Hackers.

Ils veulent l'anarchie ?

Ippolita

Nous sommes en 2017, une publicité pour une célèbre entreprise italienne de télévision IP (télévision par Internet) claironne :

> « Aujourd'hui, nous avons accès à un univers sans limites […] une galaxie infinie de [contenus] à regarder partout et à n'importe quel moment. Les nouvelles technologies nous offrent la possibilité de ne pas avoir à choisir. N'est-ce pas fantastique ? »

Non ! Cela n'a rien de fantastique, c'est même horrible. La « liberté de ne pas avoir à choisir » et de se (laisser) divertir toujours plus, la liberté d'être libérés de la liberté. Il fallait y penser ! Fini de se fatiguer ! Fini de programmer, d'imaginer, de communiquer ou d'organiser ! Nous devons faire confiance à l'oracle technologique. Trop de contenus, trop de possibilités ? Il suffit de déléguer…

Aujourd'hui, les interactions que nous entretenons avec les dispositifs numériques correspondent souvent à l'exécution de procédures mises au point par des entreprises afin que ces dernières gagnent de l'argent – parce que nous nourrissons, par exemple, leurs bases de données et leurs algorithmes. Ces derniers nous guident, pas à pas, dans le vaste monde d'Internet et, de plus en plus, dans ce que certains appellent encore le monde « hors-ligne ». Ils sont la clé de la fameuse libération de la liberté. Choisir ce que l'on va acheter et où on l'achètera, choisir où, quand et avec qui on dînera, choisir ce que l'on mangera, choisir le lieu de nos vacances, choisir avec qui nous coucherons, etc. Chaque aspect de la vie hu-

maine peut être soumis à des automatismes comportementaux assistés par ordinateur. Tu doutes ? Va te faire *nudger*[1] !

Les technologies de la domination ne se contentent pas de nous inviter à laisser aux machines le choix de telle ou telle émission plus ou moins stupide. Elles nous proposent d'alléger voire de supprimer nos efforts cognitifs (personnels) et même de prendre en charge certains aspects de nos modes d'organisation sociale. Le pire est qu'il est bien difficile de ne pas nous laisser happer par cette dynamique. Pensons aux trop fameux médias sociaux. Si nous évitons de les utiliser, nous pouvons, parfois, nous soustraire en partie à la surveillance et au contrôle de masse, mais cela implique d'assumer certaines difficultés à rester en contact avec certains de nos proches ou tout du moins ne pas être exclus d'une partie de leur vie. Dans un monde où la connexion est bientôt la chose la mieux partagée, rester « en-dehors » ou bien ne vouloir communiquer que par des canaux chiffrés et anonymes revient à « s'auto-dénoncer » ou, pour employer une expression insupportable, avouer que l'on a quelque chose à cacher.

Rafaëlle Gandini Miletto. Photographie. Barcelone, 2012. (CC BY SA)

S'il est nécessaire de comprendre toute la portée de l'informatique de la domination[2], il importe aussi d'élaborer des tactiques et des pratiques d'autodéfense aussi bien personnelles que collectives. Il est surtout indispensable de réfléchir à comment éduquer (nous éduquer mutuellement) à ces pratiques. Penser que les révolutionnaires ont pour alliés objectifs de mystérieux « hackers » qui vont se charger de bloquer – d'une façon presque magique – les flux numériques, c'est se mettre le doigt dans l'œil. Une certaine attitude hacker, par contre, est bel et bien susceptible d'engendrer de l'autonomie et de l'autogestion.

ATTITUDE HACKER ET *HACKING*

Il est assez aisé de reconnaître l'attitude hacker. Prenons une fontaine avec un robinet intrigant. Un hacker s'intéressera au fonctionnement du robinet. Il essayera de le réparer s'il est endommagé. Il le démontera. Il se demandera s'il est possible d'augmenter ou de réduire le débit de l'eau ou d'adapter le robinet sur un autre système. Les autres personnes s'intéresseront à ce qui sort du robinet et au simple fait que « ça fonctionne ».

Le *hacking* est une façon d'entrer en relation avec notre environnement, et plus spécifiquement avec le milieu technique dans lequel nous vivons. Ce n'est donc pas d'abord un hobby et encore moins une identité. Bien sûr, certains sont davantage portés à appliquer cette attitude d'une façon plus générale et systématique. Certaines personnes adorent les machines. Elles les étudient, elles les montent et elles les démontent ; elles les améliorent et elles les détruisent sans cesse. Elles sont curieuses et rien ne peut refréner leur curiosité. La crainte d'être puni pour avoir enfreint des lois n'y fait rien. C'est l'une des raisons pour lesquelles, y compris dans les représentations les plus communes, le *hacking* est souvent associé à l'illégalité et au piratage. En réalité, il s'agit plutôt d'une pratique alégale.

