Idéaux, activismes, censure et surveillance

à l'ère des média participatifs

14 août 2013

1. Introduction

Cette ère n'est pas toute jeune. Ces formes de censure et de surveillance non plus. Utopies et luttes, censures, surveillance et ripostes sont en constante expansion et reconfiguration. Depuis les débuts d'internet, les imaginaires, les alliances et les possibilités de contre-pouvoir se sont diversifiées, démocratisées. Par ailleurs, les pouvoirs menacés par ces formes médiatiques comprennent de plus en plus les risques associés à ces fuites, ces inscriptions, ces circulations, ces prises de parole. Ils ont exploré une panoplie de moyen d'exercer la censure et la surveillance en ligne. Les réponses et la riposte à la censure de l'internet se renouvellent et s'organisent, elles aussi. Dans quelles mesures ces ripostes permettent-elles une politisation globale plus critique et solidaire ?

2. Les imaginaires d'Internet

« We will create a civilization of the Mind in Cyberspace.
May it be more humane and fair than the world your governments have made before. »

John Perry Barlow, 1988

Bien que nés d'un projet de défense militaire, les premiers déploiement de l'Internet furent rapidement explorés par le réseau des universités Nord-Américaines comme un espace d'expérimentation humaine et communicationnelle chargé d'utopies sociétales. Mais le déploiement de l'imaginaire communautaire et libertaire qui a marqué la popularisation de ce réseau de réseaux tient surtout à son appropriation par la contre-culture Californienne (Fred Turner 2006). Beaucoup des pionniers du cyberespace y voient l'occasion de jeter les bases d'une nouvelle société, plus humaine, plus juste et plus égalitaire. Cet imaginaire d'internet (Flichy, 2002) se nourrit de nombreuses utopies libertaires et communautaires - mais aussi militantes et révolutionnaires. Pour comprendre ces formations à l'œuvre sur internet et sur le web, je propose d'observer les projections imaginaires et discursives, ou encore les métaphores utilisées pour décrire ce qui se vit et se joue sur l'internet. Aux origines, trois métaphores revenaient couramment: celle de la communauté, celle du réseau, celle de village global (et par extension, celle de la fracture numérique.)

2.1 La Communauté

Comme décrites par Anderson en 1983 dans son ouvrage phare : « L'imaginaire national » (*Imagined Communities*), les communautés dont les membres ne peuvent se voir en face-à-face régulier s'appuient et se nourrissent d'un imaginaire commun. Dans le cas plus particulièrement prégnant de l'imaginaire national, il est nourri à cet effet, à grand renfort de cérémonies, de rituels institutionnels et de monuments nationaux. Les communautés de l'internet s'inscrivent elles aussi dans des imaginaires collectifs, qui se veulent à l'opposé de l'idée de Nation. L'imaginaire communautaire d'internet se veut transfrontalier, ignorant les frontières et constituant de nouveaux territoires. Cela ne l'empêchera pas d'être au début majoritairement anglophone et Nord-Américain. Ainsi, comme le rappelle Cardon (2012) en revenant sur le livre de Turner (2006), l'imaginaire communautaire d'internet relevait d'une forme d'utopie de l'exil vers un monde plus juste. Mais il souligne que si *"[les pionniers d'internet] rêvaient d'une société réconciliée, universelle, abolissant les frontières entre les sexes, les âges et les catégories socioprofessionnelles [...] sociologiquement, [cet imaginaire] rassemblait une "communauté" américaine, hypermasculine, blanche et très diplômée. ».*

2.2 Le Réseau

La métaphore du réseau est tout d'abord empruntée à la forme de l'infrastructure technique supportant ses échanges. Internet s'appuie sur l'interconnexion d'un très grand nombre de réseaux. Son application fondamentale peut être décrite comme un facilitateur de transfert des informations digitales, depuis leur

point de départ jusqu'à leur destination, en utilisant un chemin adapté et un mode de transport approprié. Les réseaux sociaux avaient été étudiés bien avant l'invention d'internet et les caractéristiques de cette formation sociale nourrissaient déjà la compréhension du monde contemporain. Mais la forme de l'internet a permis de nourrir un imaginaire politique riche de projections tactiques, stratégiques et sociétales.

Selon Bennett (2003), le fonctionnement en réseau produit des idéologies plus faibles que celles propres aux communautés. En effet, un réseau peut rassembler des acteurs d'aspirations très différentes. Du point de vue des valeurs sociales, on pourrait dire qu'il n'y a pas de principe politique transcendant qui donne un objectif au réseau. Ce sont les projets qui le constituent ou l'agglomération de différents projets en différentes poches du réseau, qui, de façon ponctuelle, donne un sens et une organisation au réseau. Mais comme les réseaux permettent aussi la rencontre de plusieurs sphères hétérogènes, ils peuvent autant être antinomiques que créer des occasions uniques d'alliance spécifiques. Les lieux de discussions, les listes, les canaux ou les forums constituent des lieux d'articulation et de renouvellement des liens du réseau. Les discussions permettent de renforcer les anciennes connections et d'en former de nouvelles.

Cardon et Aguiton (2006) expliquent cependant qu'il ne faut pas nécessairement y voir une perte d'engagement politique mais une possibilité d'engagement dans des luttes plus diversifiées. Cette hybridation des engagements politiques et des critiques sociales est aussi un renouvellement des moyens d'action et de décision. Les activistes du réseau utilisent des outils de communication transversaux pour créer des ponts et des nœuds qui réunissent de nouveaux espaces-temps et génèrent des identités hybrides. Si le réseau constitue une forme d'intervention puissante, les membres du réseau peuvent également jouer de leur position dans le réseau-même, en jouant stratégiquement de la force des liens faibles, de position privilégiée de centralité ou de passage obligé. Finalement, Cardon et Aguiton notent que dans le réseau, le principe d'exclusion est l'invisibilité. Être ou ne pas être connecté définit l'extérieur et l'intérieur du réseau.

2.3 Le village global et le discours sur la fracture numérique

La dimension transfrontalière de l'imaginaire d'internet s'articule avec une conception renouvelée de l'identité planétaire. Du moins, c'est un imaginaire marquant pour la population Nord-Américaine et Californienne. Dans les années 60, les communautés hippies voyagent abondamment en Inde et au Népal. La télévision donne des images du monde entier. La NASA a produit une photo de la planète terre dans son entier (*Whole Earth*) vue de l'espace et le fondateur du *Whole Earth Catalogue* réussi à l'obtenir pour l'afficher en couverture du magazine papier de contre-culture Américaine. Il pensait que cette image pouvait être un puissant symbole, évoquant chez les gens un sentiment de destin partagé et de stratégie adaptative. C'est ce catalogue qui allait notamment servir d'inspiration aux premières communautés en ligne comme celle du WELL the *Whole Earth 'Lectronic Link*, qui avait débuté en 1985 sous le format d'un babillard électronique (*BBS*) accessible par une connexion téléphonique commutée.

