Hackers. Au cœur de la résistance numérique. Recension du livre d'Amaelle Guiton (2013)

Par **Eva Giard** et **Stéphane Couture**

Ce texte propose une recension de lecture du livre Hackers. Au cœur de la résistance numérique, publié par Amaelle Guiton (2013). Bien que le sujet des hackers ait été amplement exploité par le passé, notamment par des auteurs.trices québécois (Coleman 2016 ; Grosbois 2018) et les directeurs.trices du numéro (Couture 2015, 2020 ; Toupin 2016, 2017), nous avons préféré nous attarder dans ce numéro spécial de Possibles *à des aspects et des travaux sans doute un peu moins connus du public cible de la revue. Ceux-ci amèneront ainsi des perspectives différentes sur les phénomènes de résistance numérique. Nous ne pouvions toutefois pas ignorer le phénomène des hackers et avons donc décidé de proposer cette recension de lecture du livre de Guiton qui, bien qu'un peu daté (2013), fait directement écho au thème du numéro (la résistance numérique).*

Amaelle Guiton, l'autrice du livre *Hackers. Au cœur de la résistance numérique* (Au Diable Vauvert, 2013), est une journaliste particulièrement intéressée par les libertés numériques et leurs impacts politiques. L'autrice contribue au journal français *Libération* et tient notamment le blogue Technopolis, qui se revendique comme une « zone autonome de publication aléatoire visant à documenter, à hauteur de journaliste, les mutations sociales et politiques provoquées par l'extension du domaine du numérique. » (https://www.technopolis.net/a-propos/). Ses intérêts et son activité dans les sphères médiatiques font d'elle une observatrice bien placée pour rendre compte de la place des résistances numériques dans l'espace public.

Paru en 2013, le livre part d'un tournant dans la perception générale des hackers, que l'autrice date de 2010 et illustre de deux visages. Le premier est celui de Julian Assange, qui publie cette année-là diverses révélations sur les abus et les crimes du gouvernement américain. Son site WikiLeaks et certain.e.s de ses lanceurs et lanceuses d'alerte, dont la plus notable est certainement Chelsea Manning, amorcent de façon explosive le débat jamais vraiment clôturé de la limite à la liberté d'information. Le deuxième visage, celui-ci couvert, est le masque de Guy Fawkes, du roman graphique culte *V pour Vendetta*, récupéré par les milliers de personnes anonymes qui constituent le corps fantasque et informe d'*Anonymous*. Lorsque les Anonymous lancent des attaques sur certains sites gouvernementaux tunisiens, en plein cœur d'une révolte populaire contre le régime en place, le message est clair : Internet n'est plus un monde à part, circonscrit par ses écrans. Le langage courant se remplit de ces mots qui étaient auparavant réservés aux plus 'geeks' d'entre nous : « hacktivisme, libertés numériques… » (Guiton 2013, 11).

Non contents de simplement suinter dans le monde physique, ces hackers – dont le livre traite – ébranlent désormais les institutions les plus puissantes, jouent à pied d'égalité avec les dictatures et s'imposent comme une force politique à part entière. Mais, comme l'autrice le note, le politique s'infiltre en retour dans le réseau, par « des verrous numériques (...) sans toujours se soucier des dommages collatéraux aux libertés individuelles » (Guiton 2013, 12). Dans certains endroits du monde, l'impact politique va parfois « jusqu'à la censure et à la surveillance numérique généralisées. » (Guiton 2013, 12).

Avec des « technologies connaissant moins de frontières que les droits humains [*sic*] » (Guiton 2013, 12), de nouveaux contre-pouvoirs émergent pour défendre ces droits humains. Ces contre-pouvoirs prennent des noms et des identités aussi variés que leurs façons de faire ou leurs champs d'actions : d'abord les plus emblématiques tels que hackers ou hacktivistes, mais aussi les défenseurs des libertés d'informer et les protecteurs de la vie privée. Le tournant de 2010 marque leur arrivée sur la scène publique. Le livre se donne pour mission de dresser leur portrait et de résumer leur histoire, leurs valeurs, leurs actions et leurs idées, pour comprendre la place de ces contre-pouvoirs dans un monde où le spectre de la surveillance hante chaque innovation.

