Relations

RELATIONS

Les nouveaux habits de Big Brother

Maureen Webb et Catherine Caron

Numéro 776, janvier–février 2015

Contrôle social 2.0

URI : https://id.erudit.org/iderudit/73345ac

Aller au sommaire du numéro

Éditeur(s)

Centre justice et foi

ISSN

0034-3781 (imprimé)
1929-3097 (numérique)

Découvrir la revue

Citer cet article

Webb, M. & Caron, C. (2015). Les nouveaux habits de Big Brother. *Relations*, (776), 14–17.

Les nouveaux habits de Big Brother

La sécurité et la surveillance deviennent de plus en plus une obsession au sein de nos sociétés. Les affaires Snowden et WikiLeaks nous révèlent deux dystopies qui sont peut-être en voie de se réaliser : l'une où *l'État sait tout*, l'autre où *tout le monde sait tout*.

MAUREEN WEBB*

> « *We're going to fuck them all… crack the world open and let it flower into something new*[1]… »
> JULIAN ASSANGE

L'auteure, avocate et professeure adjointe de droit à l'Université de Colombie-Britannique, est l'auteure de *L'illusion sécuritaire. Fichage, torture… personne n'est à l'abri* (Écosociété, 2011)

Le soldat Bradley Manning tape un message électronique adressé à Julian Assange. Les lettres semblent surgir en éclats sur l'écran pour former les mots à mesure que Manning formule ses réflexions. On imagine l'écran trembler pour un moment tant cet instant est décisif : les deux hommes sont sur le point de rendre public sur le site Web de WikiLeaks, l'organisme médiatique à but non lucratif créé par Assange, le plus gros lot de documents provenant des départements d'État et de la Défense des États-Unis ayant jamais fait l'objet d'une fuite – 720 000 au total.

Bradley Manning écrit : « Hillary Clinton… des diplomates à travers le monde… vont faire un arrêt cardiaque lorsqu'un matin, ils se réveilleront… et découvriront qu'un dépôt complet de documents classifiés de politique étrangère est accessible… au grand public… cela a des répercussions sur tout le monde sur Terre. C'est de la diplomatie ouverte, de l'anarchie mondiale… *C'est beau, et horrifiant*[2]. »

Entretemps, inconnu de Manning et d'Assange, Edward Snowden, un jeune Américain qui travaillait pour un sous-traitant privé de l'Agence de sécurité nationale américaine (NSA) rassemble et organise méthodiquement, en écrivant des notes explicatives, quelque 1,7 million de documents classifiés concernant les activités de l'agence. Il révélera l'existence d'un système permettant aux États-Unis d'atteindre un pouvoir de surveillance quasi omniscient, « un système dont l'objectif est l'élimination de toute vie privée, à une échelle globale. De façon à ce que personne ne puisse communiquer électroniquement sans que la NSA ne soit capable de collecter, stocker et analyser cette information[3] ».

Les documents de Snowden, au sujet desquels Glenn Greenwald et d'autres journalistes écrivent depuis juin 2013, révèlent que la Cour de surveillance du renseignement étranger des États-Unis (FISC) a exigé par ordonnance que le géant des télécommunications Verizon remette à la NSA, *en gros et en vrac*, des millions de relevés téléphoniques appartenant à des consommateurs américains. Ils révèlent que l'Agence a un *accès direct* aux serveurs de neuf entreprises américaines majeures dont Google, Yahoo, Facebook, YouTube, Skype, Microsoft et Apple, et qu'elle regarde et écoute *le contenu* des courriels, vidéos, photos, messages dans les médias sociaux, données archivées, conversations sur Skype et autres applications du genre.

Les documents montrent même l'estimation que fait l'Agence elle-même de la quantité de métadonnées (le *qui*, *quoi*, *où* et *quand* des communications et transactions sur le Web) qu'elle a recueillies à partir des réseaux d'ordinateurs et de téléphones *partout dans le monde*. Des cartes et des relevés mensuels (97 milliards de documents en mars 2013 seulement) accompagnent le tout.

Des articles dans les journaux *Der Spiegel* et *O Globo* suivront en juillet 2013, confirmant que la NSA a espionné les métadonnées des populations de pays tels l'Allemagne et le Brésil, grâce à un programme qui met à contribution les partenaires étrangers des entreprises américaines de télécommunications. Un autre article a révélé que les câbles sous-marins qui relayent les communications téléphoniques et Internet mondiales à travers l'Atlantique et d'autres océans sont surveillés par une agence alliée de la NSA, le Service de renseignements électroniques du gouvernement britannique, *en collaboration avec la NSA et à sa solde*. Ayant pour nom de code « Opération Tempora », il s'agit d'un programme puissant qui intercepte à la fois métadonnées et contenus; il dispose de sondes attachées à plus de 200 câbles Internet sous-marins, chacune transportant des données à une vitesse de 10 gigabits par seconde.