La notion de « Village planétaire » ou de « Village global » nous vient du philosophe et sociologue Marshall McLuhan (1967), qu'il utilise pour qualifier les effets de la mondialisation, des médias et des technologies de l'information et de la communication. Selon lui, l'évolution de ces moyens de communication contribueraient à unifier l'ensemble des micro-sociétés en une seule. Il n'y aurait selon lui désormais plus qu'une culture, comme si le monde n'était qu'un seul et même village, une seule et même communauté « *où l'on vivrait dans un même temps, au même rythme et donc dans un même espace* ». La capacité, pour une personne, à récupérer des informations très rapidement en n'importe quel point de la planète (raccordé à un réseau) donnerait ainsi l'impression d'être dans le même endroit virtuel, dans le même village. Si l'on poursuit cette logique, la non connexion devient gage d'exclusion.

Dans la Société en Réseau, Manuel Castells décrit en détail la façon dont les outils de communication semblent favoriser une organisation sociale horizontale. Le réseau semble représenter une solution de pouvoir stratégique et puissante. Ainsi, l'informatisation de la société conduit a une fragmentation de la société entre les connectés et les non connectés. Cela conduit à une tension qui risque d'augmenter la fracture entre les promesses d'un monde hyper connecté et un tiers monde démunis ou désinformé. Pour faire face à cet enjeux, plusieurs initiatives se sont donc attelées à combler cette fracture numérique, en cherchant à initier les publics les plus enclins à l'exclusion. Parmi d'autres, George (2004) questionne l'emploi de cette métaphore et pointe les dimensions classicistes, colonialistes et consuméristes qui traversent cette lutte contre la fracture numérique.

3. Activismes d'internet au tournant du milliaire

J'avais l'habitude (Goldenberg 2011) de distinguer trois formes d'activismes caractéristiques de cette époque technologique, communicationnelle et médiatique que représente l'extension d'internet, à savoir les activismes technologiques, les activismes médiatiques et les activismes de l'accès. Ces trois formes d'intervention se compléteraient en s'attaquant à différents points du système et mobilisent différents types d'acteurs sociaux. Si les intérêts de ces trois groupes sont convergents, leur culture d'origine et leur vision du monde et des priorités tendent à diverger. Mon hypothèse était que ces trois activismes constituent une forme d'écosystème technicien aux apports complémentaires.

3.1. Techno-activismes

Cette première forme d'activisme s'attache à la liberté, à la transparence et au contrôle citoyen des technologies et des infrastructures technologiques. Elle a débuté bien avant l'existence d'internet et prend notamment ses sources dans la culture hacker.

Le terme *hacking* apparaît dans les années 1950 dans les communautés de radio-amateurs qui désignent par ce terme un bricolage créatif visant à améliorer le fonctionnement d'un système. Avant d'être un activiste, un *hacker* est un virtuose qui se délecte de la compréhension approfondie du fonctionnement interne d'un système, en particulier des ordinateurs et réseaux informatiques. C'est la fermeture de certains systèmes qui aurait forgé la politisation des premières communautés. Selon Steven Levy (1984) qui a retracé l'émergence des hackers aux États-Unis, ceux-ci partagent une éthique dont les principes seraient les suivants : toute information est par nature libre; l'autorité est contestable, la

décentralisation souhaitable; c'est le savoir-faire ou la prouesse qui légitime un hacker et non sa position sociale; les ordinateurs peuvent créer de l'art et de la beauté; ils peuvent aussi changer et améliorer nos vies. Beaucoup de hackers présentent ainsi cette pratique comme une philosophie plutôt qu'une virtuosité, une pédagogie de l'ouverture et du partage des connaissances qui dépasse l'univers technique pour devenir une forme d'être au monde. Pour distinguer le bon hacker (qui travaille à des fins morales) du mauvais hacker (qui cherche surtout à démontrer ses prouesses techniques en faisant intrusion dans des espaces privés pour obtenir des informations précieuses) certains ont utilisés le terme « crackers » (dépréciatif) , qui réduit la virtuosité à une prouesse seulement technique.

Une autre distinction contemporaine serait celle qui distingue le hacker de l'hacktiviste, ce dernier mettant ses talents technologiques au service de causes sociales, politiques ou militantes. Ainsi selon cybermilitant indien Harsh Kapoor, (1999) les guerres numériques ne concernent pas seulement la liberté sur internet. *« [Cyberactivistes] are clearly shifting the nature of the conduct of war. Computer failure can cause breakdowns of signals for power transmission, so defense strategists are increasingly spending time and money to figure ways of protecting computer networks, and of course seem equally interested in controlling and monitoring to intercept and also to interrupt these when needed to cause damage. »* En développant des stratégies visant à protéger la liberté d'internet, ils ont aussi participé à modifier la façon de mener des luttes sociales et politiques sur le terrain. De la même façon qu'une manifestation de rue peut bloquer la circulation dans une ville, les cyber-activistes peuvent bloquer et influencer la circulation des informations sur le web.

Plus ouvertement politique et social, le mouvement de l'informatique libre est initié en 1983 par Richard Stallman. Il repose sur les traditions de la communauté hacker, dans laquelle le partage et l'ouverture des systèmes techniques sont la norme. Mais Stallman y décèle un vide juridique et propose, avec l'aide du juriste Lawrence Lessig, de définir légalement, l'informatique comme un bien commun. Ils créent ainsi la première licence libre (la GPL) qui permet de proposer des logiciels exempts de secret industriel et pour lesquels la libre circulation du code source est garantie. Le mouvement du logiciel libre serait la fondation d'une société de la connaissance dans laquelle les outils utilisés au quotidien peuvent être partagés, étudiés et modifiés. Lessig (2000) voit dans ce mouvement la réponse politisée d'un monde fondé sur le code et le plus important travail pour la liberté observé depuis plusieurs générations qui place la liberté au centre de la société de l'information.

Autre instance importante dans l'histoire du techno-activisme, s'attaquant plus spécifiquement à l'usage d'internet, l'*Electronic Frontier Foundation* (EFF) est quant à elle une organisation non gouvernementale internationale à but non lucratif, fondée en 1990 aux États-Unis, en réponse à une série d'actions entreprises par le gouvernement Américain pour renforcer le cadre juridique de la participation en ligne. L'EFF a notamment démontré la méconnaissance des autorités à ce sujet et a lutté pour la protection des libertés civiles. L'EFF défend la liberté d'expression sur Internet en soutenant financièrement des défenses juridiques au tribunal, ainsi que des individus et des nouvelles technologies menacées par des poursuites infondées. Elle expose les malversations du gouvernement, lui offre aussi ses conseils, organise des actions politiques, fait de la diffusion de masse et prend en charge de nouvelles technologies qui préservent les libertés individuelles.

3.2. Mediactivismes

"Autonomous media are the vehicles of social movements. They are attempts to subvert the social order by reclaiming the means of communication. What defines these media, and makes them a specific type of alternative media, is that they, first and foremost, undertake to amplify the voices of people and groups normally without access to media. They seek to work autonomously from dominant institutions (…), and they encourage the participation of audiences within their projects. Media activists seek not only to provide a space for information that is an alternative to that which is found in mass media, but also to create media that breakdown hierarchies of access to meaning-making, therefore allowing those typically found at the grassroots to have a voice and to define reality."

