent vers des distances de reconnaissance de plus en plus longues pour une saisie sans contact physique. L'odeur du corps pourrait donner lieu à interprétation quant à ses sentiments ou son humeur (Oyeleye, *et al.,* 2012,). Les neurosciences notamment, s'appuyant sur le décloisonnement des frontières disciplinaires, viennent en soutien à ces recherches.

La dangerosité et l'efficacité de ces technologies de surveillance est démultipliée par les bases de données et les fichiers qui les sous-tendent, le mouvement de décloisonnement et d'interconnexion, la délégation de leur gestion à des tierces parties. Or, elles ne se contentent pas de compiler les informations communiquées. Elles détectent des « liens faibles » (centres d'intérêts, pratiques communes) qui relient plusieurs personnes. Toutefois, l'objectivité revendiquée à travers le recours à ces systèmes est réfutée par certains, qui démontrent que le codage des programmes de la part des concepteurs et des ingénieurs est orienté par leurs préjugés culturels, notamment de sexe et de race (Magnet, 2011).

Évaluer une à une chaque technologie en mettant en regard les avantages *versus* les risques sur les libertés n'a pas beaucoup de sens. C'est la convergence de l'ensemble qui doit être pensée. Parallèlement, il faut élargir la réflexion en pensant non seulement la convergence de ces technologies et ce qu'elles produisent en elles-mêmes, mais la manière dont les pratiques sociales s'en emparent.

3. Des observateurs de la surveillance aux défenseurs de la liberté, des acteurs épars

Dans le discours sécuritaire porté par les États et les gouvernements, les dispositifs de surveillance jouent le rôle de garde-fous contre les menaces en tout genre (terroriste, environnementale, démographique), réelles ou imaginaires, et servent de justificatifs dans le déploiement de bases de données d'identifiants personnels. Mais la logique sécuritaire ne suffit pas à elle seule à expliquer cette croissance exponentielle de fichiers.

La prolifération de ces fichiers obéit à des objectifs de management en permettant de contrôler les résultats des agents chargés d'exécuter les procédures afférentes. Ainsi, le parcours jalonné de fichiers des étrangers répond, outre à des finalités de contrôle, à un besoin administratif et comptable et à une recherche d'efficacité optimale dans l'organisation du travail : par exemple, assurer une meilleure fluidité du trafic en réduisant les files d'attente (Marzouki, 2010). Le changement de pratiques professionnelles qu'implique l'adaptation à ces nouvelles technologies a pour effet d'instaurer des moyens inédits de contrôle du rendement.

Parallèlement, l'individu est incité à dévoiler chaque jour un peu plus de lui-même. Après les autocommutateurs, les webcams et les logiciels de traçage font partie des outils permettant de scruter les goûts et comportements individuels et collectifs des internautes, voire leur état physique ou psychologique, selon les mots qu'ils emploient dans les moteurs de recherche. Relations amicales, pensées, échanges, déplacements, se muent en données gravées dans une mémoire virtuelle. Ces données survivent longtemps. Il devient difficile de s'en défaire, et aussi, tout simplement, de deviner qu'elles existent, où elles

se trouvent, qui les exploite, et à quelles fins. Les traces que laisseraient nos déplacements sur internet seraient d'autant plus insidieuses qu'elles sont invisibles et vont s'accumulant.

Cette collecte d'information se solde par une segmentation des populations (Van der Ploeg, 2004) : ciblage commercial, social, citoyen… Les plus visées deviennent les plus vulnérables : populations migrantes, enfants (Van der Ploeg, 2011), alors que la globalisation produit de nouvelles inégalités relatives aux mobilités géographiques (Bauman, 1999). Dans la logique économique qui va toujours plus loin dans l'analyse des goûts, des habitudes et des capacités financières des individus, les vulnérabilités sont aussi exploitées : ainsi des ordinateurs identifient des addictions au jeu mais veillent à ce que les personnes ne se détournent pas complètement de celui-ci (Burn-Murdoch, 2013).

La constitution de telles segmentations, assortie d'une aura de modernité et d'objectivité, vient à l'appui du souci de tri et de lutte contre la fraude. Dans le contexte d'une politique sécuritaire, il s'agit de distinguer le « vrai » du « faux », de prémunir les « innocents » contre les déviants ou les délinquants. Cette alliance entre l'obsession de la fraude et l'enthousiasme pour les résultats chiffrés et leur pouvoir de prédiction est à l'origine de l'essor d'une véritable « technologie du soupçon » (Mouvements, 2010).