Le livre est divisé en 5 chapitres, chacun traitant d'un enjeu ou d'un pan culturel relatif aux hackers, eux-mêmes divisés en petites sous-parties qui se lisent presque comme des aphorismes.

Le premier intitulé, « **ce que hacker veut dire** », critique d'abord le raccourci communément effectué pour les définir : décrire les hackers comme des pirates informatiques. Guiton explique que le terme *hacker* correspond plutôt à une démarche générale qu'à une activité précise qui serait forcément liée à l'informatique, et la résume en trois mots : *comprendre, bidouiller, détourner*. Cette activité débute avec une certaine façon d'appréhender le monde, empreinte de curiosité, qui cherche à comprendre les objets en se les appropriant, en les détournant. Selon Guiton, face à quelque chose qu'il ne connaît pas, le hacker ne se demande pas « qu'est-ce que c'est ? », mais plutôt « qu'est-ce que je peux faire avec ça ? » (Guiton 2013, 23).

Pour Guiton, l'esprit ludique imprègne fondamentalement la culture hacker, comme le résume la définition du hack faite par Richard Stallman (créateur du concept de logiciels libres, voir plus bas) : « S'amuser dans l'utilisation de notre intelligence » (Guiton 2013, 29). Cet esprit ludique remonte aux origines mêmes du terme, inventé au MIT par le « Tech Model Railroad Club » dont les membres s'amusaient à taillader – *to hack* – des morceaux de circuits ferroviaires miniatures. Le hack est un jeu qui s'amuse certes à contourner les modes d'emploi, mais ce n'est pas un jeu complètement dépourvu de règles. Steven Levy, journaliste de Rolling Stones, publie dès 1985 un livre sur ce qu'il appelle « l'éthique des hackers », qui décrit un ensemble de principes, plutôt descriptifs que prescriptifs, sur le *modus operandi* de ces *bidouilleurs*. Cette éthique se résume en 6 points : « l'accès aux ordinateurs, et plus généralement tout ce qui peut améliorer la connaissance, doit être total et illimité » ; « l'information doit être libre » ; il « faut se méfier de l'autorité et promouvoir la décentralisation » ; « les hackers doivent être

jugés sur ce qu'ils font et pas qui ils sont » ; « l'on peut créer de l'art et de la beauté avec un ordinateur » ; « les ordinateurs peuvent changer la vie – en mieux » (Levy 1985, dans Guiton 2013, 36).

À travers cette éthique, on retrouve les grandes lignes des premières utopies d'Internet : partage – ouverture – décentralisation – libre accès – libre communication – libre information. Internet et les hackers se sont déployés le long des mêmes axes idéologiques. C'est ce qui permet de comprendre l'extension du hacking vers des sphères qui dépassent le seul milieu informatique. C'est en très large partie une philosophie qui s'applique aussi bien à la technologie qu'à la politique, d'où l'apparition d'un terme voisin, l'*hacktivisme, un terme* que Julia Group, un Think Tank suédois sur les libertés numériques définit comme « [consistant] à aller au-delà du hack technologique pour comprendre – et hacker – les processus politiques » (Julia Group, dans Guiton 2013, 42).

Le deuxième chapitre, « **Circulez, y a tout à voir (ou presque)** », aborde des pratiques et des moments qui ont marqué l'histoire de l'hacktivisme, à commencer par les printemps arabes. Le premier volet de cette histoire se passe en Tunisie. Les pratiques autoritaires du gouvernement tunisien, particulièrement lorsqu'il s'agit de libertés numériques (comme la liberté d'expression en ligne ou le respect de la vie privée), sont rendues flagrantes par l'arrestation de quelques personnes ayant tenté d'organiser une manifestation à l'aide de Facebook. Cette arrestation marque le début d'une recrudescence de l'engagement citoyen dans l'hacktivisme, l'entièreté de la toile existant, pendant un temps, avec un seul but, la chute du régime » (Guiton 2013, 53). En parallèle, Anonymous, un nouveau groupe d'hacktivistes dont l'organisation est fluide et difficile à cerner (voir Coleman, 2016 à ce propos), diffuse des vidéos pour dénoncer l'oppression du régime. Le groupe lance également sur certains sites web gouvernementaux des attaques par déni de service distribuées (*Distributed Denial of Service attack* – DDoS). Pendant tout ce temps, des manifestations battent leur plein dans les rues, et le dirigeant tunisien fuit le 14 janvier 2011.

