La sousveillance

Camille Alloing

La sousveillance

Vers un renseignement ordinaire ?

Camille Alloing

CEREGE – Université de Poitiers

Cet article est une version « pre-print », certains éléments peuvent ainsi différer de celui publié.

Merci de citer : ALLOING, C., « La sousveillance. Vers un renseignement ordinaire ? », *Hermès* n° 76, 2016, pp. 68-76.

Caméras de surveillance urbaine, géolocalisation des téléphones mobiles, données de connexion à des sites Internet, IMSI-catcher[1], etc. Les services de renseignement, et spécifiquement ceux dédiés au renseignement intérieur, disposent d'un nombre grandissant d'outils leur permettant de collecter les données et informations que chaque citoyen produit au quotidien. L'industrie de la surveillance numérique compterait par ailleurs à ce jour plus de 500 éditeurs de logiciels spécialisés[2] (dont 46 en France). Les révélations du lanceur d'alerte Edward Snowden ont de plus mis en avant les collusions et ententes entre certaines plateformes dominantes du Web et les services de renseignement étatique.

Twitter, Periscope, Snapchat, Youtube, etc. Chaque usager du Web a lui aussi à sa disposition un ensemble d'outils lui permettant de produire et de diffuser de l'information à chaque instant. Les récentes manifestations contre la « loi travail » (mai-juin 2016) illustrent la capacité de chaque individu à « apprendre quelque chose à quelqu'un. Plus largement, [à] donner à quelqu'un une indication sur une chose » (Moinet, 2011, P. 21). C'est-à-dire à renseigner. En l'occurrence, ces manifestations ont mis en avant la plateforme Periscope.tv qui offre la possibilité de diffuser des vidéos en direct depuis un téléphone mobile.

[1] Selon Wikipédia, un IMSI-Catcher « est un matériel d'espionnage téléphonique utilisé pour l'interception du trafic de téléphonie mobile et pour pister les mouvements des terminaux et donc de leurs porteurs. Il s'agit approximativement d'une fausse « antenne-relais » agissant entre le téléphone mobile espionné et les antennes-relais de l'opérateur téléphonique. ». Source : https://fr.wikipedia.org/wiki/IMSI-catcher.

[2] Voir : https://sii.transparencytoolkit.org

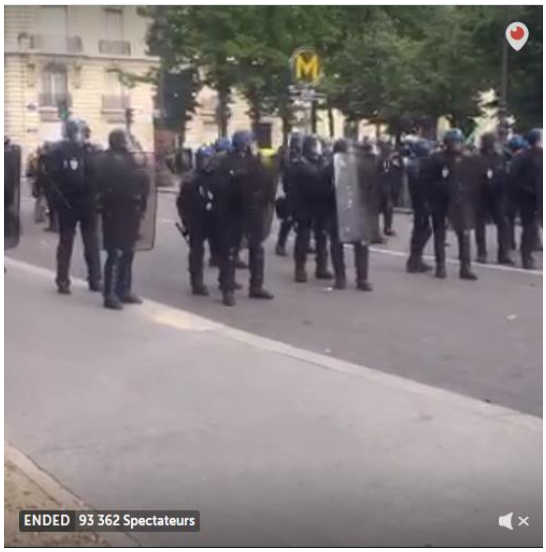

Figure 1 : capture d'un « live » sur Periscope des manifestations anti loi Travail du 14 juin 2016[3]*. A noter que ce « live » de 2h30 a réuni 93 362 spectateurs.*

Si les journalistes se sont emparés de cette plateforme, celle-ci est fortement utilisée par des militants et manifestants pour dénoncer les violences (policières notamment) qui ont eu lieu durant ces manifestations. Cet usage des dispositifs numériques visant à « surveiller les surveillants », en l'occurrence dans cette illustration les forces de l'ordre, est conceptualisé par la notion de « sousveillance » développée par le chercheur et inventeur Steve Mann.

Pour Mann et al. (2002) la sousveillance serait un panoptique (au sens de Foucault) inversé. Elle désigne alors les capacités données à chaque citoyen de faire usage des dispositifs numériques pour « regarder d'en bas » (*watching from below*) les différentes formes de pouvoirs étatiques ou commerciaux. Mann nomme cette possibilité de s'approprier les outils de surveillance exerçant une forme de contrôle social formel sur les individus, du « reflectionism » (Mann, 1998) : détourner les outils construits par certaines organisations (étatiques mais aussi commerciales –moteurs de recherche, etc.) afin d'exercer un contrôle citoyen.