L'informatique ne constitue qu'un champ particulier du *hacking*. Le terme « hacker », bien avant la massification de celle-là, était déjà utilisé pour désigner, par exemple, les radioamateurs. Dans le domaine du numérique, les hackers peuvent se livrer à toutes sortes d'activités. Les codeurs écrivent des programmes dans toutes sortes de langages et autres dialectes. Les *security hackers*

s'intéressent à la sécurité informatique et essayent de trouver et d'exploiter les failles de tel ou tel système. Dans certains cas, ils font cela pour le plaisir, pour sécuriser leur propre matériel ou parce qu'ils se sentent investis d'une mission ; dans d'autres cas, ils travaillent pour garantir et augmenter la sécurité des infrastructures des entreprises, des gouvernements, de l'armée, etc. ; dans d'autres cas enfin, ils se vendent tout simplement au plus offrant. Les *hardware hackers*, eux, s'amusent à modifier ou à construire des machines (électroniques, la plupart du temps, mais pas seulement) : ils soudent, coupent, assemblent… Les bidouilleurs et autres *geeks*, enfin, n'ont pas nécessairement de spécialité, mais ils sont capables de s'orienter aisément dans les mondes numériques.

On pourra rétorquer que ce panorama est loin d'être exhaustif. C'est absolument exact ! C'est à dessein que nous laisserons ici de côté toute une partie de la faune hacker. Cette description succincte est toutefois suffisante pour rompre avec l'image colportée par les médias faisant des hackers des jeunes (hommes) à la fois géniaux et asociaux, ne sortant guère de leur chambre (bourrée d'ordinateurs et autres machines) et exprimant leur mal-être en s'en prenant à n'importe qui. Le stéréotype se mue aussi, ces derniers temps, en une dichotomie stérile entre les hackers prétendument éthiques et les autres, les premiers œuvrant évidemment au service des institutions officielles – et suivant même parfois, à cette fin, des « formations qualifiantes », si bien que l'on se demande ce qui les différencie des traditionnels ingénieurs – et les seconds œuvrant, évidemment, dans le noir et au service du « mal ». On peut encore évoquer la mode des *fab labs* [de l'anglais *fabrication laboratory*, littéralement « laboratoire de fabrication »] et autres *maker spaces*, financés par des institutions et des entreprises privées. Une culture *do it yourself* gentillette, acceptable, jamais contestataire et surtout pleinement intégrée à l'ordre du monde libéral s'y développe. Le capitalisme néolibéral a bien compris tout l'intérêt de l'innovation par la base.

Dans tous les cas, on retrouve un invariant : la recherche d'une capacité hors du commun à tout faire faire aux machines ou du moins à les maîtriser pleinement, pour le meilleur et pour le pire. Tous les hackers seraient en puissance capables de détruire (les machines, les données…). C'est d'ailleurs pour cela qu'il existe de plus en plus d'initiatives d'intégration de la culture hacker. Bref, les

hackers ont à travers leurs savoirs et savoir-faire un certain pouvoir, il ne faudrait pas qu'il tombe dans de « mauvaises mains ».

POUVOIR

La plupart des hackers ont bien conscience du pouvoir qu'ils peuvent acquérir à travers leurs pratiques. Certains se lancent même dans le *hacking* pour cela. On sait aussi combien le passage est aisé entre la capacité à agir sur un environnement et la volonté de dominer les autres grâce à cette capacité. La maîtrise des machines dans un monde construit en large mesure grâce à – voire par – des machines est un pouvoir gigantesque. Le contrôle de ce pouvoir est source de luttes pour la suprématie.