Le deuxième volet de cette histoire des hacktivistes se passe en Égypte et met en scène Telecomix, un groupe décentralisé de cybermilitants européens et nord-américains. Le gouvernement égyptien a alors complètement coupé Internet ; des personnes associées à Telecomix se mobilisent pour mettre en place des réseaux de secours en faisant passer de vieux modems à travers la frontière du pays.

Deux axes de pratiques hacktivistes sont donc déployés tout au long des printemps arabes. Le premier, mis en évidence par Anonymous, se déploie le long des revendications du droit à la vie privée, un droit vital dans les régimes autoritaires, mais moins central dans les préoccupations du grand public des pays occidentaux. Guiton souligne d'ailleurs que l'argument classique pour s'en désintéresser est que l'on « n'a rien à cacher tant qu'on n'a rien à se reprocher » (Guiton 2013, 65). Mais Anonymous et ceux que l'on appelle parfois les 'cypherpunks' – des spécialistes en cryptographie – sont convaincus que l'anonymat et le respect de la vie privée sont des droits fondamentaux et que, dans un monde de plus en plus surveillé, l'anonymat est une forme de révolte.

Le deuxième axe de pratiques hacktivistes, mis en évidence par Telecomix, est celui de la fracture numérique. S'il y a au cœur de l'éthique hacker la conviction qu'Internet et l'informatique peuvent faire s'améliorer le monde, cela ne peut être réalisé à son plein potentiel que si le territoire et l'humanité en sont aussi largement pourvus que possible. De nombreuses initiatives cherchent donc à couvrir les « zones blanches » déconnectées d'accès au réseau, que ce soit en y apportant du matériel informatique ou en y déployant des « réseaux wifi maillés » (mesh networks), fonctionnant sur la base de technologie sans fil. L'autrice donne l'exemple d'une tentative cherchant à couvrir certaines zones maritimes par ces réseaux maillés, afin de disposer d'un accès à Internet même au large (reseaulibre.ca est un exemple expérimental d'un tel réseau maillé au Québec, dans la région de Montréal).

Cependant, si l'éthique et les enjeux propres aux hackers s'entremêlent à des visions militantes sur des scènes politiques, ce n'est pas sans friction. Amaelle Guiton relève que la vision technique et la vision militante s'affrontent parfois sur le plan des actions préconisées. Par exemple, Assange revendique « la vie privée pour les faibles, la transparence pour les puissants » (Guiton 2013, 71), mais les débats sont parfois plus polarisés, avec certains hackers qui, partisans d'une transparence totale, restent convaincus que l'information ne peut en aucun cas être entravée. La liberté d'expression est aussi sujette à débat. La liberté totale de l'information, au cœur des valeurs de certains, entre en conflit avec la perspective militante qui considère que tous les points de vue ne se valent pas.

Le troisième chapitre, « **culture du partage, partage de la culture** », revient sur les implications qu'a le principe éthique de liberté de l'information, poussé à son paroxysme. Il revient en particulier la figure majeure qu'est Richard Stallman. Initialement développeur au MIT, Stallman est progressivement devenu frustré de ce que les logiciels tendent à devenir : restrictifs, contrôlés, propriétaires. Il développe, au début des années 80, un système d'exploitation libre, GNU, et, quelques années plus tard, une licence publique qui interdit toute réappropriation privée de ce qui est publié sous son sceau. Il pose ainsi les premières bases de la culture libriste, dont les logiciels doivent, selon lui, répondre à quatre critères : chacun doit pouvoir librement l'exécuter, mais aussi le copier, le distribuer, et enfin le modifier. La seule condition est de reverser ses travaux à la communauté, ce qui implique que le code source du programme soit accessible.