Nous souhaitons discuter ici trois aspects de cette sousveillance que nous abordons comme une forme de renseignement ordinaire, car inhérente aux usages de certaines technologies. Mais la sousveillance nous parait aussi comme un renseignement « citoyen » puisqu'elle offre à chacun d'entre nous la possibilité de médiatiser les actions voire les dérives des entités nous surveillant au quotidien afin de favoriser le débat démocratique. Le premier aspect est celui de la sousveillance telle qu'énoncée par Steve Mann, dans son caractère physique pourrions-nous dire, et qui repose sur l'utilisation de dispositifs embarqués afin de rendre compte d'une situation ou d'un événement précis où le contrôle social formel s'exerce. Le second est celui que nous pouvons nommer « sous-surveillance » et qui se rapporte aux actions visant à créer un commun sur les pratiques des services étatiques de renseignement et des technologies qu'ils utilisent. Enfin, un dernier aspect, « l'equiveillance » qui consiste à articuler la surveillance et la sousveillance afin de produire un renseignement « par les foules », dans un contexte

[3] Depuis Twitter : https://twitter.com/NorthScope518/status/742759328235573248

numérique où chacune de nos actions, de nos données sont automatiquement collectées et traitées par les plateformes web.

La sousveillance comme panoptique inversé ?

Dans les premiers écrits de Steve Mann sur la sousveillance à la fin des années 1990, le chercheur ne fait pas que conceptualiser l'idée de « surveiller les surveillants » et réfléchir aux implications sociétales de ce panoptique inversé, il propose aussi de nouveaux dispositifs visant à la faciliter, comme des lunettes avec caméra intégrée. L'auteur relie ce qu'il nomme donc le « réflectionnisme » à la notion de détournement de Roger (1994), soit l'ensemble des tactiques d'appropriation des outils de surveillance (caméras par exemple) et la réutilisation de ces outils de manière désorganisée. Nous pouvons alors constater qu'aujourd'hui, ces caméras sont présentes dans de nombreux outils informatiques et de communication. Si les scénarios d'usages possibles de ces outils sont nombreux, les possibilités de braconnages, de détournements, à des fins de sousveillance le sont aussi. Le projet de Mann nous apparait comme clairement politique, au sens où il propose une forme de gouvernance de l'espace public qui s'appuierait sur la désorganisation des processus de contrôle social formel, par la multiplication des points de vue sur les actions des acteurs qui exercent au quotidien ce contrôle. A ce titre, lors des manifestations que nous citons en introduction, certains militants et journalistes ont mis en avant la nécessité de filmer les actions des forces de police afin qu'un « dérapage » ne soit « pas passé sous silence » (Figure 2).

Figure 2 : extrait de l'interview sur la chaine Public Sénat d'un photoreporter ayant couvert les manifestations contre « la loi travail »[4].

Comme l'illustre par ailleurs un journaliste de Libération à propos des manifestations du 24 mars 2016 devant le lycée Bergson de Paris : « *L'histoire* [des violences policières] *aurait pu s'arrêter là sans une vidéo postée sur les réseaux sociaux. Visionnées plus de 2 millions de fois, les images sont sans équivoque* (…). »[5].

Si cette sousveillance apparait aussi comme un recours juridique possible, une preuve de certaines exactions, sa médiatisation, l'attrait pour ces images (souvent violentes) spécialement sur le web et les réseaux socionumériques explique en partie leur multiplication. Ces images

[4] Source originale : https://twitter.com/publicsenat/status/738770747678543872

[5] « Bavures à Bergson : «Quand mon bras s'est lancé, il était trop tard», par I. Halissat, Liberation.fr, 19/09/16. En ligne : http://www.liberation.fr/france/2016/09/19/bavures-a-bergson-quand-mon-bras-s-est-lance-il-etait-trop-tard_1503133