Ces dernières années, parmi les personnes les plus puissantes et influentes au monde, de nouvelles têtes sont apparues. Il s'agit en bonne part de hackers, d'ex-hackers ou de *wannabe-hacker*. En quelle mesure Bill Gates (le fondateur de Microsoft) ou feu Steve Jobs (le fondateur d'Apple) sont-ils des hackers ? Cela donne lieu à bien des controverses. Il est en tout cas indéniable que tous deux viennent du bouillon de culture constitué par les bidouilleurs de la Silicon Valley des années soixante-dix. Larry Page et Sergey Brin ont créé Google à l'Université de Stanford. Mais dans la « plus pure » tradition hacker, ils se sont, par la suite, transférés dans un garage pour abriter les machines du moteur de recherche naissant. Mark Zuckerberg est, à l'origine, un *nerd* très à l'aise avec les ordinateurs. L'histoire est désormais célèbre, il s'est servi de ses compétences pour créer un système lui permettant de décrocher des rendez-vous galants. Ce même système est aujourd'hui le média social le plus utilisé au monde : Facebook.

On pourrait toutefois penser que ces personnes n'ont rien à voir avec d'autres hackers célèbres. Julian Assange, le très controversé *security hacke*r, fondateur de Wikileaks, a, lui, mis au défi les gouvernements du monde entier en publiant des câbles diplomatiques secrets. Linus Torvalds, le créateur du noyau du système d'exploitation Linux, fait partie des programmeurs qui consacrent corps et âme à améliorer constamment leurs codes. Richard Stallman, le fondateur de la FSF (Free Software Foundation), est probablement l'incarnation la plus évidente du hacker « pur et dur », de celui qui

ne fait aucun compromis, sur rien et avec personne pour suivre ses propres idéaux de liberté.

Certes, on pourrait dresser ici une distinction entre hackers « désintéressés » et hackers convertis en patrons. On remarquera toutefois que parmi l'ensemble de ces personnages, aussi frondeurs puissent-ils (pour certains) paraître, aucun ne s'inspire de la tradition libertaire. Des deux côtés, par contre, on retrouve des partisans de différentes sortes de libéralisme et même quelques libertariens.

On peut aussi relever plusieurs tendances communes. Le culte de l'excellence est l'une d'entre elles. Faire toujours mieux, toujours plus puissant est impératif ! Les limites doivent être toujours repoussées. Cette recherche va de pair avec une culture du défi et même du duel. Un évident esprit de compétition agite les milieux hackers. Il donne souvent lieu à des comportements méritocrates. Ainsi, est-il mal vu de « déranger » les autres en leur posant des questions considérées comme trop simples. L'acronyme RTFM pour *Read The Fucking Manual* [Lis le p*** de manuel] rend bien cette idée. L'effort individuel est un prix à payer pour être reconnu parmi les meilleurs. L'orgueil d'avoir trouvé une solution plus rapide ou plus élégante – le tout grâce à un savoir-faire technique difficilement acquis – est monnaie courante. Il est toutefois difficile de s'étonner d'un tel individualisme chez des personnes qui se regroupent pour bricoler des ordinateurs individuels[3]. Une évidente hiérarchie en découle. Les élites semblent avoir une aura. Les apprentis hackers qui font trop de bruit, eux, sont affublés de toutes sortes de noms moqueurs : *lamer* [nul, boiteux], *script kiddie* [gamin à script, pour désigner ceux qui essayent de s'infiltrer dans des systèmes en utilisant des programmes mis au point par d'autres]… Chez les hackers, il y a des sphères exotériques, accessibles au grand public, et des sphères ésotériques, réservées aux initiés.

Quant aux non-hackers… Tant pis pour eux !

RÉVOLUTION ?

On entend parfois que l'informatique aurait produit une véritable « révolution numérique ». Une chose est sûre, ce genre de « révolution » n'a rien de libertaire. Les évolutions des technologies numériques depuis une vingtaine d'années ont par contre largement

contribué à une « révolution de l'ordre » que bien des hackers ont épousée. Celle-ci est d'orientation libertarienne, voire anarcho-capitaliste. Elle provoque des changements rapides, intenses et profonds dans les façons dont les personnes entrent mutuellement en relation et se rapportent aux institutions. Elle refond aussi le monde du travail. La frontière entre public et privé est de plus en plus floue.

La « révolution numérique » est, dans les faits, une révolution de la surveillance (qui génère du contrôle) et du consumérisme. Le marché doit être toujours plus lisse. Cela peut passer par des choses apparemment aussi éloignées que le profilage ou la libération de l'information. La force du phénomène réside dans son caractère paradoxal proprement néolibéral : d'une part, il implique l'explosion de certains carcans et ouvre des espaces de liberté et, d'autre part, il fait en sorte que cette même liberté s'inscrive strictement dans l'ordre du marché comme ordre du monde. En bonne part, les hackers illustrent bien ce paradoxe ; traditionnellement, ils ont tendance à se méfier des institutions étatiques, mais ils ont beaucoup moins de problèmes avec le mode de production capitaliste. On ne compte plus parmi eux, outre les anarcho-capitalistes convaincus, les Messieurs Jourdain du libertarianisme[4].