> Les gens commencent ainsi à sentir viscéralement la « fin potentielle de la vie privée » – la fin de la pensée privée, de la conversation éphémère, de la liberté d'association.

Toujours en juillet 2013, l'un des outils les plus troublants de la NSA est révélé : il s'agit du système XKeyscore. Si un analyste dispose d'informations permettant d'identifier un individu – comme une adresse courriel ou IP –, il peut chercher dans le système entier de la NSA, qui inclut l'information collectée par les services de renseignement de l'Australie, du Canada, de la Nouvelle-Zélande, du Royaume-Uni et des États-Unis (alliance connue sous le nom de « *Five Eyes* »). Il aura ainsi accès au contenu et aux métadonnées d'à peu près n'importe quelle action faite par cette personne sur Internet, *en temps réel*. Aucun mandat n'est requis : l'analyste n'a qu'à remplir un formulaire en ligne. De la chambre d'hôtel où il s'était réfugié à Hong Kong, Snowden avait affirmé : « Moi ici, assis à mon bureau,

Jean-Pierre Rivet, *Mystère de la bonté*, 2013, feutre et craie sur papier

je pourrais mettre sur écoute n'importe qui, que ce soit vous ou votre comptable, ou bien un juge fédéral, voire même le président, si j'avais une adresse électronique personnelle[4]. »

À la fin de l'été 2013, les journaux révèlent que la NSA a percé les codes d'encryptage utilisés par des millions de personnes pour leurs courriels, leurs transactions électroniques et financières, et qu'elle a travaillé à affaiblir les standards internationaux en la matière. Pour quiconque écoute même sporadiquement les nouvelles, il est désormais clair que les États-Unis espionnent leur propre population et celle d'autres pays, et qu'aucune information électronique n'est nécessairement privée dorénavant. Dans un document coulé de la NSA, publié en novembre 2013, l'agence affirme elle-même que son objectif ultime est d'être capable d'avoir accès à ce dont elle a besoin « n'importe où, n'importe quand, concernant n'importe qui ».

DYSTOPIE

Ces lanceurs d'alerte que sont Snowden, Manning et Assange sont des messagers du futur. Ils révèlent deux dystopies aussi effrayantes l'une que l'autre et qui sont peut-être en train de se réaliser. La première est celle selon laquelle *l'État sait tout*, l'autre, celle où *tout le monde sait tout.*

Dans la dystopie annoncée par les révélations de Snowden, *l'État sait tout.* Le choc que provoquent ses révélations ne tient pas seulement du fait que l'État, apparemment, veut tout savoir, mais qu'il le peut désormais grâce à la vitesse avec laquelle la technologie s'est développée ces dix dernières années. Les gens commencent ainsi à sentir viscéralement la « fin potentielle de la vie privée » – la fin de la pensée privée, de la conversation éphémère, de la liberté d'association. La fin de « l'anonymat dans la foule » qui, comme le réalise notamment la jeune génération, était la condition dont dépendaient les libertés modernes et libérales. Or, une société où l'État espionne, collecte et scrute l'information, *pouvant y déceler tout et n'importe quoi*, promet un monde où la sécurité de l'État est accrue, mais au prix d'une sécurité et d'une autonomie personnelles grandement diminuées.

De manière contrastée, la dystopie que laissent présager Manning et Assange est celle d'un monde où *tout le monde sait tout* – ce qui inclut les entreprises, les employeurs, les voleurs d'identité, le crime organisé, les journalistes et n'importe quel autre individu qui, bien intentionné ou non, veut en savoir plus sur un autre individu. L'État a ouvert une véritable boîte de Pandore par son investissement dans la technologie, son affaiblissement intentionnel des standards d'encryptage et de sécurité sur Internet, son trésor de renseignements collectés. De ce fait, la sécurité personnelle et l'identité même des personnes se trouvent à la merci de forces (prédatrices ou simplement intrusives) qui dépassent l'État. Parallèlement, cela le place, ainsi que toutes les institutions sociales et politiques, devant une exigence de transparence absolue. Or, si la transparence est une valeur démocratique, il n'est pas certain qu'un État ou une institution puisse mener toutes ses affaires en totale transparence, en particulier en matière de relations internationales. Ils ont besoin d'une sphère protégée où réfléchir, débattre, négocier, élaborer et évaluer des politiques publiques, étudier des avis légaux, etc., tout en devant rester imputables pour leurs actions et soumis à la *Loi sur l'accès à l'information.*

Les États-Unis profitent ainsi de leur domination du cyberespace, mais compte tenu de l'avancée rapide des technologies et de ceux qui ont un intérêt financier à les

* Traduit de l'anglais par Catherine Caron.

