Comment déjouer les dispositifs de surveillance ?

Lazaro, Christophe

Published in:
Kairos

Publication date:
2016

Document Version
le PDF de l'éditeur

COMMENT DÉJOUER LES DISPOSITIFS DE SURVEILLANCE ?

RUSES ET TACTIQUES DE RÉSISTANCE DANS LES ENVIRONNEMENTS NUMÉRIQUES

Face à l'émergence spectaculaire de technologies de plus en plus intrusives capables de collecter, d'analyser, de traiter des quantités gigantesques de données à des fins de profilage et de surveillance, les citoyens se trouvent de plus en plus démunis. Comment faire pour échapper au traçage permanent dans un contexte où les dispositifs techniques facilitent l'exploitation de données à l'insu des personnes ? Est-il réaliste d'attendre des citoyens qu'ils «gèrent» leurs données et assurent un contrôle sur leurs profils alors qu'ils manquent très souvent de la plus élémentaire familiarité avec les technologies qu'ils utilisent ?

Les débats contemporains autour de la vie privée et des données dites «personnelles» opposent à leurs extrêmes deux conceptions totalement contradictoires du pouvoir de l'individu à l'ère de la nouvelle «*gouvernementalité algorithmique*»[1] : ils consacrent, d'un côté, le fantasme d'un pouvoir absolu de l'individu autonome et responsable sur ses données ; de l'autre, le cauchemar d'une hétéronomie totale d'un individu passif et impuissant. Représentant les deux faces d'une même médaille, ces conceptions négligent de prendre en compte l'émergence progressive d'une variété de formes quotidiennes de résistance qui se déclinent à travers la mise en scène d'actions modestes, minuscules et fragmentaires[2]. Parmi les formes subtiles de contrôle situées dans cette zone grise entre autonomie et hétéronomie totale, il est en effet possible d'identifier une série de pratiques subversives procédant de ce qu'on appelle communément la ruse. Conscients des limites inhérentes aux processus de réglementation ou d'autorégulation pour répondre aux risques soulevés par la prolifération des mécanismes de profilage dans les environnements numériques, différents acteurs se sont organisés de manière plus ou moins formelle et ont développé ces dernières années un ensemble de projets destinés à déjouer ces mécanismes, à retourner l'arme de l'ennemi contre lui-même et à «traquer les traqueurs».

Ces projets visent à concevoir et diffuser sur Internet des outils techniques permettant à la fois d'informer les utilisateurs et de leur donner l'opportunité de résister aux mécanismes de profilage et de surveillance grâce à différents subterfuges. D'un point de vue technique, ces projets se manifestent généralement par leur grande simplicité. Ils ne s'appuient pas, ou que très rarement, sur le développement d'architectures techniques lourdes et complexes, comme les procédés de cryptographie. En outre, ils mettent à disposition des utilisateurs des logiciels ou des applications non seulement faciles d'usage, mais qui en plus ne nuisent pas au bon fonctionnement de leur machine. Ensuite, les outils mis à la disposition des utilisateurs par ces projets diffèrent dans leurs effets d'autres tactiques bien connues visant à garantir le secret ou l'anonymat. On pense par exemple à l'usage de plates-formes anonymes comme Tor[3]. Pour les protagonistes de la ruse, la disparition, le secret, l'anonymat ou le refus total ne sont pas vraiment des options. A celles-ci, ils préfèrent l'intelligence pratique et l'art de la tromperie.

La ruse est une notion faisant généralement référence à l'ingéniosité, l'inventivité et la créativité déployée dans des usages quotidiens. A ce titre, cette notion entretient un lien fort avec l'habileté, les gestes, les routines et les savoir-faire requis notamment pour développer et manipuler les objets techniques et les machines. Dans la littérature dédiée aux usages des médias ou des technologies de l'information et de la communication, cet «art du truc» ou du bricolage a été largement commenté pour décrire, par exemple, la virtuosité technique des développeurs de logiciels libres ou des pirates informatiques. Les développeurs participant aux projets que nous évoquons ici témoignent assurément des mêmes qualités. L'intelligence pratique caractérisant la *ruse* se décline ici à travers un premier mouvement tactique consistant, grâce à un procès de familiarisation avec les mécanismes de traçage et de profilage, à «trouver le truc» qui va permettre d'en exploiter les failles[4]. Il s'agit alors prioritairement d'ouvrir les «boîtes noires» algorithmiques, grâce à des procédés de rétroingénierie, pour en comprendre les rouages. Un tel rapport familier aux objets est justement ce qui fait très souvent défaut aux «utilisateurs ordinaires» dont les capacités et compétences semblent plus que limitées lorsqu'il s'agit d'une part de manipuler leurs machines, d'autre part de protéger leurs données. Dans leurs rapports quotidiens aux environnements et aux dispositifs numériques, la plupart des individus ordinaires s'engagent dans des routines maladroites, voire contradictoires, qui ne leur offrent pas de prises sur leurs données et peuvent s'avérer dangereuses. C'est ce que les différents protagonistes de ces projets s'efforcent de compenser en mettant à la fois leur virtuosité et leurs astuces au service des utilisateurs profanes.