Il est fort peu probable que la description du monde du *hacking* qui a été donnée jusqu'ici attire les personnes animées d'un esprit libertaire. Pourtant tout n'est pas à jeter dans le *hacking*. Loin de là. Il existe même des ponts entre certaines initiatives militantes et certains groupes de hackers. Il faut évoquer ici les *hackmeetings* italiens ou de la péninsule ibérique[5] : ces événements autogérés qui réunissent des participants des hacklabs et autres espaces autogérés où se mélangent culture libertaire et attitude hacker – et où l'on retrouve une population bien plus mixte que dans les milieux hacker traditionnels. On ne saluera jamais assez, en outre, le travail que font, sur la toile, autistici.org, riseup.net, nadir.org… On peut encore évoquer les projets de mettre au jour des infrastructures de communication par la base[6]. On peut enfin citer des initiatives comme le *Guide d'autodéfense numérique,* qui donne quelques précieuses pistes pour commencer à se protéger[7] de la surveillance de masse.

Étant donné le monde dans lequel nous sommes désormais contraints de vivre, ces initiatives nous aident à devenir toutes et tous un peu hacker. Nous devons néanmoins nous questionner sur

leur portée effective. La difficulté technique est bel et bien réelle. Pour beaucoup de gens, les hackmeetings et autres hacklabs ne sont pas vraiment attirants. Les serveurs militants, pour leur part, demeurent plus compliqués à utiliser et fonctionnent parfois « moins bien » que ceux des géants du Net – en réalité, ils n'ont ni les mêmes ressources à disposition ni les mêmes finalités. Quant aux traités qui visent à nous apprendre à nous défendre, ils demeurent inaccessibles à la plupart des gens, lesquels abandonnent leur lecture à la dixième page et remettent à la Saint-Jamais le passage à la pratique. Sans compter que la péremption des conseils qu'on y prodigue va parfois plus vite que les mises à jour du texte ! Il ne faut pas se voiler la face, les pratiques numériques de la plupart des gens (et les militants libertaires n'y échappent pas, loin de là) sont édifiantes !

Mais sombrer dans le pessimisme ne sert à rien. Étant donné que nous ne pouvons nous soustraire absolument à la technologie, nous devons prendre conscience de notre degré d'exposition à sa domination et accroître notre autonomie en relation aux objets techniques et en particulier numériques. Nous voudrions proposer, à partir de notre expérience, une piste à explorer pour essayer de se sortir de cette situation. Cette approche nous l'appelons *pédagogie hacker*. Elle reprend à son compte *l'attitude* hacker – que nous décrivions au début de ce texte et qui ne se limite pas, nous insistons, à des questions de défense et d'attaque, de cryptographie et de code – dans une perspective clairement libertaire. Plutôt que de chercher uniquement à former à des pratiques numériques, elle se veut générale et essaye de conjuguer alphabétisation numérique et alphabétisation politique. Nous l'expérimentons autant dans des contextes militants que non militants.

PÉDAGOGIE HACKER

Ippolita a commencé à utiliser l'idée de pédagogie hacker dans le cadre de formations d'autodéfense numérique. Notre intention était de souligner la valeur pédagogique des compétences et des attitudes qui caractérisaient les premiers computer clubs et hacklabs – contexte dans lequel Ippolita est née et a fait ses premiers pas. Cette attitude pédagogique, en généralisant le concept de hacker, se fonde sur des éléments incontournables :

1. Un regard curieux et critique sur le monde, en général, et sur la technologie, en particulier.

Il s'agit d'apprendre à questionner et à problématiser la réalité qui nous entoure. Une fois identifié un problème, il faut se mettre au travail pour essayer de le résoudre. Tout peut être réinventé, réagencé, réadapté. Un hacker est l'opposé d'un utilisateur passif. Gare toutefois au solutionnisme technique qui prétend que tout problème rencontré dans la vie courante peut connaître une solution technique !

2. L'apprentissage comme plaisir

Le plaisir de l'apprentissage motive le hacker à apprendre. Les hackers programment avec enthousiasme, ils aiment affiner leurs compétences et utilisent leur intelligence. Mais il faut aussi retrouver le plaisir de collaborer.