Le monde universitaire (notamment au Canada, mais aussi au Royaume-Uni et en Australie) a investi ces questions, et il existe un courant international structuré des « surveillance studies ». Leurs études portent entre autres sur les imbrications de la surveillance dans les processus sociétaux, sur la manière dont les individus se conforment aux dispositifs et s'inscrivent dans les processus de surveillance. Elles mettent notamment en exergue le déplacement actuel de dispositifs verticalisés (par l'État en particulier) vers des formes de surveillance polycentriques, en réseau, dans lesquelles les proches jouent un rôle. La surveillance, indépendamment des méthodes ou des technologies nouvelles, a toujours pour vocation le tri social, en vue d'un classement des populations envisagé comme prélude à un traitement différencié (Lyon, 2001).

Se développent ici et là des mouvements contestataires, ou des organisations – plus ou moins légitimées par les pouvoirs en place –, qui visent à faire prendre conscience du rétrécissement de l'espace privé et de l'atteinte aux libertés, voire à s'y opposer. Ils œuvrent avec des buts divers : faire de la veille, informer et éclairer la population pour faire évoluer les mentalités et créer des « résistances », apporter des propositions aux États afin d'infléchir les législations.

Les acteurs qui tentent de résister à la société de surveillance peuvent être classés de façon simplificatrice en quatre grandes familles :

– Ceux venus des droits de l'homme : centres de recherche (*Electronic Privacy Information Center* ou EPIC)[2], organisations non gouvernementales (*Privacy International*[3], participant au site Privacy.org[4] avec l'EPIC), associations à but non lucratif comme l'Union américaine pour les libertés civiles (*American Civil Liberties Union* ou ACLU[5]) ou d'autres ayant une vocation plus large (la Ligue des droits de l'homme en France[6], *Big Brother Watch* en Angleterre[7]).

– Ceux venus des technologies de l'information : l'*Electronic Frontier Foundation* ou EFF[8]. Les personnalités à l'origine de ces technologies qui façonnent aujourd'hui notre monde (ordinateur personnel, internet, web…) ont depuis les années 1970 défendu vigoureusement à la fois la liberté d'information que ces technologies sont censées faciliter par des logiques de distribution et le refus de toute forme de surveillance – notamment étatique. Le hacker (figure, certes, plurielle), est l'incarnation type de cette revendication, récemment représentée par des personnalités comme Aaron Schwartz ou Julien Assange.

– Ceux venus de la donnée : depuis le milieu des années 2000, un mouvement de plus en plus structuré a émergé pour revendiquer que les données de source publique soient mises à disposition de tous (open

2. Electronic Privacy Information Center. http://epic.org/
3. Privacy International, https://www.privacyinternational.org/
4. http://privacy.org/index.html
5. American Civil Liberties Union, http://www.aclu.org/
6. Ligue des droits de l'homme, http://www.ldh-france.org/Nous-contacter
7. Big Brother Watch, http://www.bigbrotherwatch.org.uk/
8. Electronic Frontier Foundation, https://www.eff.org/fr

data), au nom de la transparence, considérée comme une garantie de qualité démocratique.

– Des individus dits « ordinaires » ou des intellectuels (Da Cunha, 2014, 20) qui se constituent en collectifs au gré des événements et en réaction à l'avènement de certaines technologies perçues comme intrusives. Par exemple, les groupes de parents luttant contre l'usage de la biométrie à l'école, le collectif *Pièces et main d'œuvre*, qui considère comme une servitude technologique la connexion permanente et la dépendance envers un système technicien qui nous ferait entrer dans une « société de contrainte » (Rousseaux, 2010), le mouvement *Stop the Cyborgs*, initié par trois Londoniens ; le programme baptisé Glasshole.sh qui détecte la « signature » des Google Glass et les empêche de se connecter à un réseau Wifi ; le projet *Cyborg Unplug.* Steve Mann, considéré comme le père des *wearable devic*e propose l'utilisation de ces technologies (en l'occurrence son EyeTap) à des fins de ce qu'il appelle « sousveillance », une forme de résistance individuelle et citoyenne en retournant les dispositifs de surveillance contre leurs instigateurs.