L'intelligence pratique propre à la ruse se déploie alors à travers un second mouvement prenant la forme d'une «pédagogie de la ruse». Une fois les boîtes noires des mécanismes de traçage et de profilage *dé-faites*, on en dévoile le fonctionnement aux utilisateurs ordinaires. Dans cette perspective, ces différents projets ont pour ambition d'informer les utilisateurs et de mettre à leur disposition divers instruments (tels que des bases de données de cookies, des cartographies de traces, des systèmes d'évaluation des entreprises, etc.) permettant de mieux comprendre l'utilisation qui est faite de leurs données par les réseaux publicitaires, les fournisseurs de données comportementales, les éditeurs de sites web et autres sociétés qui s'intéressent à leur activités en ligne. Il s'agit en quelque sorte de promouvoir une éthique du *Do it Yourself* en révélant aux utilisateurs ordinaires trucs et ficelles afin de rendre leur expérience dans les environnements numériques plus sensée.

Au-delà de leurs vertus pédagogiques, n'oublions pas que ces différentes tactiques de résistance servent avant tout à tromper. Tel est le propre de la ruse. Or si celle-ci a pour objectif de jouer un (mauvais) *tour*, il faut avoir à l'esprit que les effets recherchés ainsi que les moyens peuvent varier. En effet, plusieurs artifices/artéfacts peuvent être utilisés pour différents types de mystifications.

Par exemple, certains de ces projets ont recours à ce que Brunton et Nissenbaum appellent l' «obfuscation» et qu'on peut définir comme la production et la communication de données trompeuses, ambiguës ou fausses dans le but de susciter la confusion et de rendre la collecte de données moins fiable et donc moins précieuse pour les agrégateurs de données[5]. Le projet TrackMeNot (TMN), notamment, propose une extension de navigateur (*browser extension*) ayant pour objectif de prévenir, ou du moins de limiter, le profilage exercé à travers les moteurs de recherches. Au lieu de recourir à des outils cryptographiques afin de couvrir les traces, TrackMeNot masque les requêtes des utilisateurs en s'appuyant paradoxalement sur la stratégie inverse : le bruit et l'obfuscation. Avec TMN, les requêtes réelles des utilisateurs sont cachées au milieu de recherches fantômes générées par le système et lancées sur les moteurs que les utilisateurs choisissent. En d'autres termes, TMN masque les recherches des utilisateurs dans une nébuleuse de fausses recherches afin de compliquer le profilage des utilisateurs et de le rendre inefficace. Dans le même ordre d'idées, le projet bien nommé Ad Nauseam clique automatiquement sur toute publicité préalablement bloquée et, ce faisant, enregistre une visite pour l'annonce concernée au sein des bases de données des réseaux publicitaires. Ce flux de clicks omnivore et ininterrompu révèle une absence totale de logique, rendant ainsi les données collectées inutilisables à des fins de profilage, de ciblage ou de surveillance. En simulant le comportement d'un utilisateur sans déguiser son identité et sans rendre ses données comme telles illisibles, ces logiciels visent à brouiller son profil en le «cachant dans la foule», en le noyant dans la masse.