Dubois et Langlois, 2005

Depuis la fin des années 1990 on a vu émerger des plates-formes de médias alternatifs et autonomes très politisées, le plus souvent supportés par des CMS, supportant des médias citoyens, alternatifs, autogérés. Les luttes de Seattle, en 1998, ont donné naissance aux premiers centres de média indépendant (*Independant Media Center, IMC*), qui permettaient de donner une alternative informationnelle à la version des médias de masses. Le réseau Indymédia allait constituer l'un des premiers réseaux d'information critique. Chaque nœud Indymedia s'appuyait sur un centre local, avec des politiques éditoriales propres à chaque contexte mais répondant globalement à des critères d'ouverture, et de discussion du contenu a posteriori. Fortement opposé à la censure, il s'agissait de trouver une politique éditoriale autorisant la participation du plus grand nombre tout en évitant une appropriation conservatrice, haineuse, sexiste, raciste.

Dans chacun des centres se développait une culture de la critique médiatique et éventuellement des pratiques inclusives d'éducation au journalisme citoyen et à l'écrit public. Cela impliquait généralement de nombreuses discussions et concertation en ligne et sur place entre participants, lecteurs mais aussi une compréhension des enjeux ayant trait à la responsabilité des hébergeurs supportant ces plate-formes. Ceux-ci constituaient en effet le lieu probable d'intervention de la censure étatique, soit par le biais d'une saisie de serveur, soit sous la forme d'une identification des éditeurs. Le travail bénévole allait produire des fatigues et des défections menant à un progressif épuisement du réseau.

Selon Granjon et Cardon, 2010, les plate-formes de médias alternatifs auraient ainsi laissé place à d'autres formes de médiatisation relayée par les réseaux sociaux plus rapides et diffus mais impliquant moins de concertation. La multiplication des médias sociaux aurait diminué l'importance de ces centres médias indépendant au profit d'une culture de la capture et de la diffusion informationnelle beaucoup plus rapide, mobile, quasi-instantanée. Ces pratiques médiatiques impliqueraient une population plus large mais risqueraient de fragmenter le discours critique au gré de l'individualisation expressive et de mobilisations plus ponctuelles et superficielles.

Dans ce contexte, faisons-nous face à un affaiblissement ou à une réorganisation des mobilisations informationnelles? Quelles sont les formes sociales qui émergent de ces nouvelles pratiques de critique médiatique? Permettent-elles de contourner les formes de censure propres à cette nouvelle ère ?

3.3. Activismes de l'accès

Les activismes de l'accès du début du siècle répondent notamment à cette utopie communautaire et planétaire et aux inquiétudes des effets de la fracture numérique. En 1999, l'ITU[1] produit un discours sur l'internet comme projet de développement (*Internet For Development*). Certaines initiatives consistent ainsi principalement à équiper ou connecter des populations considérées comme démunies ou défavorisées. La vision sous-jacente est qu'un citoyen connecté aura plus de chance de s'émanciper en pouvant rejoindre le paradis égalitaire de la société (et des autoroutes) de l'information. Dans les années 2000, on voyait surtout se multiplier les efforts pour développer des ordinateurs simplifiés, libres, ouverts, robustes et bon marché (comme le *Simputer* en Inde, le *One Laptop Per Child* ou OLPC développé par le MIT) permettant aux populations les plus marginalisées (les paysans, les enfants des pays défavorisés) de participer activement à cette société de l'information. Mais beaucoup de ces projets sont emprunts d'une idéologie développementaliste, qui pose la technique comme voie d'émancipation sociale, économique, politique, sans compréhension sensibles des enjeux locaux.

Des initiatives plus ancrées dans le tissu social ont surtout travaillé à associer une appropriation des technologies numériques avec une forme d'alphabétisation aux pratiques numériques et aux formes d'intervention en ligne. Au Québec, citons par exemple le travail du CDEACF[2], qui associe alphabétisation, autonomisation des adultes et apprentissage de la culture numérique. Ou encore les projets menés par Communautique[3], qui travaille depuis les années 80 à l'éducation et l'autonomisation des groupes communautaires Québécois en matière de communication numérique.

Plusieurs collectifs et initiatives ont fait émergé un discours critique anti-colonial et anti-développementaliste, comme le projet *Cybermohohalla*[4] (cybervoisinage) à New Delhi, qui visent à proposer des *Medialab* communautaires dans les bidonvilles. On y parle hindi, on y exprime un être au monde, un être en ville, un rapport à l'urbanisme, avec des technologies libres, ouvrables et *low tech*.

4. L'émergence d'un Web « participatif »

Parallèlement à ces efforts d'inclusion sociale, la commercialisation des outils mobiles et la diffusion des applications de réseaux sociaux allaient reconfigurer les formes et les logiques de la participation en ligne. Le Web 2.0 désigne l'ensemble des techniques, des fonctionnalités et des usages qui se sont développé à partir des années 2003-2004. Elle désigne une évolution du Web vers une forme de simplicité nécessitant moins de connaissances techniques et informatiques de la part des utilisateurs. Elle s'appuie sur une forte participation et une forte interactivité (permettant à chacun, de façon individuelle ou collective, de contribuer, d'échanger et de collaborer sous différentes formes).

Les internautes contribuent à l'échange d'informations et peuvent interagir (partager, échanger, etc.) de

1 http://www.itu.int/ITU-D/ict/publications/inet/1999/
2 http://www.cdeacf.ca/
3 http://www.communautique.qc.ca/
4 http://www.sarai.net/practices/cybermohalla

façon simple, à la fois avec le contenu et la structure des pages, mais aussi entre eux, créant ainsi ce qui est aussi appelé le Web social. L'expression « Web 2.0 (Oreilly, 2005) s'appuie sur des principes-clés : le Web est conçu comme un réseau de plate-forme interconnectée; Il s'appuie sur une architecture participative; L'innovation s'appuie sur l'assemblage de systèmes et de sites distribués et indépendants ; Le modèle économique s'allège en s'appuyant syndication de contenu et de services ; Les logiciels n'ont plus besoin de cycle d'adoption (on sort de l'ère de la « la perpétuelle version bêta»).

Or, dans cette configuration de participation généralisée sur des applications commerciales pré-formatées, l'usage d'internet semble loin du rêve d'une contre-culture et encore plus des trames techniques et médiatiques de la formation d'un contre-pouvoir. Pourtant les années 2010 semblent être plus que jamais, marquées par la censure et la surveillance d'internet. Dans quelle mesure une critique du monde social et une lutte numérique est-elle encore possible ?

5. Censure et surveillance à l'ère du Web 2.0

5.1. Censurer le Web

Internet n'a techniquement aucune frontière géographique ou politique. Un réseau de réseau de libre circulation, cela peut poser un problème à bon nombre de gouvernements. Pour l'utilisateur final un site peut-être hébergé dans le même pays ou à l'autre bout du monde, cela ne fait aucune différence.