Ainsi, les technologies de la surveillance sont-elles controversées. La presse se fait l'écho des peurs et des résistances. La puce RFID apparaît comme une menace (Draeta et Delanoë, 2012), les compteurs intelligents suscitent la suspicion (Fauteux, 2012), les drones sont combattus par des organisations anti-drones, etc. Les protestations de ces différents acteurs s'élèvent dans un contexte où la menace du terrorisme (Commission Européenne, 2015) se montre propice à des valeurs et des orientations idéologiques et politiques autoritaires (Cohrs, *et al.,* 2005).

En dehors de ces inquiétudes liées aux libertés civiles, la perspective d'implants électroniques dans le corps humain fait émerger des questions plus philosophiques liées au statut du corps, à la frontière entre l'humanité et l'animalité, entre le corps et les techniques, et à la mutation en cours du vivant et de l'humanité elle-même. Simultanément à l'expansion des technologies de l'information, apparaissent de plus en plus d'accessoires médicaux destinés au diagnostic de la condition humaine et au maintien des fonctions vitales, via notamment la surveillance des organes (pulsations du cœur, …). Le corps s'entoure

d'une technologie connectée en réseau, basée sur des implants et des capteurs (Andreeva, 2012).

La création d'un Internet des objets, caractérisé par la mise en réseau de tous les objets, et dont les services accompagneraient les utilisateurs dans chacune de leurs activités (dans des domaines aussi divers que l'éducation, les services de proximité, la santé, les loisirs, la citoyenneté, la gestion des villes ou encore la maîtrise de l'énergie) pourrait, si elle se généralisait, faire de nos biens, des objets que nous amenons avec nous, des vêtements que nous portons, des espions à même de renseigner sur notre vie.

4. Vers une servitude volontaire ?

La constitution des bases de données d'envergure entraîne, au-delà des questions techniques de sécurisation des données, ou juridiques de protection de la vie privée, une évolution culturelle de notre société, vers une « société de surveillance » qui change de paradigme. L'œil unique du surveillant se mue en « œil absolu » (Wajcman, 2010), au fur et à mesure de la globalisation de la surveillance (Mattelart, 2007). Quant aux individus, ils participent de plus en plus par leurs actes quotidiens à la perpétuation et à la dynamique de la société de surveillance. « Nous faisons volontairement beaucoup de choses que les pouvoirs totalitaires cherchaient à imposer par la force et la violence ou la peur » (Poulet, 2013).

La société pourtant se méfie des risques d'erreur et de fraude à l'identité, de la menace qui pointe d'une société orwellienne dont le maillage se resserrerait un peu plus chaque jour. Un des risques serait que l'on utilise certaines pratiques à d'autres finalités que celles avancées (quand elles le sont), sans qu'on ait le moyen de le vérifier. Or, de plus en plus, ces technologies, pour se déployer, doivent s'appuyer sur le corps. Le glissement du corps anatomique vers le corps numérique, et le traitement dont il fait l'objet, représente une mutation anthropologique sans précédent. Le corps livre de lui-même des informations indéchiffrables ou incompréhensibles par l'individu. Des organismes tels que la CNIL en France réservent à tout individu le droit d'accès et de rectification aux données personnelles le concernant : mais

que dire des propriétés de l'algorithme ou du codage censé représenter notre empreinte digitale ? Comment évaluer sa justesse ou sa fiabilité ? Pourrais-je le faire « rectifier » au même titre que je peux aujourd'hui prétendre corriger mon adresse ou mon lieu de naissance ? En serais-je même capable ?

La transformation de certaines caractéristiques physiques en données numériques *via* les technologies fait que le corps apparaît sous d'autres critères, « corps rationalisé » et divisé, fait de données abstraites (Lyon, 2011). Ceci met à mal la dichotomie distinguant le corps, de l'information *relative à ce corps*, puisque le corps lui-même consiste en des informations qui contribuent à le définir (Van der Ploeg, 2007).

Le film de science-fiction *Time Out* d'Andrew Niccol (2011), présente la version d'un corps comme instrument d'épargne et d'échange contre des services : un compteur intégré à l'avant-bras de chacun se recharge en temps, devenu l'unité monétaire permettant de payer ses dépenses et qu'on acquiert par divers moyens. L'exemple de ce film montre que les imaginaires accompagnent les évolutions technologiques. Avec eux, les discours et l'insertion sociale des technologies constituent trois temps d'une innovation technique (Scardigli, 1992). Or, les technologies concernées sont peuplées d'imaginaires (Schunadel, 2011). « Il est patent que la part de l'imaginaire est désormais croissante dans la définition et la stimulation des marchés. D'une certaine manière, au sein de l'ordre marchand contemporain, le rêve est aux commandes (…) Ce à quoi nous assistons consiste probablement en la mise en place d'articulations fines entre science, technologie, marchés et imaginaires » (Pajon, 2008). Ces objets techniques sont mis en récit dans les séries télévisées de police scientifique (Chouteau et Nguyen, 2014).