1. « On va tous les baiser… faire éclater le monde et le laisser se transformer en quelque chose de nouveau… »
2. Cité dans Glenn Greenwald, *No Place to Hide*, Toronto, McClelland & Stewart, 2014.
3. *Idem.*
4. Glenn Greenwald, « *XKeyscore : NSA tool collects "nearly everything a user does on the internet"* », *The Guardian*, 31 juillet 2013.

Jean-Pierre Rivet, sans titre, 2012, encre sur papier

disséminer, d'autres États et acteurs non étatiques vont les suivre de très près. Il est facile d'imaginer le déclenchement d'une nouvelle course à l'armement cybernétique; une nouvelle écologie du secret et du mensonge, puisque plusieurs joueurs se disputent pour dominer les autres ou s'en défendre; une nouvelle économie avec de nouveaux joueurs, de nouvelles sortes de valeurs et de profits, de nouvelles formes d'exploitation.

En envoyant son courriel à Assange, Manning semblait sentir, avec effroi, à portée de main, le danger d'une telle déstabilisation rapide et radicale des rapports de pouvoir existants.

ANTICIPATION

Après le 11 septembre 2001, l'administration Bush a commencé à parler avec agressivité d'empêcher les attaques

La lucrative industrie des données personnelles

STÉPHANE LEMAN-LANGLOIS

L'auteur, professeur de criminologie, est titulaire de la Chaire de recherche du Canada en surveillance et construction sociale du risque de l'Université Laval

La multiplication des sources d'information et des services distribués par Internet, combinée au fait que l'architecture du «réseau des réseaux» n'a pas été conçue pour le commerce sécurisé, a obligé, au cours des dernières années, les multinationales du contenu en ligne à user de créativité pour générer des revenus. D'abord, l'espace publicitaire qu'on vendait jadis à fort prix, quand le téléspectateur était captif d'une poignée de services quasi monopolisés par quelques grands réseaux, a vu sa valeur dégringoler dans le cyberespace, où l'attention du visiteur moyen se compte en fractions de secondes. On l'a appris de façon abrupte lors de l'implosion de la première bulle «.com», à la fin du siècle dernier. Ensuite, la solution payante, ou le «*pay wall*», où l'usager paie pour le contenu ou le service qu'il consomme, ne fonctionne réellement que pour les sites extrêmement spécialisés ou pour ceux jouissant déjà d'une grande notoriété.

La tendance lourde est donc de «personnaliser» la publicité en ligne, c'est-à-dire d'investir uniquement dans les visiteurs les plus faciles à «convertir» en consommateurs: ceux qui ont déjà un intérêt pour les produits, les services ou l'information qui sont offerts. Cela implique donc qu'il faut connaître l'usager: observer ses actions, ses déplacements, son réseau. En construisant une base de données où sont décrites ces caractéristiques, on peut produire un profil de chaque consommateur, qui permettra d'identifier à la fois les produits qui peuvent l'intéresser et la meilleure manière de les lui vendre.

C'est ce système qui a donné naissance à des courtiers en données comme Gnip, Acxiom ou Datalogix, qui vendent les données de millions d'usagers d'Internet à des entreprises commerciales. Leurs profils sont fondés sur des informations glanées auprès des détaillants de biens, de services et d'information (en ligne ou non), des compagnies d'assurance, des vérificateurs de crédit, des fournisseurs de télécommunications, etc. L'usager, consciemment ou non, participe à la création de ces banques de données de plusieurs manières. Entre autres, en fournissant volontairement ses renseignements personnels pour obtenir une carte de fidélisation, ou simplement en donnant son code postal aux caissiers qui le demandent – ce qui permet aux courtiers de combiner des données existantes à son sujet.

C'est sans compter, bien sûr, les fournisseurs de services et d'information «gratuits» ou à faible coût comme Google

terroristes avant qu'elles ne puissent se produire. Dans le domaine de la sécurité publique et du renseignement, les agences n'ont plus mis l'accent sur la collecte d'information concernant des risques spécifiques, à l'intérieur de cercles précis, en développant des pistes d'action déterminées. Elles se sont plutôt mises à vouloir prédire qui d'entre nous tous pourrait être un terroriste, faisant de chacun un suspect potentiel. Selon cette logique, chercher des communications entre terroristes ressemble à chercher une aiguille dans une botte de foin; il vaut donc mieux avoir « toute la botte » (comme l'a avoué l'ex-directeur de la NSA, Keith Alexander). Ainsi, depuis 2011, affirmait le *Washington Post* dans une série d'articles intitulée *Top Secret America*, quelque 1271 organisations gouvernementales et 1931 sous-traitants privés travaillent à des programmes reliés au contre-terrorisme, à la sécurité intérieure et au renseignement dans quelque 10 000 sites à travers les États-Unis.