La censure sur Internet peut s'expliquer par de nombreuses raisons[5]. Elle s'inspire des espoirs de rétablir des frontières institutionnelles ou géographiques. Elle peut avoir des raisons politiques **:** les gouvernements veulent censurer les points de vue et opinions contraires aux leurs. La censure peut se donner des raisons sociales : les gouvernements veulent censurer les pages Web relatives à la pornographie, aux jeux d'argent, à l'alcool, aux drogues, et tout autre sujet qui pourrait nuire ou être choquant pour la population. Le plus souvent, sont invoqués des raisons de sécurité nationale : les gouvernements veulent bloquer le contenu qui menace la sécurité nationale, ce qui incluse généralement des contenus associés à des mouvements dissidents. Les institutions peuvent user d'une pluralité de moyens de censure.[6]

5.1.1 Mesures techniques

Pour être consultable, un site doit être hébergé sur un ou plusieurs serveurs (ordinateur connecté en permanence), son adresse doit être enregistré dans une base de donnée de nom de domaine (DNS) et associé à un numéro (ou adresse IP) et à une adresse internet (URL).

Un des premiers moyens de censure (depuis longtemps utilisé par la Chine notamment) est le filtrage des noms de domaine (DNS), c'est à dire des adresses enregistrées sur une base de données internationale. Si le registre national des DNS est configuré pour bloquer l'accès à certains sites, il

5 Cette classification suivante est adaptée de l'Open Net Initiative http://opennet.net/

6 Cette section est largement inspirée de FLOSS Manuals 2011, *Comment Contourner La Censure Sur Internet.*

définis une liste noire des noms de domaines bannis. Lorsque le navigateur demande l'adresse de l'un des domaines figurant sur la liste noire, le serveur DNS donne une réponse fausse ou ne répond pas du tout.

Un autre moyen de bloquer l'accès à des informations sur le Web est de bloquer l'URL (l'adresse internet) d'un site web. Le filtrage par URL peut être effectué localement, par l'utilisation de logiciels spéciaux installés sur des ordinateurs (comme ceux d'un cybercafé par exemple qui bloqueraient l'accès à certains sites), à par un point central du réseau, via un serveur proxy forçant ou encourageant les utilisateurs à passer par ce filtre.

Si les censeurs veulent empêcher les utilisateurs d'accéder à certains serveurs qui hébergeraient des sites Web contentieux, ils peuvent aussi configurer les routeurs qu'ils contrôlent afin que ceux-ci jettent, ignorent et abandonnent les données destinées aux adresses IP censurées. Ce mode filtrage basé uniquement sur l'adresse IP bloque tous les services fournis par un serveur donné, par exemple à la fois les sites Web et les serveurs d'e-mails.

Un contrôle plus fin est possible. Les données envoyées à travers Internet sont groupées en petites unités, appelées paquets. Le contenu des paquets peut être inspecté à la recherche de mots-clefs bannis. Comme les routeurs réseaux n'examinent normalement pas tout le contenu du paquet, un dispositif supplémentaire est nécessaire appelé DPI (« *Deep Packet Inspection* » ou « Inspection des paquets en profondeur »). Une communication où serait identifiée du contenu prohibé pourrait être coupée en bloquant les paquets directement où en créant un message pour dire aux deux interlocuteurs que l'autre a terminé la conversation.

Une autre technique, qui s'applique à l'ensemble du réseau est celle de la latence des flux. Elle peut-être utilisée par les gestionnaires d’un réseau pour fluidifier le réseau en priorisant certains types de paquets et en retardant d'autres types de paquets correspondant à certains critères. Si les censeurs veulent restreindre l'accès à certains services, ils peuvent aisément identifier les paquets liés à ces services et accroître leur latence en leur donnant une priorité faible. Cela conduit les utilisateurs à l'impression trompeuse que le site visité est lent ou peu fiable, ou cela peut tout simplement rendre le site défavorisé d'usage peu agréable comparé à d'autres sites.

Dans les cas extrêmes, les gouvernements peuvent décider de couper leur population de l'accès à Internet. Cette mesure est généralement perpétrée par des États en réponse à des événements politiques et/ou sociaux brûlants. Toutefois, la rupture complète des communications du réseau, aussi bien domestiques qu'internationales requiert un travail intense, puisqu'il est nécessaire de couper non seulement les protocoles qui connectent le pays au réseau international, mais aussi les protocoles qui connectent les Fournisseurs d'Accès à Internet entre eux et avec leurs abonnés. Des pays ont déjà complètement coupé l'accès à Internet (le Népal en 2005, la Birmanie en 2007, l'Égypte, la Libye et la Syrie en 2011) comme moyen de réprimer une agitation politique. Ces coupures ont duré de quelques heures à plusieurs semaines, bien que quelques personnes aient réussi à se connecter par l'intermédiaire d'un fournisseur d'accès étranger, ou en utilisant des accès de téléphonie mobile ou un lien satellitaire.

5.1.2 Mesures envers les éditeurs de contenu

Les censeurs peuvent également essayer de supprimer le contenu et les services à leur source en s'attaquant à la capacité de l'éditeur à publier ou à héberger l'information. Ceci peut être accompli de plusieurs façons : on édictant ou en appliquant des restrictions légales, en forçant les hébergeurs à dés-enregistrer un nom de domaine, à fournir les données d'identification des éditeurs ou plus radicalement, en procédant à une saisie de serveur. En effet, les serveurs hébergeant du contenu sont nécessairement localisés quelque part, tout comme l'administrateur qui les gère. Si ces endroits sont sous le contrôle légal ou extra-légal de quelqu'un opposé au contenu hébergé, le serveur peut être déconnecté, ou les administrateurs contraints de le désactiver.

5.1.3. Mesures envers les utilisateurs

Finalement, les censeurs peuvent aussi essayer de décourager les utilisateurs de ne serait-ce qu'essayer d'accéder au contenu banni de plusieurs manières. Les mécanismes ci-dessus empêchent d'accéder à un contenu banni, mais ils sont à la fois grossiers et faillibles. Une autre approche, qui peut être appliquée en parallèle au filtrage, est de surveiller les sites Web visités. Si un accès à un contenu prohibé est détecté (ou une tentative d'y accéder), alors des mesures légales (ou extra-légales) pourraient être utilisées comme représailles. Si la répréhension est connue, elle pourrait décourager d'autres de tenter d'accéder aux contenus bannis, y compris si les mesures techniques pour empêcher l'accès sont insuffisantes. Dans certains endroits, les censeurs essaient de créer l'impression que leurs agents sont partout et que tout le monde est surveillé en permanence, que ce soit le cas ou non.

5.2. Surveillance

"If you're doing nothing wrong, you have nothing to hide from the giant surveillance apparatus the government's been hiding."

Stephen Colbert[7]

Comme la censure est une approche visible et que des techniques et des solidarités de contournement, la surveillance semble faire ces preuves, seulement un moyen d'intimidation. Au contraire, plusieurs gouvernement et entreprises bien plus ont intérêt à utiliser la surveillance de manière discrète, afin de suivre les pratiques, déplacement, associations, action des utilisateurs de ces médias participatifs.