sont en effet filmées du point de vue de l'individu qui est exposé à l'événement. Elles permettent de se mettre à sa place, d'obtenir des visions subjectives et multiples. Face à des chaines TV d'information en continue, la sousveillance telle que pratiquée dans des manifestations apparait comme une défiance, un regard sans filtre (si ce n'est celui automatisé des plateformes web) et donc potentiellement sans censure. L'identification à l'auteur des images semble plus aisée, puisque celles-ci peuvent être diffusées par un proche, ou par un contact sur un réseau social numérique. Pour autant, nous ne percevons pas cette sousveillance comme une forme de « journalisme citoyen » (Tétu, 2008). Si nous sommes bien face à une dé-médiation, au sens où le filtre médiatique « classique » est absent, de nombreux autres éléments de médiation propres au contexte numérique ont lieu : algorithmes des plateformes, médiations identitaires (Merzeau, 2012) et réputationnelles (Alloing, 2016). Pour nous, la mise en forme du renseignement menant à la production d'une information n'est pas effectuée par l'acteur de la sousveillance (celui qui diffuse les images), elle peut être effectuée par la suite par des journalistes ou par d'autres entités. Au contraire, cette forme de renseignement offre une multitude d'interprétations possibles, elle permet de donner accès à des images devenues conversationnelles sur le web (Gunther, 2014) et ainsi ouvrir le débat. Pour autant, on ne peut élaguer l'intentionnalité voire les idéologies des citoyens effectuant cette sousveillance, qui parfois peuvent s'organiser en réseaux ou associations afin de médiatiser au mieux les faits qu'ils jugent nécessaires de mettre en visibilité dans l'espace public.

Cette surveillance directe des forces de police se structure depuis 1990 aux USA avec le mouvement « copwatch », réseau d'associations militant pour la fin des violences policières, et aujourd'hui présent dans plusieurs pays dont la France. Le site *copwatch.com* s'accompagne d'une base de données et d'un forum permettant de mettre en ligne les films ou photos d'interventions jugées abusives, violentes voire illégales de la police. Mais ce site offre aussi de nombreuses informations quant aux règles régissant ces interventions ou aux recours juridiques possibles. Là où Mann supposait une forme de désorganisation due à des tactiques de braconnages non-concertées, en fait une non-centralisation, les « copwatchers » ont à leur disposition de nombreux conseils voire méthodes pour effectuer leur sousveillance. A titre d'exemple, l'ouvrage « Copwatch Handbook »[6] librement accessible en ligne, propose « *d'initier les gens aux principaux concepts de l'observation de la police* » (p.2). L'ouvrage propose ainsi un historique du *copwatching* (depuis sa naissance à Berkeley en 1990), ses objectifs, les lois qui régissent ou non ces pratiques (afin de protéger celui qui effectue la sousveillance), mais aussi un ensemble de tactiques, de conseils techniques, de codes radio de la police, ou encore de manières de réagir en cas d'arrestation.

La sousveillance telle que conceptualisée par Steve Mann peut donc être « citoyenne », au sens où elle est pratiquée de manière réactive par un individu étant face à une situation où les « surveillants » semblent aller au-delà de leurs prérogatives ou de la loi dans l'espace public. Mais elle est aussi organisée par des associations et autres structures non-étatiques afin de favoriser une forme de contrôle citoyen de l'espace public, tout en permettant à chacun de s'informer sur les pratiques de renseignement.

La sous-surveillance pour renseigner sur les structures de surveillance

[6] http://www.berkeleycopwatch.org/resources/Handbook_06.pdf

La sousveillance met au centre le point de vue de l'individu. Mais cette vision « par le bas » n'offre que des fragments des formes les plus visibles, directes voire extrêmes (car supposant des interactions physiques) de contrôle. L'auteur des images devient un surveillant qui ne participe qu'à un niveau minime à l'appréciation globale des modes de surveillance étatique et commerciaux qui s'installent durablement dans nos sociétés. En France, des associations et collectifs proposent alors de créer un commun sur le renseignement, de rendre accessible des informations s'intéressant aux structures mêmes qui permettent cette surveillance, qu'elle soit effectuée par des états par le biais de logiciels spécialisés, de manière quotidienne par des caméras de surveillance, ou encore que cette surveillance soit légitimée par l'évolution constante du cadre législatif. Ce que ces collectifs de citoyens nomment sous-surveillance consiste donc plus à fournir une vision d'ensemble des dispositifs (techniques et législatifs principalement) de surveillance, qu'à documenter les actions les plus visibles des surveillants.

Le site *sous-surveillance.net* se présente ainsi comme un « outil de lutte », et met à disposition une carte des caméras de surveillance de différentes villes de France. Le site accompagne par ailleurs n'importe quel individu souhaitant créer un site local pour cartographier les caméras de sa ville. Les cartes ainsi créées peuvent être alimentées par n'importe qui, sur l'idée du « crowdsourcing ». L'objectif nous semble ici moins tactique (éviter d'être filmé par ces caméras par exemple), que de fournir des éléments factuels et globaux venant alimenter une critique de la surveillance quotidienne.