Le 'libre' de 'logiciel libre' est ambigu, d'autant plus que 'free' signifie en anglais à la fois libre et gratuit. Deux visions s'affrontent donc à ce propos. La première est celle de Stallman, pour qui le logiciel libre est une philosophie et un projet politique plus qu'un simple fonctionnement technique. Il prône la liberté des utilisateurs, l'égalité dans l'usage de cette liberté et la 'fraternité' par la coopération. La deuxième vision est celle du hacker Eric S. Raymond, théoricien de « l'Open Source », qui met de l'avant les avantages techniques du modèle plutôt que ses implications idéologiques, dans la perspective d'en favoriser l'adoption par la sphère marchande (voir Coris 2006 à ce propos). L'Open Source peut en effet avoir une vraie efficacité économique, comme le démontrent des projets comme Thunderbird, Libreoffice, VLC ou Firefox, mais surtout aujourd'hui les nombreux logiciels souvent invisibles utilisés dans la construction des plateformes de Google, Facebook et autres réseaux similaires.

Malgré la croissance continue du monde du logiciel libre, maintenant affirmé comme un modèle de fonctionnement efficace, il reste relativement restreint à un public 'geek' et déjà à l'aise avec la technologie. Passer au logiciel libre est rarement le choix le plus ergonomique et accessible, et de nombreux militants en faveur du modèle libriste revendiquent une éducation poussée à la technologie pour qu'une plus large portion de la population puisse sortir de la servitude aux logiciels propriétaires.

Le domaine où les hackers convainquent le plus facilement le grand public, c'est pour l'accès aux produits culturels. Au début des années 2000, c'est d'abord Napster qui popularise le partage en pair à pair. Quelques années plus tard, Anonymous attaque les sites du département de la justice, d'Universal et de Warner, suite à la fermeture du site de streaming Megaupload. Une guerre légale commence contre le piratage de contenu culturel, avec entre autres la loi Hadopi en France et l'invention des mesures techniques de protection (Digital Rights Managements, DRM), qui rendent beaucoup plus difficile le partage des œuvres. Les défenseurs des libertés numériques réagissent, revendiquant le droit au partage qui préexistait la dématérialisation de la culture. Par exemple, le célèbre site The Pirate Bay, connu et souvent décrié pour le partage illégal de contenu, était initialement un Think Tank visant à discuter des implications du *copyright* sur le partage de la culture. Parmi les axes de développement des revendications du partage de la culture, Guiton mentionne également les hackerspaces, qui visent à créer des lieux physiques empreints de l'éthique hacker et de l'importance du décloisonnement de l'information, de la connaissance et du partage. Les hackerspaces se multiplient, chacun avec des modalités et des objectifs différents, mais tous ayant à cœur le développement de la bidouille et une logique DIY, pour favoriser l'apprentissage personnel (pour approfondir, voir Toupin 2017).

Le quatrième chapitre, « **Démocratie 2.0** » détaille l'investissement par les hackers des sphères politiques plus traditionnelles. La politique n'est au final qu'un système « hackable » comme un autre. « La loi, c'est du code. Et le code, s'il est pourri, on le réécrit », affirme Bluetouff, un hacker interviewé par Guiton (2013, 154). Les projets de lois qui tentent d'altérer le fonctionnement d'Internet inquiètent les hackers, comme le projet qui remettait en question la neutralité du web aux États-Unis, ou encore la loi hadopi, la « loi favorisant la diffusion et la protection de la création sur Internet » mise en place en France en 2009 pour tenter de freiner le partage de fichiers en pair à pair. Des organismes comme l'Electronic Frontier Foundation (EFF) aux États-Unis ou la Quadrature du net en France tentent d'influer sur le jeu politique. Certains Think Tank ont été créés, comme en Suède où le gouvernement l'a lui-même demandé ; beaucoup de législateurs ont des lacunes au niveau de leur compréhension du fonctionnement d'Internet.