Cette approche est d'autant plus facile que de plus en plus de services sont fournis par des entreprises commerciales qui font leur profit sur la revente de données personnelles. Par ailleurs, les médias sociaux et les applications mobiles sont toute à fait accordées a un suivi des données des utilisateurs.

La surveillance est donc plus efficace et plus discrète que la censure. À condition que les usagers et les citoyens concerné.e.s l'ignorent, ou mieux, qu'elles et ils se laissent convaincre que celle-ci se fait pour leur bien.

C'est ainsi qu'aux yeux du grand public, les révélations des activités de surveillance de la NSA

7 cité par Philippe de Grosbois dans quelques remarques sur la NSA http://www.ababord.org/spip.php?article1654#nb1

semblent à la fois banales et scandaleuses. Banales, parce qu'on s'habitue vite au fait d'être surveillé, pour notre bien, notre sécurité ou pour nos intérêts (commerciaux par exemples). Les caméras de surveillance ont envahis le quotidien de nos déplacements depuis longtemps déjà. Nous avons bien remarqué que nos achats et nos navigations sont observés, vue le caractère délicatement ciblé des publicités que nous recevons ou qui s'affichent dans nos navigateurs. Nous pouvons facilement imaginer que nos communications téléphoniques sont géo-localisables, que nos GPS sont traçables, nos échanges lisibles et nos historiques de vie enregistrées. Nos média sociaux affichent déjà beaucoup de ces informations à la vue de tous. La bureaucratie de nos pays, de nos frontières, de nos institutions possèdent déjà toutes ses données sur nous. Nous leurs fournissons régulièrement, de plus en plus souvent et de plus en plus complètement, associant à ses données personnelles des données biologiques (dossier médicale, empruntes digitales, photo rétinienne, DNA...).

À quoi bon s'alarmer ? À quoi bon vouloir encore cacher quelque chose ou quoique ce soit ? Qu'a bien pu révéler le scandale de la NSA? Je reprend les mots de Philippe de Grosbois,2013[8] qui résume bien ce que la nature de ses révélations :

Si vous n'avez pas suivi cette affaire, on y a appris :

que la NSA collecte de la part de la compagnie téléphonique Verizon les méta-données de tous ses clients américains (les méta-données sont les informations qui entourent la conversation elle-même : les personnes contactées, le moment, le lieu et la durée de la communication, etc.). Elle fait probablement de même avec d'autres compagnies téléphoniques ;

que la NSA a accès aux serveurs des corporations Microsoft, Yahoo, Google, Facebook, Apple, Skype et d'autres pour y puiser des informations auprès d'usagerEs à travers le monde, tels que le contenu des courriels, le transfert de fichiers, l'historique de recherche, les chats, etc. ;

que le GCHQ britannique interceptait les communications de déléguéEs étrangerEs lors du G20 tenu à Londres en 2009 (y compris de déléguéEs de pays alliés), allant même jusqu'à construire de faux cafés internet pour intercepter leurs courriels ;

que ce même GCHQ s'abreuve à même 200 câbles de fibre optique pour amasser au moins autant d'informations que la NSA sur l'usage d'Internet par des citoyenNEs du monde entier.

Pourquoi la révélation de la surveillance opérée par la NSA fait-elle scandale ? Est-ce parce-qu'elle révèle des collaborations internationales inimaginées qui nous font réaliser la préciosité de nos données personnelles ? Est-ce parce-que cette surveillance dépasse certaine frontière étatique et qu'elle transgresse certaines limites diplomatiques ? Est-ce parce-que cette surveillance centralise des données ou des méta données à une échelle encore mésestimé ? Pourquoi poursuivre Edward Snowden, l'auteur de ces révélations pour espionnage, alors qu'il a justement révélé une immense affaire d'espionnage ?

8 Ibid

6. Ripostes

« The most fundamental mythology of the Net goes like this. The Internet was built to withstand bomb outages. Therefore, it can withstand anything. Defy authority. Whee! »

Wendu Grossman, 2011

Par rapport aux années 2000, l'internet des années 2010 est donc devenu plus participatif, plus multiculturel et plus dynamique. En même temps il n'a jamais autant été censuré et surveillé. Comment la critique et la riposte s'organise-t-elle dans cette nouvelle configuration technique, politique et culturelle ? Quelles sont les nouvelles figures de l'activisme technologique et informationnel contemporain ? Dans quelle mesure et dans quels contextes les hacktivistes vont-ils défendre des luttes sociales et politiques dépassant leur besoin et intérêt propre? Par quelles métaphores viennent-ils rendre visible et exprimer leur modus operandi?

6.1 Techno-activisme

"The Net interprets censorship as damage and routes around it."

John Gilmore, 1993

L'augmentation des possibilités de censure et de surveillance ont amené les militants du web à redoubler d'effort pour défendre les valeurs libertaires qui leurs sont chères. Une des figures les plus marquantes de cette mobilisation est celle d'Anonymous, un groupe d'activistes qui œuvrent dans l'anonymat pour (r)établir la justice sur le web et via le web. Face à cette être de surveillance totalitaire, il s'agit donc de confronter et de relever les défis de « l'assimétrie informationnelle » :

« *Dans le langage économique, cette notion indique une situation dans laquelle un agent dispose d'informations pertinentes sur un autre qui, lui, n'en a aucune. Ainsi, pour renverser cette nouvelle forme de domination immatérielle, il faut imposer un maximum de transparence aux puissants de l'Internet (entreprises, États, agences, banques, etc.) et, dans le même temps, la reconnaissance, la promotion et la protection du droit à l'anonymat pour les individus.*»

Christophe Ventura, 2013

6.1.1 Anonymous ou la nuée

Anonymous est à l'origine une communauté d'utilisateurs qui se coordonnaient sur internet pour réaliser des farces sur des sites internet. Ils partagent une culture d'un humour autant virtuose que cynique et prennent plaisir à empêcher le web de tourner en rond, et se reconnaissent dans la pratique du “lulz," (une pluralisation déformée de *laugh out loud (lol*)). C'est à partir de 2008 qu'un regroupement d'Anonymous s'engage dans des actions a caractère politique en protestation contre les abus de la Scientologie : Anonymous diffuse des vidéos confidentielles puis organise une série de manifestation publiques au travers le monde. En 2010, Anonymous se fait connaître dans leur soutien à Wikileaks en

attaquant les services Paypal et Mastercard qui avait bloqué leurs services de paiement pour le site. Cette opération distribuée d'attaque de site web (DDoS) donna la première couverture médiatique des talents spectaculaires d'Anonymous. Au Canada, une aile d'Anonymous se fait connaître en retrouvant en l'espace de deux jours, les auteurs du viol de Rehtaeh Parsons et que la police n'avait jamais recherché malgré les demandes de la victime qui s'est suicidée au printemps 2013.