Cette critique, motivée par la multiplication des dispositifs de surveillance, de lois liées au renseignement, et de révélation diverses de lanceurs d'alertes médiatisés (Julian Assange, Edward Snowden et d'autres), ne se limite pas à la recension des dispositifs de surveillance, mais vise aussi à devenir un outil du débat démocratique. Lors de la discussion et du vote de la « loi renseignement » en France, l'association *La Quadrature du Net* (en partenariat avec la *Fédération FDN* et le *French Data Network*) a ainsi créée le site *sous-surveillance.fr* afin de recenser les arguments gouvernementaux pour le déploiement de ce qu'elle qualifie de « surveillance totale » des citoyens. Ce site s'accompagnait par ailleurs d'un wiki[7] proposant diverses analyses des textes de loi, les positions sur la question de chaque député, ou encore des transcriptions des débats à l'Assemblée Nationale. Mais plus que produire de la transparence là où les services de renseignement étatique évoluent dans l'opacité, la mise en commun et en visibilité de ces informations ont été accompagnées d'actions concrètes : appels à des élus afin de connaitre leur position[8] et les inciter à ne pas voter la loi, organisation de manifestations, mise en ligne de bannières ou d'avatars en ligne pour dire non à la « loi renseignement ».

Là où la sousveillance joue sur l'affect des publics, les représentations qu'ils ont de la surveillance étatique et de ses acteurs de terrain comme les forces de l'ordre, la sous-surveillance se veut factuelle et apparait comme un outil démocratique offrant un commun nécessaire à la coordination d'actions citoyennes. L'objectif n'est plus de documenter au quotidien, mais de fournir une représentation globale et structurée de ce qui permet la surveillance des citoyens par leurs états (lois, dispositifs techniques). Pour autant, si la sousveillance et la sous-surveillance se dévoilent en premier lieu comme du renseignement sur

[7] https://wiki.laquadrature.net/Portail:Loi_Renseignement
[8] Voir : https://pad.lqdn.fr/p/PJLsenateurs

les pratiques de surveillance étatique, il parait difficile de ne pas interroger celle faite en continue par les acteurs commerciaux d'Internet et du Web.

La sousveillance en contexte numérique : une question de médiation

Facebook, Google, Twitter, Snapchat, etc. Ces plateformes Web sont depuis quelques années mises en lumière pour la collecte et le traitement continus des données personnelles et de l'agir de leurs usagers. Ainsi que le souligne Quesseda (2010, p56), cette surveillance s'appuyant sur des technologies numériques ordinaires a la particularité d'être invisible : « *le « surveillant » (qui n'existe plus en tant qu'entité individualisée) et le surveillé (qui n'existe plus en tant que tel, en tant qu'« anormal » isolé, surveillé ou surveillable) sont invisibles, tout autant que le dispositif de surveillance lui-même (composé de l'entrecroisement de multiples techniques)* ». Quesseda utilise lui-même le terme de « sousveillance » pour mettre en exergue le fait que les modes de surveillance actuels ne sont plus surplombants, ils ne sont plus « sur », mais sont « en », ils sont propres aux (ou permis par) les dispositifs sociotechniques que nous utilisons au quotidien pour communiquer et nous informer. Serions-nous alors dans une forme de sousveillance généralisée, au sens où nous sommes devenus les propres producteurs de notre surveillance en égrenant nos données personnelles en ligne ? Et que les premiers des surveillants seraient nos « amis » et contacts en ligne ? Cette hypothèse supposerait un libre arbitre éclairé quant à l'utilisation de ces dispositifs, mais de nombreux auteurs (Tubaro et al., 2013) soulignent que la question du consentement (suis-je au fait de ce que je donne ou de ce que l'on me prend ?) est primordiale. Les plateformes web brouillent les distinctions entre sphères publiques et sphères privées/intimes, et il est ainsi difficile (juridiquement mais aussi en termes de sociabilités) de circonscrire le surveillant : la plateforme ? Les publicitaires ? Les autres usagers ? Les services de renseignement qui collectent des données par ce biais ?