En dehors de la perte de repère qu'elles induisent quant à la représentation de soi, les données font du corps un moyen utilisé à des fins par des tierces parties qui y trouvent un intérêt (financier, marketing,…) qui leur est propre. Cela induit pour l'individu une perte de contrôle sur soi. La question est alors de savoir si celle-ci est consciente, volontaire, et/ou contrainte, et dans le dernier cas, si la réversibilité du processus est possible. On peut aussi légitimement

s'interroger pour savoir si ces mutations contemporaines tant dans leurs activités que dans les nouvelles relations de service qu'elles induisent, ne représentent pas de nouvelles formes de servitude volontaire, en tentant de donner un prolongement contemporain à la réflexion de La Boétie (1978). Le concept de servitude volontaire associe chez La Boétie une double détermination : l'une renvoyant à l'extériorité échappant au contrôle de la volonté du sujet, l'autre relevant de l'intériorité : c'est la servitude volontaire par désir ou par consentement, en toute conscience de ce à quoi on renonce. La servitude est communément associée à la soumission et à la dépendance. Elle renvoie aussi à des situations contractuelles bien définies telles que la relation de service (Hamraoui, 2005).

Suivant cette approche, et au regard des nouvelles technologies, la servitude pourrait prendre la forme du consentement, celui-ci se muant, de manière empirique, en une transaction. Un utilisateur accepterait de livrer des fragments de sa vie privée, voire de son identité, contre du « confort » (une meilleure « expérience » utilisateur, des contenus personnalisés, le corps comme « sésame » remplaçant une liste à rallonge de mots de passe...) Le consentement n'est pas soumis à une forme particulière et il peut résulter d'actes divers. Nous consentons chaque jour à quantité de traitements ou de collectes de données liées à notre activité et à notre comportement (la visite d'un site web en sachant qu'il utilise des cookies, l'entrée dans un magasin qui a un dispositif de vidéosurveillance visible, la navigation sur un moteur de recherche gardant en mémoire cet historique…), parfois même sans nous en rendre compte. En effet, notre consentement est aussi souvent récolté par le biais de conditions générales ou de politiques de confidentialité, rarement lues. Si certaines clauses font l'objet d'un contrat discuté et négocié entre les parties, alors on admettra que chacun savait à quoi il s'engageait. On ne pourrait réglementairement s'y opposer que si elles sont insolites (inattendues) ou abusives (disproportionnées), ce qui rendrait le consentement invalide. Le législateur en France prévoit que le consentement, pour être valable, doit être libre et éclairé, et que seuls trois cas justifient qu'il ne soit pas acquis : l'erreur (sur la nature de la chose), la violence, le dol (manœuvre frauduleuse) [Code civil, article 1109].

On le voit ici, le consentement peut être appréhendé « dans son sens juridique (formaliste ou contractualiste) ou par les voies de l'empirie, dans sa dimension procédurale et interactionniste » (Coste *et al.*, 2008). C'est un moyen subreptice de justifier une atteinte à la sphère privée. Et l'exposition de soi via les nouvelles technologies pourrait, dans certains cas, s'apparenter à la servitude volontaire par méprise, en raison de l'ignorance, d'un manque de vigilance ou d'une course aux honneurs.

En tout état de cause, le consentement engage souvent l'individu dans la durée. André Mondoux considère que les médias sociaux, plus que des outils permettant une expression personnelle, sont le lieu de « déploiement de stratégies de quête/construction de soi » qui ne se réalisent pleinement que si « je me soumets au regard de l'autre » ; et c'est ce regard automatisé et reconduit dans le temps qui, tout en rassurant sur le besoin d'être reconnu de l'autre « dès qu'il se manifestera » se transforme en surveillance. Ainsi banalisée, celle-ci s'intègre aux rapports de socialisation et aux processus identitaires, embarqués dans une dynamique de reproduction sociale (Mondoux, 2012).