Anonymous constituerait les nouveaux justiciers du Web. Des justiciers masqués qui travaillent laborieusement à leur mystère, associant l'anonymat des citoyens à l'une de leur revendication politique. Toutes les actions d'Anonymous n'ont pas un caractère politique mais elles ont la puissance d'un groupe d'intervention armée de la force de la multitude. Selon son motus : "Anonymous est légion. Anonymous ne pardonne pas et n'oublie pas". C'est la riposte du nombre face à l'ère totalitaire de surveillance, d'opacité et de censure. C'est la réponse collective à l'injustice, à l'oubli, à l'ombre douteuse. Contrairement aux communautés, cette forme n'implique pas d'affiliation longue. Contrairement aux réseaux, les liens sont invisibles.

Et c'est dans cette libre association qu'un accord ponctuel sur un objet d'action permet une intervention spectaculaire et limitée dans le temps. Anonymous ne porte pas d'identité collective, alors c'est la loi du nombre ou la force de convection des fluides qui guidera le geste. La nuée est certainement l'une des formes de riposte les plus efficace à cette ère de la surveillance. On doit croire à l'intelligence des foules. On peut craindre cependant que l'agrégation rassemble aussi des masses stupides et surtout imbues de leur puissance, révèlent les informations individuelles d'innocents, s'attaque à une cible plus spectaculaire que menaçante ou problématique. On peut ainsi se demander dans quelle mesure est inclusive. A quelles conditions peut-on influencer la nuée? Qui prend part aux choix des attaques ?

6.1.2 Tor ou le web incognito

Un des technologies phare pour l'esquisse de cette surveillance est le réseau Tor, qui permet aux utilisateurs de cacher leurs adresses IP et donc leurs coordonnées géographiques. Ce réseau mondial décentralisé de routeurs est organisés en couches, appelés nœuds de l'oignon, dont la tâche est de transmettre de manière anonyme des flux d'information utilisant le protocole TCP. Le projet permet aussi de fournir un ensemble de services cachés, comme la publication de sites web en cachant l'identité du serveur qui les héberge. Mais son usage est controversé : si l'anonymat fourni par Tor est bien reconnu comme une condition primordiale aux militantismes et journalismes qui utilisent internet, il a beaucoup été critiqué pour soutenir un réseau d'impunité et favoriser le déploiement d'actes illicites comme des réseaux de pédophilie. Le réseau permettrait aussi aux gouvernements ou aux sociétés privées de surveiller ou d'espionner leur population en limitant la possibilité de se faire détecter.

6.2 Mediactivismes

6.2.1 Les réseaux sociaux : la démultiplication des relais et des filtres

À l'opposé de ces pratiques de dénonciation soigneusement camouflées et anonymisés, les réseaux sociaux commerciaux (Facebook et Twitter notamment) ont permis à un grand nombre d'internautes, de diffuser, de relayer et de filtrer l'information produites ou capturées ailleurs, et ce à une vitesse éclair.

Le rôle d'internet et des média sociaux a bien été considérable pour les révolutions arabes. Il a permis de supporter un contre pouvoir, de s'organiser contre l'état en place, contre la police et de coordonner des actions de terrain. Répondant aux premières aspirations de l'internet comme espace de libre expression et de critique libertaire, ces usages militant d'internet ont pourtant été boudé ou ignoré par de nombreux média activistes traditionnels. Ces usages démocratisés ignorant les technologies alternatives constituent des pratiques fragiles et attaquables, traçables et peu sécuritaires, une faille du réseau. Mais la puissance du nombre rappelle la forme de la nuée d'Anonymous. Ces réseaux sociaux sont actionnés par des milliers ou des millions d'individus qui fournissent aussi des contre-expertises médiatiques en direction des institutions politiques et journalistiques. Assez pour provoquer des vagues de censure. Des formes de solidarités techniques libertaires ont alors vu le jour, pour contourner la censure et redonner accès à un internet plus sécurisé pour ses usager.es. Et de nouveaux média alternatifs ont pris naissance, renforçant et focalisant certaines de ces pratiques médiatiques de fortune.

6.2.2 Renouvellement des média alternatifs

Dans la lignée des pratiques de journalismes citoyens initiés par des acteurs et des collectifs militants de la fin des années 90, de nouveaux groupes se sont structurés, soit en pérénisant leur mode de fonctionnement, soit en renouvelant leur style d'intervention.

Au Canada, la Coop Média a ainsi été lancée en 2006 à l'initiative de membres du collectif éditorial du journal alternatif Dominion[9] . Ce réseau pancanadien de coopératives locales se consacre à assurer une couverture médiatique participative et locale. La création de la Coop Média vient de la reconnaissance des limites du processus éditorial rigoureux et exigeant en termes de main d'œuvre du Dominion et du besoin pour une organisation de média participative plus large. Elle est financée par son lectorat et gérée par ses membres. La Coop entend représenter les intérêts communs de différents groupes et proposer une couverture médiatique de qualité et locale. Elle rémunère donc ses contributrices afin de leur permettre de travailler sans la précarité associées au bénévolat.

D'autres projets sont nés dans au coeur d'une contestation sociale, travaillent dans l'urgence des luttes et s'attachent à des sujets plus concis et se spécialisant dans la couverture en direct (abondamment relayée par les réseaux sociaux). Lors du printemps érable au Québec, citons par exemple le travail de la télévision universitaire CUTV[10], qui camera au poing, utilise une connexion large bande pour transmettre en direct l'évolution des luttes sur le canal #manifencours.. Dans la même lignée, le projet 99% media[11] né lors du mouvement Occupy, s'engage dans la production de contenu médiatique et documentaire vidéo retraçant l'évolution des luttes sociales. Sur un ton plus ironique, le Guet des Activités Paralogistiques, Propagandistes et Anti-démocratiques (G.A.P.PA) s'est spécialisé dans la dénonciation médiatiques des formes de violence, de censure et de surveillance.

9 http://www.dominionpaper.ca/

10 http://www.cutvmontreal.ca/

11 http://www.99media.org/

6.2.3 Wikileaks et l'art de la fuite

Né en 2006, WikiLeaks est un site Web dénonciateur qui donne une audience aux fuites d'informations en publiant des documents ainsi que des analyses politiques et sociales, tout en protégeant ses sources et ses auteurs. Le site reste relativement peu connu du grand public jusqu'à ce qu'en avril 2010, lorsque WikiLeaks donne à voir une vidéo titrée *Collateral Murder* qui relate une bavure américaine lors d'un raid aérien à Bagdad. En juillet 2010 suite à une délation d'un de ses proches, les autorités américaines désignaient Bradley Manning comme l'informateur de cette vidéo et l'emprisonnent pour haute trahison En novembre 2010, le site révèle des télégrammes de la diplomatie américaine, qui sont cette fois filtrés par de nombreux grands journaux, ce qui permet de conférer aux révélations un style journalistique plus facile à appréhender et d'occulter d'éventuelles mentions dangereuses pour des particuliers. En 2011, suite à plusieurs attaques sur ses serveurs, au blocus financier orchestré à son encontre par de nombreuses compagnies de transfert d'argent, WikiLeaks suspend officiellement ses activités éditoriales, mis une kyrielle de sites miroirs ou de projets similaires voient le jour et le processus de fuite se répand. La décentralisation de WikiLeaks a marqué une première étape d'une prolifération de plate-formes de fuite. Si Julian Essange reste une figure centrale, médiatisée, on pourrait et on devrait vouloir s'inspirer dans la décentralisation de la démarche amorcée. Les médias ont très certainement cherché et trouvé un bouc émissaire, qui en retour, joue bien ce jeu – et celui d'un des héros de la culture hacker . Mais la fuite d'informations confidentielles concernant la sécurité de l'état est très vraisemblablement un processus plus large qui ne concernera plus seulement les gouvernements mais les industries agronomiques pharmaceutiques, minières, financières ou bancaires.

