Relations

RELATIONS

La lucrative industrie des données personnelles

Stéphane Leman-Langlois

Number 776, January–February 2015

Contrôle social 2.0

URI: https://id.erudit.org/iderudit/73346ac

See table of contents

Publisher(s)

Centre justice et foi

ISSN

0034-3781 (print)
1929-3097 (digital)

Explore this journal

Cite this article

Leman-Langlois, S. (2015). La lucrative industrie des données personnelles. *Relations*, (776), 16–17.

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…