L'usage des nouvelles technologies actuelles brouille la frontière entre consentement, contrainte, séduction, soumission, obéissance, résignation : développer une éthique du consentement en mettant à jour ce processus de « surveillance identitaire » (Mondoux, 2012) à l'œuvre pourrait être une piste pour redonner à l'individu l'exercice de sa liberté.

5. Conclusion

Dans les années 1960, l'informatique avait permis aux entreprises et administrations de se doter de fichiers dont la taille allait rapidement croître. L'utilisation non contrôlée de ces fichiers allait bientôt poser problème. La raison première tenait à la sensibilité des sociétés civiles à la défense de la vie privée dans le contexte des années 1970 et des grands mouvements de défense des droits et libertés (droits civiques, droits des femmes, etc.). Mais ce sont des scandales qui ont permis que le débat débouche sur l'adoption de règles et la création d'instance de régulation et de contrôle. Aux États-Unis, une série de lois ont été votées

entre 1973 et 1976, à la suite du scandale du Watergate, lois qui fixaient des limites strictes à la collecte et aux croisements de fichiers par les organes de sécurité et autres institutions publiques. Par extension, ces règles se sont appliquées aux entreprises et à leurs fichiers. Le débat a eu lieu en France dans des termes très comparables, la Commission nationale de l'informatique et des libertés (CNIL) ayant été créée en 1978 par une loi votée après le scandale du fichier Safari.

La dataveillance pose des problèmes de même nature, mais à une toute autre échelle. La divulgation par le *Washington Post* et le *Guardian* en juin 2013 de la surveillance de la totalité des communications téléphoniques aux États-Unis ainsi que celle des grands acteurs du web et des télécoms par le programme américain de surveillance des internautes étrangers, Prism, pourrait jouer un rôle similaire aux scandales du Watergate et du fichier Safari. Mais, si une partie de la société est sensibilisée à la défense de la vie privée, la crainte du terrorisme crée un climat idéologique très différent de celui des années 1970. Le sociologue allemand Ulrich Beck analyse les transformations de nos sociétés en présentant le risque comme une nouvelle question centrale (Beck, 2001) : nos sociétés sont de moins en moins tolérantes au risque et les demandes assurancielles augmentent. Mais, alors que les États étaient supposés fixer les normes et donner les garanties qui protégeraient de ces risques, leur multiplication et la réduction de l'État-providence renvoient aux individus les décisions d'arbitrage sur ces risques et leurs probabilités.

À cet égard, les évolutions du législateur, les mouvements de résistance collective (qu'elle soit de grande ampleur ou le fait d'une minorité organisée) quant aux mesures de surveillance de masse, les pratiques émergentes du *quantified self* (Pharabod, *et al.,* 2013) seront à surveiller de près. Les outils numériques, avec, en premier lieu, le smartphone, de plus en plus polyvalent, sont destinés, d'une part, à permettre une accessibilité totale et immédiate à l'information et à la communication, d'autre part à la traçabilité virtuellement constante de données (physiques, motrices, visuelles, comportementales…), contribuant à définir notre identité numérique. Le corps intègre dans ses modes de perception et de relation ces outils et techniques, qui finissent par innerver jusqu'à ses manières d'être. Les nouveaux

comportements induits, en se substituant peu à peu à des savoirs patiemment acquis, font évoluer à leur tour normes et conventions culturelles. La culture de la surveillance s'intègre ainsi progressivement et subrepticement à la culture numérique proprement dite et entraîne le brouillage des frontières entre des domaines de discipline auparavant bien distincts. Aussi, la rapidité ou la facilité avec laquelle ces outils seront adoptés sans contrainte, réserve, résistance, questionnement, ou recherche d'alternative quant à leurs dispositifs de surveillance (jusqu'à la possibilité de déconnexion), et les données communiquées volontairement par chacun sur les réseaux sociaux ou le cloud, pourront être interprétés comme des indices supplémentaires de la « servitude volontaire » : un paramètre essentiel, selon certains, pour comprendre la modernité contemporaine en Occident (Chaignot, 2012).