6.3 Activismes de l'accès

Le discours sur la fracture numérique, qui caractérisait le regard développementaliste technophile du tournant du millénaire tant peu à peu à disparaître avec la multiplication des possibilités d'accès au « réseau », et en particulier aux outils mobiles et aux applications de réseau social. Les activismes de l'accès visent désormais une appropriation des dimensions politiques des technologies numériques.

6.3.1 Télécomix et les solidarités globales

Telecomix est né en suède, d'un regroupement de hackers cherchant à apporter des solutions d'entraides effectives sur le terrain. Le collectif cherche principalement à soutenir les luttes globales en offrant aux citoyens des solutions de contournement en cas de censure. Telecomix refuse ainsi de s'inscrire dans rhétorique pirate, impliquant attaque masquée et démasquage. Leur approche de la politique s'inspire de l'hacktivisme au sens philosophique et pédagogique du terme. Il s'agit d'associer des savoir-faire technologiques à des analyses politiques profondes, et de développer des compétences à long terme. Telecomix s'appuie sur les mêmes outils de coordination (I'IRC) et les mêmes logiques non-hiérarchiques qu'Anonymous, mais le but est moins de réaliser des attaques spectaculaires que de construire des structures et des solutions d'émancipation. Télécomix *s*'est d'abord fait connaître en Tunisie, lorsque début janvier 2011 le gouvernement a bloqué la possibilité de mettre en ligne sur Facebook des vidéos montrant les exactions du régime. Des membres de Télécomix proposé une méthode permettant de les mettre en ligne à partir du territoire européen. Les activistes tunisiens

pouvaient ainsi continuer à les partager et à les diffuser sur le réseau social Facebook. Plus tard la même année, lorsque l'internet a été coupé en Égypte, le groupe a cherché à restaurer les connexions Internet en utilisant des vieux modems, des télécopieurs et en redirigeant le trafic. Il a réalisé une opération similaire en Syrie. L'épisode le plus marquant de leurs actions est peut-être la publication des fichiers log des dispositifs de surveillance de la firme américaine *Blue Coat Systems*, qui a finalement avoué que leur technologie était bien utilisée par le gouvernement Syrien.

6.3.2 CryptoParty : démocratiser la protection des données

Les *Crypto Parties (*fêtes cryptographiques) visent à offrir une introduction aux bases de la cryptographie, c'est à dire à la protection, la confidentialité, l'authenticité et l'intégrité de nos données et outils de communication. Le projet a été conçu à la fin août 2012 lors d'une conversation Twitter entre la médiactiviste australienne Asher Wolf et des experts en sécurité informatique suite à la proposition d'une loi australienne obligeant les fournisseurs à conserver les données de leurs usagers pendant deux ans. Ce mouvement auto-organisé de démocratisation de la protection personnelle est rapidement devenu viral. Lors d'une soirée amicale et ouverte, les participant.e.s sont initié.e.s à des outils tels que le réseau Tor, la signatures de clefs PGP[12] et l'usage de réseaux privés virtuels. Une douzaine de Crypto Parties autonomes se sont ainsi organisés dans les heures suivantes en Australie, aux États-Unis, au Royaume-Uni et en Allemagne, puis bientôt au Chili, aux Pays-Bas, Hawaï et en Asie. Une certaine Crypto Party de Londres s'est notamment rendu célèbre en rassemblant prés de 130 participants, dont certains vétérans d'Occupy London. La rencontre a dû être déplacée du HackerSpace de Londres vers le campus de Google Tech City. À la mi-octobre 2012 quelque 30 CryptoParties ont eu lieu dans le monde, dont certains sur une base continue. Crypto Party a reçu des messages de soutien de l'Electronic Frontier Foundation, d'Anonymous, de Wikileaks et du journal en ligne Wired. On le présente comme l'un des plus important projet civique contemporain de contre surveillance, certains les comparant aux « réunions Tupperware de l'apprentissage cryptographique».

Mais beaucoup de Crypto Parties s'adressent à des convaincus et rassemblent des utilisateurs enthousiastes mais déjà initiés, dont la politisation se restreint à la question de la protection personnelle. Ainsi, des partenariats avec des firmes de cryptographie et de surveillance, le soutien de gouvernements ou le financement de partenaires comme Google n'a pas toujours été exclu. Mais c'est surtout l'entrisme blanc et masculin et une forme d'élitisme techno-machisme qui est déploré. Fin décembre 2012, Asher Wolf publie une lettre[13] indiquant les raisons politiques qui l'amènent à quitter le projet Crypto Party. Elle y évoque le machisme ambiant, le laisser-faire des autres membres de la communauté, le détournement élitiste et les dérives apolitiques du projet. La lettre a beaucoup circulé et été commentée, les justifications ont fusé ainsi le soulagement des célèbres hackers, expliquant à l'initiatrice du mouvement qu'il valait mieux laisser ce projet à des « mains plus expertes ».

---

12 Les clefs PGP (pour *Pretty Good Privacy ou* « Assez Bonne Confidentialité »), renvoient à des logiciels de chiffrement et de déchiffrement cryptographique. Créé par l'américain Phil Zimmermann en 1991, PGP garantit la confidentialité et l'authentification pour la communication des données (textes, e-mails, fichiers, répertoires et partitions de disque dur...) pour accroître la sécurité des communications par courriel.

13 http://asherwolf.net/dear-hacker-community-we-need-to-talk/101/

7. Hacking with care[14] : attention, inclusion et solidarités dans les luttes technomédiatiques

Dans une société médiatique la plus participative qu'elle soit, nous vivons beaucoup de choses à distance, en pointant nos regards sur les images qui circulent, les textes, les formes, les récits sont leur véhicules. Nous vivons et ressentons ces histoires à travers nos filtres et nos épidermes culturels, sensibles et politiques. Les histoires donnent sens à l'imaginaire de nos actions.