Toutefois, faire partie du débat démocratique peut être compliqué pour les hackers. La politique est lente, alors que le hack est rapide. Il y a donc un équilibre à trouver entre un système politique très codifié, opaque, et ce qui caractérise les hackers. Certains se sont tout de même risqués à la formation de partis politiques en bonne et due forme. Un mouvement de ce qu'on appelle les partis pirates apparaît, avec, dans les enjeux qui leur tiennent à cœur, ce qui a toujours été partie intégrante des intérêts des hackers : le droit à la vie privée, la liberté d'expression et la réforme de la propriété intellectuelle. Le

problème s'avère que cela ne constitue pas un programme politique à part entière, et que s'ils veulent prétendre agir en politique, cela implique de se placer sur l'échiquier politique et de prendre position sur des enjeux qui ne concernent pas nécessairement Internet. Ils apportent cependant un renouveau certain à la politique, en faisant évoluer les outils de la participation citoyenne par le biais de plateformes collaboratives et en proposant une vision idéologique ayant à cœur la décentralisation et l'horizontalité des prises de décision.

Avec les hackers prenant part à la vie politique, la question de l'institutionnalisation se pose ; difficile de s'immiscer dans un système sans qu'il change nos façons d'être. L'autrice s'interroge : les hackers et leurs partis pirates vont-ils vers une radicalisation de la politique ou une institutionnalisation de l'esprit d'Internet ?

Le cinquième chapitre, « **du bazar dans les cathédrales** », part du format de fonctionnement des logiciels libres et « open source » décrit par Eric S. Raymond. Pour Raymond, les cathédrales, c'est la façon de faire hiérarchique et verticale, le bazar, c'est ce qu'il propose ; un modèle libre, flexible, ouvert à tous. C'est un modèle qui s'applique autant à l'Open Source qu'à la structure physique d'Internet ou à l'éthique hacker… Pour Guiton, le modèle du bazar est partout, à tous les niveaux de la toile, et peut parfois décontenancer celles et ceux qui n'y sont pas habitués. Anonymous, pour ne nommer que ce groupe, fonctionne sans membres ou structure claire, répondant à un régime de « do-ocratie », le pouvoir à « celui qui fait » (Guiton 2013, 194). Dans les médias, il était pourtant souvent présenté comme un « groupe » fixe. Dans les faits, leur visée n'est jamais très claire, constamment redéfinie par les individus qui s'identifient à Anonymous. Certains sont très politiques, d'autres uniquement motivés par le « lulz » et la simple envie de mettre le bazar un peu partout. Amaelle Guiton explique que la communauté du net propose une nouvelle manière à part entière d'organiser le pouvoir. Ce n'est pas simplement une contre-culture, mais une réinvention de la culture.

Pour Guiton, une cathédrale en particulier a été très affectée par le bazar du web ; les médias. D'abord parce qu'Internet permet à tout un chacun de devenir son propre média, remettant en question les institutions médiatiques traditionnelles, mais aussi en s'affirmant comme un contre-pouvoir très puissant par le biais de la liberté d'information souvent revendiquée, comme par WikiLeaks. L'auteure s'interroge sur les possibilités futures de fuites aussi massives que celles que le site avait permises. Chelsea Manning s'est vue traitée de façon qui découragera certainement les prochains potentiels lanceurs d'alerte, beaucoup des grands médias lui ayant tourné le dos. Wikileaks aura toutefois laissé au moins un héritage, celui de méthodes et de bonnes pratiques pour aider le journalisme d'investigation à s'adapter aux nouveaux enjeux technologiques. L'exemple le plus important demeure la sécurité des données : si elle n'est pas garantie, le danger peut être réel pour les personnes impliquées.

Guiton s'interroge aussi sur la naissance éventuelle d'un nouvel « altermondialisme numérique ». De la même façon que Occupy se revendique des « 99 % », Anonymous se décrit comme « étant légion » ; c'est le système entier, la distribution du pouvoir qui est mise en question, avec la multitude contre les élites.

L'autrice note toutefois qu'il est difficile de réduire les hackers à un mouvement uniforme, ou de leur attribuer une case politique trop rapidement. Le panorama des défenseurs des libertés numériques est diversifié : des hackers qui ne sont pas des hacktivistes, des cybermilitants qui ne sont pas des hackers, des hacktivistes avec pour seul objectif d'améliorer les outils de communication, etc. Mais c'est cette diversité qui leur est propre, car c'est précisément ce qu'ils revendiquent : la décentralisation, l'horizontalité.