3. L'apprentissage est le résultat d'une recherche et d'une expérience personnelles et collectives, les parcours d'étude officiels ne nous intéressent pas.

La formation des hackers suit principalement des canaux non officiels. Le point de départ est pratique et expérimental. Il faut « mettre les mains dans le cambouis » et ne pas déléguer. L'entraide est aussi de rigueur.

4. La dimension sociale du savoir et la connaissance comme bien commun

Tout hacker ressent le besoin de faire circuler ce qu'il a appris. La connaissance est pour lui un bien collectif. Il doit donc la mettre à disposition de toute personne qui pourra s'en servir. Le savoir est un bien qu'il n'est possible de construire que collectivement.

À cela s'ajoute un point sur lequel nous désirons insister un peu plus. S'il est souvent difficile de sortir de certaines pratiques problématiques liées à l'usage des outils numériques, c'est en bonne part à cause de la gamification qui caractérise la plupart des plateformes de masse. Bon nombre de risques liés aux usages des technologies reposent sur des éléments « infratechniques » : habitudes à telle ou telle pratique ou manière de faire, addiction à telle ou telle plateforme, incapacité à faire quelque chose sans telle ou telle application… Une couche de chiffrement ou un simple passage au logiciel libre n'y change rien ! Aujourd'hui on « joue » beaucoup

trop. On joue en ligne – et pas seulement à des jeux – afin d'accéder à des statuts, à des privilèges, de recevoir le plus de *likes* possibles, voire pour gagner un peu de cryptomonnaie. Tous ces dispositifs sont créés en insérant des schémas de jeu au sein d'activités et de procédures qui n'ont rien à voir avec des jeux et dont tout l'enjeu est de servir les propriétaires des plateformes numériques. Contrairement aux jeux traditionnels, dans ces jeux *gamifiés*, on ne trouve ni rituels d'entrée ou de sortie clairs (à part peut-être l'insertion du nom d'utilisateur et du mot de passe, souvent automatisé), ni distinction des espaces (on nous invite à être connectés aux plateformes en permanence). Quand aux prix, aux likes, aux statuts, aux badges, etc., ils visent à nous inciter à une perpétuelle compétition, ils nous engagent, sans même que nous nous en rendions compte, à produire toujours plus (notamment des données et métadonnées, la matière première de l'économie du profilage) tout en nous récompensant à coup de décharges de dopamine.

Devant l'ampleur du phénomène, nous avons donc décidé de travailler sur la dimension ludique de nos ateliers. Les jeux que nous proposons sont bien différents de ces jeux gamifiés. Ils visent même à démasquer les schémas de jeux subrepticement introduits dans toutes sortes d'activités en ligne, à en explorer les dimensions et les implications sociales politiques et psychologiques. Nous cherchons à déprogrammer les automatismes que les jeux de la domination ont construits en nous.

La méthode suivie dans nos laboratoires est donc aussi une déclaration d'intention : en tant que « hackers » nous jouons pour libérer le jeu, pour récupérer sa dimension révolutionnaire ou encore le fait qu'il implique un acte libre ouvert, créatif – comme a pu le montrer Johan Huizinga à la fin des années trente dans son ouvrage *Homo Ludens*. Le jeu n'est donc pas utilisé comme un outil éducatif pour « apprendre en s'amusant », mais parce qu'il est susceptible de réveiller des capacités à imaginer, à subvertir… Parce qu'il est capable de faire tomber certaines barrières aussi, celles liées aux difficultés techniques qui vont de pair avec le monde de l'informatique notamment. La récompense en tout cas est à même le jeu. Nous sommes les prix, ou plutôt, tout l'enjeu est de nous reconquérir de faire un pas de plus dans le sens de notre émancipation.

Ippolita

Notes :

1. La théorie du « Nudge », issue des sciences comportementales, veut que les suggestions indirectes et les incitations soient plus efficaces que la contrainte ou l'obligation directes. Elle est un composant théorique de bien des dispositifs de l'informatique de la domination.
2. Voir l'article de Tomás Ibáñez sur le nouveau totalitarisme dans ce numéro.
3. Traduction de *Personal Computer*, PC.
4. Voir à ce propos notre ouvrage : Ippolita, *J'aime pas Facebook*, Paris, Payot, 2012.
5. Voir hackmeeting.org/.
6. Évoquées notamment dans le texte de Crimthlnc. publié dans ce numéro.
7. https://guide.boum.org/.

Rafaëlle Gandini Miletto. Photographie. Barcelone, 2012. (CC BY SA)