Dans cette rétrospective d'une vingtaine d'années de luttes techniques et médiatique, on a retracé les idéaux humanistes, libertariens, universels des l'origine d'internet. On voit cependant qu'en fil rouge perdure une forme de centrisme culturel ainsi qu'un élitisme technique, qui s'impose soit comme marche à suivre, soit comme des points de focalisation niant ou relativisant l'importance d'autres combats politiques et sociaux, soit comme hiérarchie de classe avec des exclusions basées sur le genre et l'éducation technique. Malgré son discours égalitaire et libertaire, le contrôle et le contenu d'internet restent un lieu de pouvoir où se rejoue une vieille chanson : la prédominance d'un imaginaire Nord-Américain (Australien) et masculin.

L'histoire de la militante Asher Wolf, dont le projet fut encensé pour ses dimensions inclusives et révolutionnaires, et qui se voit exclue pour des raisons supposément techniques, est trop tristement significative. Aussi, les métaphores d'engagement et de militantisme à l'origine du Web continuent de puiser dans ces origines culturelles restreintes et excluantes.

Comment renverser cette tendance qui associe le techno-militantisme à une figure de la virtuosité blanche et masculine ? Peut-on encore imaginer l'émergence d'une politisation plus radicale et d'une introspection critique, féministe ou anti-coloniale des activismes techniques et médiatiques ?

Si au delà du culte de l'exploit, les hacktivistes et les médiactivistes ont bien des visées politiques et sociales[15], l'urgence de solidarités et d'inclusion entre genres et cultures devrait pouvoir trouver écho. Nous pouvons imaginer que les actrices et les acteurs de ces luttes porteront l'attention aux conditions d'émergence d'une intelligence collective, attentive, solidaire, inclusive et durable. Nous pouvons espérer que la multiplication des rencontres entre hackers, activistes médiatiques, sociaux, féministes, anti-coloniaux et anti-autoritaires feront de ces luttes des mouvements d'apprentissage de la solidarité dans la diversité. Nous pouvons aspirer à ce que les lieux de rencontre et d'actions soient plus solidaire, inclusif et attentionnés (Toupin, 2013, Goldenberg 2013). Alors la riposte à la censure et à la surveillance ne sera pas seulement une réponse anti-étatique, elle sera aussi le véhicule de transformation des rapports entre humains, technologies et connaissances.

---

14 Ce terme est issu d'un article publié dans le numéro 27 de la revue dpi , voire Goldenberg 2013 puis d'un projet collectif présenté au festival hacker OHM https://ohm2013.org/wiki/Project:HackingWithCare

15 Voire à ce titre l'introduction au numéro 27 de la revue dpi *Hacktivisme* par Haralanova, 2013 http://dpi.studioxx.org/fr/no/27-hacktivisme

Bibliographie

Anderson, Benedict, 1991, *Imagined communities: reflections on the origin and spread of nationalism* (édition de 1983, révisée et augmentée). Londres

Bennett, W. Lance, 2003, “Communicating Global Activism,”in Win van de Donk, Brian Loader, Paul Nixon, and Dieter Rucht, eds., *Cyberprotest: New Media, Citizens, and Social Movements*, Routledge.

Cardon Dominique et Christophe Aguiton, 2006, « L’équipement technologique des débats altermondialistes », in S. Proulx, L. Poissant, M. Sénécal (dir.), *Communautés virtuelles. Penser et agir en réseau*, Laval, Presses Universitaire de Laval, p. 335-349.

Cardon Dominique, 2010, « Confiner le clair-obscur : réflexions sur la protection de la vie personnelle sur le web 2.0 », in Millerand F., Proulx S. et Rueff J. (dir.), *Web social. Mutation de la communication*, Québec, Presses de l’Université du Québec, p. 315-328.

Cardon Dominique et Fabien Granjon, 2010, *Médiactivistes*. Presses de Sciences Po.

Castells Manuel, 1998, *La Société en réseaux.* Ier tome de *L’Ere de l’information*, trad. fr. Fayard, 1999.

Coleman Gabriella, 2012, *Coding Freedom: The Ethics and Aesthetics of Hacking.* Princeton University Press.

De Grosbois, Philippe, 2013, Quelques remarques sur la fuite de documents de la National Security Agency (NSA) En ligne : http://www.ababord.org/spip.php?article1654#nb1

Dubois, Frederic et Langlois, Andréa, 2005, *Autonomous Media, Activating Resistance & Dissent.* Montreal : Cumulus Press.

FLOSS manual (collectif), 2011. « Comment contourner la censure sur internet ». En ligne : http://fr.flossmanuals.net/comment-contourner-la-censure-sur-internet

Feenberg, Andrew and Barney, Darin, eds. 2004. *Community in the digital Age*. Rowman and Littlefield.

Flichy Patrice, *L’imaginaire d’Internet* La Découverte, Paris, 2001, 273 p.

George, Eric, 2003. La fracture numérique en question, in Eric Guichard, dir., Mesures de l’Internet. Paris : ed des Canadiens en Europe, p. 152-165

Gilmore John, 1993, December 6 "First Nation in Cyberspace" in *Time Magazine's December 06*

Goldenberg, Anne et Serge Proulx, 2011, « L’agir politique au regard des technologies de l’information et de la communication » in Globe Revue Internationale d’Études Québécoises. Vol 14. Montréal.

Goldenberg, Anne, 2013, « Hacking with Care », in *Hacktivismes, Dpi 27.* En ligne : http://dpi.studioxx.org/en/hacking-care-attention-bien-%C3%AAtre-et-politique-de-l%E2%80%99ordinaire-dans-le-milieu-hacktiviste

Grossman,Wendy, 2011, "Blackout in Egypt, or how to close the internet" in *NewsWireless.* En ligne : *http://www.newswireless.net/index.cfm/article/8811*

Haralanova, Christina, 2013, " Hacktivism: the Art of Practicing Life and Computer Hacking for Feminist Activism" in *Hacktivismes, Dpi 27.* En ligne : *http://dpi.studioxx.org/fr/no/27-hacktivisme*

Kapoor, Harsh 1999, "Harsh Kapoor on the blocking of the Dawn Internet Edition", in *Spider.* Archive en ligne : *http://groups.yahoo.com/group/cjesa/message/3216*

Lessig lawrence, 2000, *Code and other laws of cyberspace,* Basic Book, New York

Levy, Steven, 1984, *Hackers: Heroes of the Computer Revolution*, Anchor Press, Double Day , New York

Barlow john Perry, 1988, "*A Declaration of the Independence of Cyberspace"*. En ligne : *https://projects.eff.org/~barlow/Declaration-Final.html*

Toupin, Sophie, 2013, "*Feminist Hackerspaces as Safer Spaces ?"* in *Hacktivismes, Dpi 27.* En ligne: http://dpi.studioxx.org/feminist-hackerspaces-safer-spaces

Turner, Fred 2006, *From Counterculture to Cyberculture Stewart Brand, the Whole Earth Network, and the Rise of Digital Utopianism.* Presses de l'Université de Chicago

Ventura, Christophe, 2013, *La bataille du cyberespace*, in Mémoire des luttes. En ligne: *http://www.medelu.org/La-bataille-du-cyberespace*

Wolf Asher, 2012, "Dear Hacker Community, We Need To Talk". En ligne: http://asherwolf.net/dear-hacker-community-we-need-to-talk/101/