L'auteure conclut en resituant les hackers dans un monde où les enjeux des libertés numériques sont de plus en plus sensibles et en danger. Eux « sauront toujours crocheter les serrures » (Guiton 2013, 238), mais la dystopie de la surveillance généralisée n'est pas un monde dont ils veulent. Les circonstances les mettent sur le devant de la scène, parfois un peu malgré eux. Leur éthique se popularise et se répand, avec le risque attaché de la dilution. Mais, « qu'ils le veuillent ou non, les hackers portent en eux le germe d'une subversion politique, celle d'une nouvelle distribution du pouvoir, et du savoir » (Guiton 2013, 241).

Bien que l'autrice ne conceptualise pas explicitement la notion de résistance numérique, la lecture du texte fait ressortir l'idée que les pouvoirs qui s'exercent sur la toile opèrent de façon distribuée, dispersée. Pour lutter, il ne s'agit pas de cibler un.e ennemi.e et l'attaquer de front, mais de proposer de nouvelles modalités d'actions qui échappent aux logiques de contrôle et aux prescriptions de dispositifs du numérique de plus en plus opaques et verrouillés. Les hackers représentent une forme de résistance numérique, moins par leurs revendications en tant que telles que par leur façon d'être, intrinsèquement politique et subversive. Le grand défi, à notre avis, reste de concilier cette « façon d'être » avec l'éventail actuel des luttes environnementales et la justice sociale, et d'intégrer en leur sein une plus grande diversité d'actrices et d'acteurs (Dunbar-Hester 2019).

Guiton, Amaelle. 2013. Hackers. Au cœur de la résistance numérique. Vauvert : Au Diable Vauvert.

Biographies

Eva Giard est étudiante au baccalauréat en sciences de la communication à l'Université de Montréal et auxiliaire de recherche pour Stéphane Couture.

Stéphane Couture est professeur adjoint au département de communication de l'Université de Montréal.

Références

Coleman, E. Gabriella. 2016. Anonymous : hacker, activiste, faussaire, mouchard, lanceur d'alerte [traduit de l'anglais par Nicolas Calvé]. Futur proche. Montréal : Lux éditeur.

Coris, Marie. 2006. « Chronique d'une absorption par la sphère marchande : les Sociétés de Services en Logiciels Libres. » Gérer & Comprendre 84: 12-24.

Couture, Stéphane. 2015. « Le contrôle des communs numériques à des fins commerciales : le cas des logiciels libres », Éthique publique. Revue internationale d'éthique sociétale et gouvernementale 17(2). https://doi.org/10.4000/ethiquepublique.2275.

Couture, Stéphane. 2020. « Free and Open Source Software », dans : M. O'Neil, C. Pentzold et S. Toupin (Dir.) The Handbook of Peer Production, pp. 153-68. Hoboken: Wiley. https://doi.org/10.1002/9781119537151.ch12.

Dunbar-Hester, Christina. 2019. Hacking Diversity : The Politics of Inclusion in Open Technology Cultures. Princeton : Princeton University Press.

Grosbois, Philippe de. 2018. Les batailles d'Internet : assauts et résistances à l'ère du capitalisme numérique. Montréal : Écosociété.

Guiton, Amaelle. 2013. Hackers. Au cœur de la résistance numérique. Vauvert : Au Diable Vauvert.

Levy, Steven. 1985. Hackers heroes of the computer revolution. New York: Dell.

Toupin, Sophie. 2016. « Gesturing towards anti-colonial hacking and its infrastructure ». Journal of Peer Production 12: 1-27. En ligne : http://peerproduction.net/editsuite/issues/issue-9-alternative-internets/peer-reviewed-papers/anti-colonial-hacking/ (Page consultée le 21 mai 2021).

Toupin, Sophie. 2017. « Le hacking féministe : La résistance par la spatialité ». « Les implications spatiales de la résistance numérique », dans : M. Bonenfant, F. Dumais et G. Trépanier-Jobin (Dir.), Les pratiques transformatrices des espaces socionumériques, pp. 161-180. Québec : Presses de l'Université du Québec.