Dans son ouvrage « Voir et pouvoir : qui nous surveille ? » (2010), Jean-Gabriel Ganascia propose la notion de « Catopticon » afin de mettre en exergue cette sousveillance généralisée induite par l'utilisation des plateformes web. Il interroge ainsi une possible « equiveillance », soulignant la nécessaire recherche d'équilibre entre une surveillance en surplomb (modèle du panoptique de Foucault) et en dessous (catopticon). Ce possible équilibre ne peut néanmoins s'absoudre de la prise en considération centrale des dispositifs sociotechniques du Web comme médiateurs. Lorsqu'un militant ou un citoyen met en ligne une vidéo de manifestation, lorsqu'un autre participe à alimenter un site collaboratif de sous-surveillance, il fournit potentiellement des données personnelles permettant de l'identifier, de le tracer, ce qui n'est pas sans risques dans des états non-démocratiques et de manière générale pour sa vie privée (Lerch, 2014). Là encore, de nombreux collectifs se mobilisent afin de fournir des dispositifs sécurisés : *plugins* de navigateurs pour bloquer la captation de données personnelles, messageries cryptées, méthodes pour effacer ses traces numériques.

A la suite de Lessig (1999), il est nécessaire de rappeler que « code is law » : ce sont des acteurs privés qui édictent les règles d'usage de leurs plateformes, ce sont leurs programmes informatiques et algorithmes qui régulent les interactions, et ce sont leurs impératifs commerciaux qui dirigent leurs modes de gouvernances. Emergent alors les questions de « droit à l'oubli », de diffamation mais aussi de désinformation. Si les filtres de ces informations mises

en ligne sont algorithmiques et répondent à des impératifs privés, la sousveillance affaiblie son projet politique d'origine en prenant le risque de ne plus être qu'un « contenu » parmi d'autres, qui circule de manière automatisé dans des espaces régulés par des firmes privées.

De notre point de vue, il nous parait essentiel de développer une réelle éducation aux médias numériques afin de transformer les différentes pratiques de sousveillance et de sous-surveillance en réel outil de renseignement démocratique. Les dispositifs numériques que nous utilisons de manière ordinaire, et qui permettent ainsi des formes de braconnage du contrôle social, ne sont pas neutres. Si la sousveillance permet de fournir un autre regard sur les formes de surveillance, de documenter les structures étatiques ou privées les déployant, d'alimenter le débat démocratique sur les questions de renseignement et de vie privée, les médiations techniques qui favorisent le développement de ces débats dans l'espace public doivent être comprises de tous. Une culture du renseignement citoyen, qui associerait à la fois des questions éthiques et de culture informationnelle et technique, serait un projet envisageable pour assurer un équilibre entre une surveillance « du dessus » et une « du dessous ».

Bibliographie

ALLOING, C., *[E]réputation. Médiation, calcul, émotion*, CNRS Editions, Paris, 2016.

GANASCIA, J. G., *Voir et pouvoir: qui nous surveille? Un essai sur la sousveillance et la surveillance à l'ère de l'infosphère*, Le Pommier, Paris, 2009.

GUNTHERT, A., « L'image conversationnelle. Les nouveaux usages de la photographie numérique », *Études photographiques*, 2014, no 31.

LESSIG, L., « Code is law », *The Industry Standard*, 1999, vol. 18.

MANN, S., « Reflectionism » and « Diffusionism »: New Tactics for Deconstructing the Video Surveillance Superhighway », *Leonardo*, 1998, p. 93-102.

MANN. S., NOLAN, J., WELLMAN, B., « Sousveillance: Inventing and Using Wearable Computing Devices for Data Collection in Surveillance Environments », *Surveillance & Society*, 2002, vol. 1, no 3, p. 331-355.

MERZEAU, L., « La médiation identitaire », *Revue française des sciences de l'information et de la communication*, 2012, no 1.

MOINET, N., *Intelligence économique: mythes et réalités*, CNRS Editions, Paris, 2011.

QUESSADA, D., « De la sousveillance. La surveillance globale, un nouveau mode de gouvernementalité », *Multitudes* 2010/1 (n° 40), p. 54-59.

TETU, J-F., « Du « *public journalism* » au « journalisme citoyen » », *Questions de communication* [En ligne], 13 | 2008. URL : http://questionsdecommunication.revues.org/1681

TUBARO, P., CASILLI, A. A., SARABI, Y., *Against the Hypothesis of the End of Privacy : An Agent-Based Modelling Approach to Social Media*, Springer Science & Business Media, 2013.