Dans ce contexte, les sciences humaines et sociales, dont une des fonctions scientifiques est de comprendre les mécanismes qui sous-tendent le monde social, questionnent l'avènement possible de nouvelles formes de pouvoirs : biopouvoir annoncé par Michel Foucault (un concept mis à jour par Donna Haraway sous l'appellation techno-biopouvoir), et dont la particularité serait la participation active de la plupart d'entre nous à ces nouvelles modalités de contrôle et de domination, sujettes à controverses et susceptibles d'engendrer des mouvements sociaux spécifiques. Elles mettent aussi en évidence l'apparition d'une rupture épistémologique : passage d'une production de connaissances par une communauté autonome de scientifiques travaillant sous leurs propres normes, à un mode reposant sur l'idée que celle-ci se fait désormais aussi dans un contexte ouvert, en relations étroites avec les utilisateurs potentiels. En effet la numérisation généralisée, le recueil, l'analyse et le traitement des données, mettent les technologies de l'information au cœur de tous les domaines scientifiques et techniques, ce qui oblige dans le même temps à des approches transdisciplinaires, faisant naître de nouveaux questionnements sociologiques grâce à la mise en visibilité d'objets jusque-là invisibles.

Bibliographie

Andreeva Ekaterina (2012). Alternative Biometric as Method of Information Security of Health Systems. *Proceeding of the 12th Conference of Fruct Association,* p. 210-214.

Ball Kristie, Murakami Wood David, (2006). *A report on the surveillance society for the Information Commissioner, Summary Report,* http://www.ico.org.uk/upload/documents/library/data_protection/practical_application/surveillance_society_summary_06.pdf.

Bauman Zygmunt (1999). *Le coût humain de la mondialisation*, Paris, Hachette Littérature, coll. Forum.

Beck Ulrick (2001). *La société du risque. Sur la voie d'une autre modernité*, Paris, Éditions Aubier.

Berthoud Gérald (2002). L'horizon d'une surveillance omniprésente ?, *Revue européenne des sciences sociales*, http://ress.revues.org/623 ; DOI : 10.4000/ress.623

Burn-Murdoch John (2013). *UK technology firm uses machine learning to combat gambling addiction*, http://www.theguardian.com/news/datablog/2013/ aug/01/uk-firm-uses-machine-learning-fight-gambling-addiction.

Chaignot Nicolas (2012). *La servitude volontaire aujourd'hui : esclavages et modernité*. Paris, Presses Universitaires de France.

Chouteau Marianne, Nguyen Céline (2014). Ecrans, lampes et mallettes. Les objets techniques dans l'univers des Experts. *Alliage, Science en fiction*, automne 2014, n° 74, p. 68-78.

Clarke Roger (1988). Information technology and dataveillance. *Communications of the ACM*, vol. 31, n° 5, p. 498-512, http://dl.acm.org/citation.cfm?id=42413

Cohrs Christopher J., Kielmann Sven, Maes Jürgen, Moschner Barbara (2005). Effects of right-wing authoritarianism and threat from terrorism on restriction of civil liberties. *Analyses of Social Issues and Public Policy*, vol. 5, n°. 1, p. 263-276.

Commission européenne (2015). *European Agenda on Security: Strengthening EU cooperation in the fight against terrorism, organised crime and cybercrime*, http://ec.europa.eu/dgs/home-affairs/what-is-new/news/news/2015/20150428_01_en.htm.

Coste Florent, Costey Paul, Tangy Lucie (2008). Consentir : domination, consentement et déni. *Tracés* n° 14, p. 5-26

Da Cunha Amaury (2014). Voleurs d'images. Pour cerner l'impact des Google Glass, un Américain a arpenté les rues de sa ville armé d'une caméra*. Le Monde*, 25 août 2014.

Draeta Laura, Delanoë Alexandre (2012). *RFID, une technologie controversée. Ethnographie de la construction sociale du risque*, Cachan, Hermes-Lavoisier, Coll. Mondialisation, hommes et sociétés.

D'Urso Scott C. (2006). Who's Watching Us at Work? Toward a Structural–Perceptual Model of Electronic Monitoring and Surveillance in Organizations. *Communication Theory* 16, p. 281-303.

European Parliament (2000). *Crowd Control Technologies, Working document for the STOA panel, final study*, http://www.europarl.europa.eu/RegData/etudes/etudes/stoa/2000/168394/DG-4-STOA_ET%282000%29168394_EN%28PAR02%29.pdf

Fauteux André (2012). *Compteurs intelligents : des experts dénoncent la désinformation flagrante*, https://maisonsaine.ca/sante-et-securite/electrosmog/compteurs-intelligents-experts-denoncent-desinformation-flagrante.html

Forest David (2009). *Abécédaire de la société de surveillance*. Paris, Syllepse.