D'autres projets développent des outils basés sur un modèle de ruse différent. Ils visent notamment à travestir l'identité des utilisateurs sur les réseaux sociaux. Le projet Undefined propose un outil permettant aux utilisateurs d'altérer automatiquement leurs identités sur les réseaux sociaux comme Facebook, Foursquare ou Twitter[6]. En utilisant cet outil, l'utilisateur accepte de laisser Undefined poster du contenu sur les réseaux sociaux et interagir à sa place avec les autres personnes. Ces actions peuvent être présélectionnées par l'utilisateur parmi une liste de différentes tactiques, censées permettre d'altérer les identités digitales qui sont la proie des algorithmes de surveillance. D'autres projets, comme Vortex[7], proposent notamment aux utilisateurs d'observer comment les algorithmes de profilage réagissent si on fait varier les entrées (inputs) de différentes façons, notamment en jouant avec les cookies. Encore à l'état de prototype, Vortex est une extension de navigateur, conçue comme un *data management game*, permettant aux utilisa-

(1) A. Rouvroy & T. Berns, «Gouvernementalité algorithmique et perspectives d'émancipation. Le disparate comme condition d'individuation par la relation ?», *Réseaux*, 2013/1 (n° 177), p. 163-196.

(2) G.T. Marx, «A Tack in the Shoe: Neutralizing and Resisting the New Surveillance», *Journal of Social Issues*, Vol. 59, No. 2, 2003, pp. 369-390.

(3) https://www.torproject.org.

(4) J. Pasteur, «La faille et l'exploit : l'activisme informatique», *Cités*, n° 17, 2004, pp. 55-72

(5) F. Brunton & H. Nissenbaum, *Obfuscation. A User's Guide for Privacy and Protest*, MIT Press, 2015. Voir aussi leur article disponible sur Internet en libre accès: «Vernacular resistance to data collection and analysis: A political theory of obfuscation», First Monday, Vol. 16, No. 5, 2 May 2011, http://firstmonday.org/ojs/index.php/fm/rt/printer Friendly/3493/2955.