CORRÉLATION

Dans un article récent de *Foreign Affairs*, intitulé « *The Rise of Big Data* » (nº 28, mai-juin 2013), les auteurs observent qu'à travers la majeure partie de l'histoire, les outils pour recueillir, entreposer et analyser des données ont été déficients. Ce n'est que récemment que la perspective de rassembler des lots complets de données sur n'importe quel problème est devenue une réelle possibilité. Cette capacité est en train de transformer la pensée dans le domaine des sciences, des sciences sociales, des affaires et de la sécurité. L'idée de « *big data* » « est qu'en utilisant un vaste corpus d'information, nous pouvons comprendre des choses que nous ne pouvions pas saisir lorsque nous utilisions seulement de petites quantités d'information ». L'étude des corrélations en vient à remplacer l'étude des causes dans le travail d'enquête. Désormais, il n'est plus nécessaire d'établir les causes, les corrélations pouvant fournir tellement d'indications pour agir. La connaissance, « qui a déjà signifié la compréhension du passé, commence à signifier une habileté à prédire le futur ».

Clairement, l'obsession sociétale pour la sécurité et la surveillance n'est qu'un commencement. Notre capacité de réguler la surveillance et le *big data* – soit l'utilisation qui est faite de l'information et de l'étude des corrélations – déterminera largement si ce nouveau monde qui émerge se révélera magnifique – ou horrifiant. ●

et Apple, par exemple. En tant qu'écosystèmes de services, de contenus et d'appareils, ces firmes disposent de sommes gigantesques d'information sur leurs usagers, dont plusieurs sont disponibles en ligne, en temps réel. Google épluche ainsi les courriels qui sont envoyés ou reçus par son service de messagerie Gmail pour y trouver des mots clés sur nos intérêts et activités; Apple, de son côté, suit ses iPhones à la trace et vend leur localisation géographique à ses partenaires. Comme le dit l'adage, « si c'est gratuit, c'est que *vous* êtes le produit ». Du point de vue industriel, l'objectif de ce modèle d'affaires est le contrôle du comportement du consommateur.

Dans les faits, les résultats de cette publicité hyperciblée restent mitigés. Pour une foule de raisons, les consommateurs n'achètent pas assez pour en couvrir les coûts. Mais faisons un peu de futurologie : dans un proche avenir, nous devrions néanmoins assister à une escalade extrême dans la collecte de renseignements personnels. Tout simplement parce que l'industrie continue d'y investir massivement et de vendre le concept de la publicité ciblée aux acheteurs industriels. On suggérera sans doute d'améliorer le produit par davantage de ciblage, et donc davantage de surveillance. Si la stratégie ne fonctionne pas, il y a risque d'une nouvelle implosion de la bulle technologique. Si elle fonctionne, en revanche, la moindre de nos actions sera surveillée. L'avènement de l'« Internet des objets » fournira des outils d'une puissance sans précédent pour y arriver. Bientôt, *chaque* objet de notre quotidien communiquera des informations à des serveurs interconnectés sur lesquels nous n'aurons aucun contrôle ni droit de regard : réfrigérateurs, sièges de vélo, filtres de piscine et même l'entrée d'eau et la sortie d'égout de notre demeure. Sans compter les objets pour lesquels la transformation est déjà en cours, comme nos téléviseurs, nos thermostats, nos montres, nos serrures et nos compteurs d'électricité.

L'État viendra-t-il nous défendre contre ces outils intrusifs? Il est certain que non, pour deux raisons. La première est que, collectivement, nous continuerons sans doute à faire peu de cas de cette surveillance, qui nous apporte tant de bénéfices – coupons rabais, offres alléchantes, informations émoustillantes, etc. La seconde est que l'État cherche à profiter lui aussi de cette manne d'information. Plusieurs projets de lois récents au Canada, notamment C-13, dont certaines dispositions permettraient aux services policiers et gouvernementaux d'obtenir sans mandat des informations sur des internautes, démontrent aisément l'appétit toujours grandissant des institutions gouvernementales pour les renseignements accumulés par les industries de l'information. Et c'est sans oublier les révélations d'Edward Snowden…