Hamraoui Eric (2005). Servitude volontaire : l'analyse philosophique peut-elle éclairer la recherche pratique du clinicien ? *Travailler* 2005/1, n°13, p. 35-52.

La Boétie Etienne De (1978 (1576)). *Le discours de la servitude volontaire*, Paris, Payot.

Lipovetsky Gilles, Serroy Jean (2007). *L'écran global*, Paris, Seuil.

Lyon David (2011). Les insignes corporels : la biométrie comme perte de l'histoire personnelle. *L'identification biométrique : Champs, acteurs, enjeux et controverses*, Paris, Editions de la Maison des sciences de l'homme.

Lyon David (2001). *Surveillance society : monitoring everyday life,* Open university press, Buckingham.

Magnet Shoshana Amielle (2011). *When Biometrics Fail: Gender, Race, and the Technology of Identity*. Durham, NC: Duke University Press.

Marzouki Meryem (2010). Fichiers : logique sécuritaire, politique du chiffre ou impératif gestionnaire ? *Mouvements*, 2010/2 n° 62, p. 85-98. DOI : 10.3917/mouv.062.0085.

Mattelart Armand (2007). *La globalisation de la surveillance. Aux origines de l'ordre sécuritaire*, Paris, Éditions La Découverte.

Mondoux André (2011). Identité numérique et suveillance. *Les Cahiers du numérique*, 2011/1, vol. 7, p. 45-59.

Mouvements (2010). La technologie du soupçon : tests osseux, tests de pilosité, tests ADN. *Mouvements*, n° 62, p. 80-83.

Oyeleye C. Akinwale, Fagbola Temitayo M., Babatunde R. Seyi, Adigun Adebisi A. (2012). An Exploratory Study Of Odor Biometrics Modality For Human. Recognition, *International Journal of Engineering Research & Technology*, vol. 1, n° 9, http://www.ijert.org/view-pdf/1555/an-exploratory-study-of-odor-biometrics-modality-for-human-recognition.

Pajon Mark (2008). Les technologies convergentes et leurs maîtres enchanteurs. *Les imaginaires du corps en mutation*, Paris, L'Harmattan, p. 321-336.

Pharabod Anne-Sylvie, Nikolski Véra, Granjon Fabien (2013). La mise en chiffres de soi. Une approche compréhensive des mesures personnelles. *Réseaux*, n° 177, p. 97-129.

Poulet Bernard (2013). Les pires dictatures n'auraient pas osé rêver de Facebook, interview de Zygmunt Bauman. *Au fait*, juin 2013, n°002, p. 60-77.

Rousseaux Agnès (2010). Avec les nanotechnologies, nous entrons dans une société de contrainte, totalitaire. *Basta!* 29 janvier 2010, http://www.bastamag.net/Avec-les-nanotechnologies-nous

Scardigli Victor (1992). *Le sens de la technique*, Paris, PUF.

Schunadel Nicolas (2011). *Les Schèmes anxiologiques : de l'affectivité transcendantale aux dynamismes de l'imaginaire, suivi d'une application à l'imaginaire de la RFID.* Thèse en littérature et sciences humaines, Université de Grenoble.

Schwartzbrod Alexandra (2013). La guerre devient un télétravail pour employés de bureau, interview de Grégoire Chamayou. *Libération*, 19 mai 2013, http://www.liberation.fr/monde/2013/05/19/la-guerre-devient-un-teletravail-pour-employes-de-bureau_904153.

Singer Peter W., Deville-Fradin Valentine (traductrice de l'original en anglais), (2013). La guerre connectée : les implications de la révolution robotique, *Politique étrangère*, automne n° 3, p. 91-104.

Van der Ploeg Irma (2011). Le corps biométrique : différences corporelles, normes intégrées et classifications automatisées. *L'identification biométrique : Champs, acteurs, enjeux et controverses*, Editions de la Maison des sciences de l'homme, coll. PraTICs, p. 329-369.

Van der Ploeg Irma (2007). Genetics, biometrics and the informatization of the body. *Ann Ist Super Sanită*, vol. 43, n° 1, p. 44-50.

Van der Ploeg Irma (2004). Biometrics and the body as information: normative issues in the social-coding of the body. *Surveillance as social sorting: privacy, risk, and automated discrimination*, New York, Routledge, p. 57-73.

Wajcman Gérard (2010). *L'œil absolu*. Paris, Denoël.