(6) http://vincentdubois.fr/undefined.php

(7) http://www.milkred.net/vortex

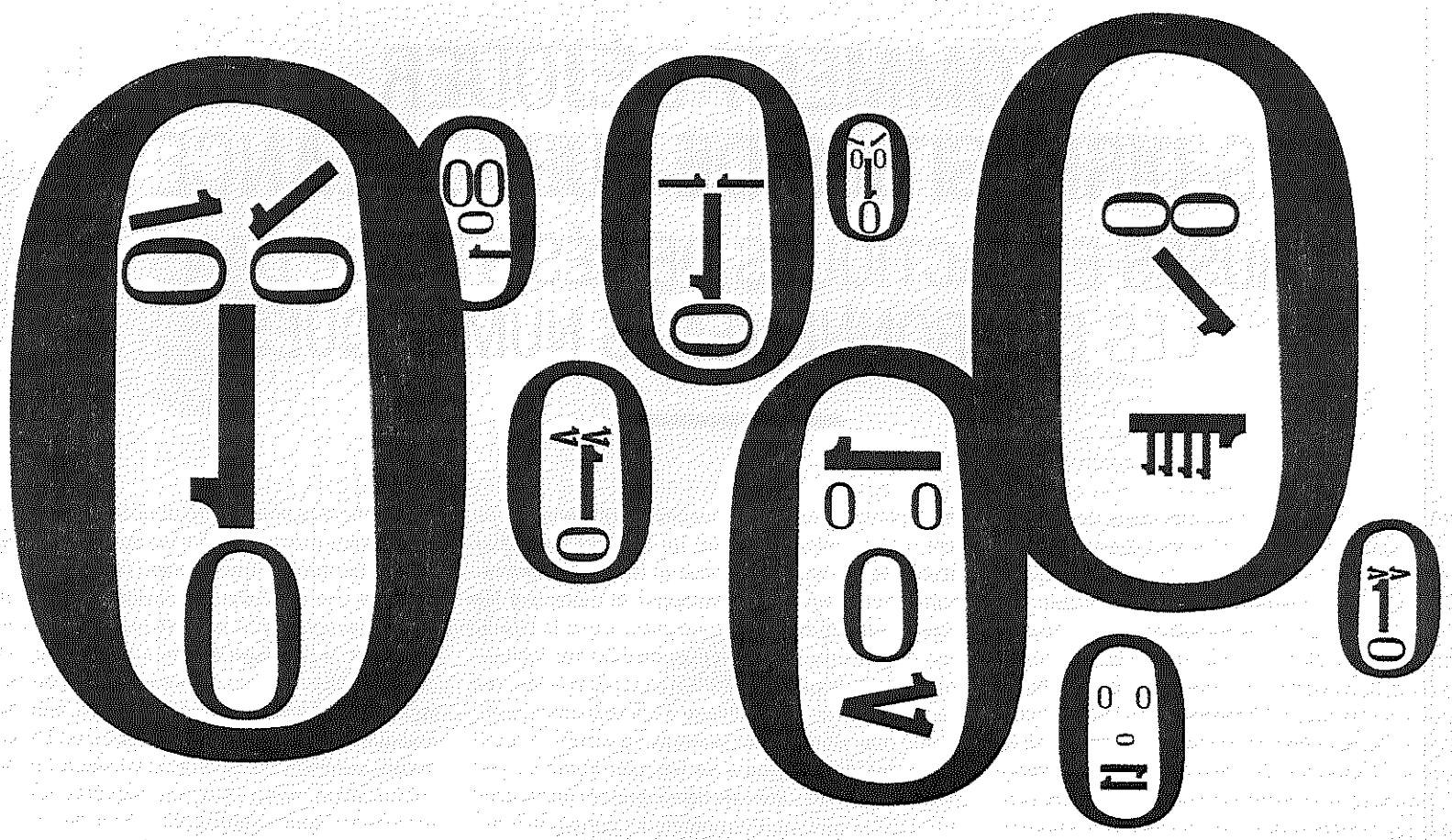

Illustration : Fabienne Loodts

teurs-joueurs de gérer leurs identités digitales en les invitant à échanger les cookies et à observer en temps réel les comportements de leur navigateur en fonction des cookies utilisés. Sur cette base, il devient alors possible de brouiller ses traces et de rendre le profilage moins aisé.

Obfuscation, simulation, diversion, blocage, camouflage… une réelle diversité de tours et de tactiques sont progressivement développés pour tromper les algorithmes traqueurs. Le registre sémantique utilisé par les protagonistes de ces projets lui, par contre, ne trompe pas : il relève de l'art de la guerre ou du combat[9]. La ruse, à travers les stratagèmes qu'elle met en œuvre, s'impose comme une arme servant à déjouer les plans de l'ennemi. Elle est une pratique de résistance qui se situe dans un rapport de force et tente de faire un bon usage des circonstances. La ruse se nourrit donc du conflit et de la rivalité par rapport à une rationalité qui prétend s'imposer sans discussion, fût-elle politique, économique ou techno-scientifique. Dans cette optique, l'engagement tactique et militant des acteurs développant ces différents projets les amène à concevoir des «*contre-artéfacts*»[9] destinés à compenser les situations d'asymétrie ou de déséquilibre structurel auxquelles les utilisateurs de dispositifs numériques (y compris eux-mêmes) sont confrontés en matière de collecte et de traitement de données. Les pratiques rusées qu'ils développent sont des formes de résistance visant à lutter contre la «tyrannie des données» engendrant des situations de faiblesse et de vulnérabilité qu'il s'agit de compenser autant que faire se peut.

Les pratiques rusées développées au sein de ces projets revêtent donc un caractère éminemment politique. En révélant les rouages des dispositifs techniques de profilage, ces projets mettent en évidence les formes spécifiques de subordination qui passent par les choses et qui aujourd'hui désarment particulièrement la critique. En particulier, ces projets mettent en évidence le fait que, dans les environnements numériques, les citoyens ne disposent pas de réelles prises qui leur permettraient d'exercer une éventuelle maîtrise sur leurs données. Alors même qu'on attend de la part du sujet qu'il (re)prenne le contrôle sur ses données, l'environnement dans lequel un tel contrôle est censé s'effectuer n'est absolument pas façonné en ce sens. Les seules prises qu'il offre à l'individu se révèlent être *in fine* les meilleurs moyens d'assurer son emprise. Ainsi en est-il notamment de la fameuse *user-friendliness* des dispositifs et des interfaces constituant le web 2.0, censée faciliter la participation, le partage, l'interactivité et l'autonomie. Les promesses d'aisance et d'interactivité ont inéluctablement comme contrepartie la cession consentie ou involontaire d'informations détaillées à des systèmes toujours plus performants de collecte et d'analyse de données[10].

Compte tenu des situations de déséquilibre profond dans lesquelles sont engagés les utilisateurs, les pratiques rusées, à travers leur «créativité tactique», visent prioritairement à «travailler» les choses afin de se les approprier et de les rendre habitables. Les réflexions de M. de Certeau sont à cet égard précieuses[11]. En effet, pour cet auteur, la tactique, entendue comme la ruse du subalterne, est une façon originale de traiter avec le pouvoir et d'accéder à des ressources. Cela renvoie à une façon de se mouvoir dans un espace qui n'est pas possédé en propre. Les «arts de faire» que nous avons examinés s'apparentent alors à des tentatives pour mieux «faire avec», des arrangements temporaires et provisoires, tirant parti des failles au sein d'un espace strié par des forces indéterminées et démesurées. Dans un tel espace, la ruse ne prémunit pas contre l'incertitude, ni ne garantit la révolution. Tout au plus offre-t-elle une variété d'options pour y naviguer, pour s'en arranger à travers des moyens permettant de rétablir une certaine forme de contrôle…

«*Arme du faible*»[12] visant à s'accommoder au mieux de l'ordre social et de la violence des choses, la ruse aborde la problématique de la vie privée sur un mode agonistique et, ce faisant, contribue à relativiser grandement les fantasmes contemporains sur le contrôle individuel des données. Dans un monde où il devient toujours plus difficile d'effacer ses traces, la ruse est-elle alors la seule solution qu'il nous reste ? L'arme de dernier ressort ? Accepter une telle issue nous semble dangereux car cela reviendrait à réduire trop rapidement l'homme à son animalité, à faire seulement de lui, comme disait Deleuze dans son célèbre abécédaire, un «*être aux aguets*»…

Christophe Lazaro

(8) Voy. aussi G. Deleuze, *Pourparlers* 1971-1990, Les Éditions de Minuit, (1999) 2003, pp. 229-239. Lorsqu'il forge le concept de «société de contrôle», G. Deleuze évoque la nécessité de «*chercher de nouvelles armes*»…

(9) B. Pfaffenberger, *Technological drama*, Sci. Technol. Human Values, Vol. 17, No. 3, 1992, pp. 282-312.

(10) M. Andrejevic, «Privacy, exploitation, and the digital enclosure», *Amsterdam Law Forum*, Vol 1, No 4, 2009, p. 6, http://amsterdamlawforum.org/article/view/94/168.

(11) M. de Certeau, *L'invention du quotidien*, tome 1 : Arts de faire, Gallimard, Paris, 1990.

(12) J. C. Scott, *Weapons of the weak: Everyday forms of peasant resistance*, Yale University Press, New Haven, CT, 1985, p. 29.

(13) http://www.urmesurveillance.com.

(14) https://cvdazzle.com.

(15) http://interventionsjournal.net/2014/03/13/artist-project-facial-weaponization-suite.

LISTE DES PROJETS

- **TrackMeNot**
  http://cs.nyu.edu/trackmenot/fr/
- **AdNauseam**
  http://dhowe.github.io/AdNauseam/
- **Privacy badger**
  https://www.eff.org/privacybadger
- **Undefined**
  http://vincentdubois.fr/undefined.php
- **Are we private yet?**
  http://www.areweprivateyet.com/
- **Adchoices**
  http://www.youronlinechoices.com/ie/your-ad-choices
- **FaceCloak**
  https://crysp.uwaterloo.ca/software/facecloak/
- **Disconnect**
  https://disconnect.me/
- **Vortex**
  http://www.milkred.net/vortex
- **Cryptagram**
  http://cryptogram.prglab.org/
- **Terms of Service; Didn't Read**
  https://tosdr.org/downloads.html

Certains projets revêtent une nature plutôt artistique. Les tactiques de résistance se déploient, par exemple, à travers l'élaboration des masques prothétiques ou des procédés de maquillage-camouflage visant à lutter contre les systèmes de reconnaissance faciale (le projet URME Surveillance[13], CV Dazzle[14], ou le projet Facial Weaponization Suite[15]). Dans ces différents projets, les visages sont défigurés, reconfigurés, voire effacés ; les vertus subversives du masque sont réhabilitées dans un rejet carnavalesque de la surveillance et de l'identification. D'autres initiatives, davantage consacrées aux environnements numériques, démontrent plutôt un caractère techno-militant.