Vous êtes « natif du numérique » ? – Ce n'est pas si grave, mais…

La vie privée est-elle un problème de vieux cons ? demandait Jean-Marc Manach dans un excellent ouvrage. Bien sûr que non, mais on aimerait tant nous le faire croire…

« Natifs numériques », « natifs du numérique », « génération numérique »… Ce genre d'expressions, rencontrées dans les grands médias désireux d'agiter le grelot du jeunisme, peut susciter quelque agacement. D'autant que cette catégorie soi-disant sociologique se transforme bien vite en cible marketing pour les appétits des mastodontes du Web qui ont tout intérêt à présenter la jeunesse connectée comme le parangon des usages du net.

En s'attaquant à cette dénomination, Cory Doctorow [1] entend aussi remettre en cause ce préjugé. Selon lui, les adolescents sont tout à fait soucieux de la confidentialité et de leur vie privée. Mais ils sont loin de maîtriser tous les risques qu'ils sont susceptibles de prendre et comme nous tous, ils ont besoin d'outils et dispositifs qui les aident…

Vous n'êtes pas un « natif numérique » : la vie privée à l'ère d'Internet

par Cory Doctorow sur ce blog

Traduction Framalang : Amargein, lamessen, r0u, teromene, goofy, Clunär

On raconte que Frédéric II, à la tête du Saint-Empire Romain germanique, avait ordonné qu'un groupe d'enfants soit élevé sans aucune interaction humaine, afin que l'on puisse étudier leur comportement « naturel », sans que celui-ci ne soit corrompu par la culture humaine, et découvrir ainsi la véritable nature profonde de l'animal humain.

Si vous êtes né au tournant du XXIe siècle, vous avez certainement dû supporter au moins une fois que quelqu'un vous appelle « natif numérique ». Dans un premier temps, ça sonne de façon plutôt sympathique : une éducation préservée du monde hors ligne et très imprégnée d'une sorte de sixième sens mystique, donnant l'impression de savoir ce que devrait être Internet.

Mais les enfants ne sont pas d'innocents mystiques. Ce sont de jeunes personnes, qui apprennent à devenir adultes de la même manière que les autres : en commettant des erreurs. Tous les humains se plantent, mais les enfants ont une excuse : ils n'ont pas encore appris les leçons que ceux qui se sont déjà plantés peuvent leur éviter. Si vous voulez doubler vos chances de réussite, vous devez tripler vos risques d'échec.

Le problème quand vous êtes catalogué « natif numérique », c'est que cela transforme toutes vos erreurs en une vérité absolue sur la manière dont les humains sont censés utiliser Internet. Ainsi, si vous faites des erreurs concernant votre vie privée, non seulement les entreprises qui vous incitent à les commettre (pour en tirer profit) s'en sortent impunies, mais tous ceux qui soulèvent des problèmes de vie privée sont exclus d'emblée. Après tout, si les « natifs numériques » sont censés ne pas être soucieux de leur vie privée, alors quiconque s'en préoccupe sérieusement passe pour un dinosaure complètement à la ramasse, plus du tout en phase avec ''les Jeunes''.

« Vie privée » ne signifie pas que personne au monde ne doit être au courant de vos affaires. Cela veut dire que c'est à vous de choisir qui peut s'en mêler.

Quiconque y prête attention s'apercevra qu'en réalité, les enfants se soucient énormément de leur vie privée. Ils ne veulent surtout pas que leurs parents sachent ce qu'ils disent à leurs amis. Ils ne veulent pas que leurs amis les voient dans leurs relations avec leurs parents. Ils ne veulent pas que leurs professeurs apprennent ce qu'ils pensent d'eux. Ils ne veulent pas que leurs ennemis connaissent leurs peurs et leurs angoisses.

Ceux qui veulent s'insinuer dans la vie privée des jeunes ne communiquent pas du tout sur ce point. Facebook est une entreprise dont le modèle économique repose sur l'idée que si elle vous espionne suffisamment et vous amène à révéler malgré vous suffisamment sur votre vie, elle pourra vous vendre des tas de trucs à travers la publicité ciblée. Quand on l'interpelle sur ce point, elle se justifie en disant que puisque les jeunes finissent par dévoiler tant de choses de leur vie personnelle sur Facebook, ça ne doit pas être un problème, vu que les natifs numériques sont censés savoir comment se servir d'Internet. Mais quand les gamins grandissent et commencent à regretter ce qu'ils ont dévoilé

sur Facebook, on leur dit qu'eux non plus ne comprennent plus ce que ça signifie d'être un natif numérique, puisqu'ils sont devenus adultes et ont perdu le contact avec ce qui fait l'essence même d'Internet.

Dans « It's Complicated: The Social Lives of Networked Teens[2] » [NdT « La vie sociale des jeunes connectés, un problème complexe »], une chercheuse nommée danah boyd[3] résume plus de dix ans d'étude sur la manière dont les jeunes utilisent les réseaux, et dévoile une lutte continue, voire désespérée, pour préserver leur vie privée en ligne. Par exemple, certains des jeunes interviewés par Boyd suppriment leur compte Facebook à chaque fois qu'ils s'éloignent de leur ordinateur. Si vous supprimez votre compte Facebook, vous avez six semaines pour changer d'avis et réactiver votre compte, mais durant le temps où vous êtes désinscrit, personne ne peut voir votre profil ou quelque partie que ce soit de votre journal (''timeline''). Ces jeunes se réinscrivent sur Facebook à chaque fois qu'ils reviennent devant leur ordinateur, mais s'assurent de cette manière que personne ne peut interagir avec leur double numérique à moins qu'ils ne soient là pour répondre, supprimant les informations si elles commencent à leur causer des problèmes.

C'est assez extraordinaire. Cela nous enseigne deux choses : premièrement, que les jeunes vont jusqu'à prendre des mesures extrêmes pour protéger leur vie privée ; deuxièmement, que Facebook rend extrêmement difficile toute tentative de protection de notre vie privée.

Vous avez certainement entendu un tas d'informations concernant Edward Snowden et la NSA. En juin dernier, Edward Snowden, un espion étatsunien, s'envola pour Hong Kong et remit à un groupe de journalistes étatsuniens des documents internes à la NSA. Ces documents décrivent un système d'une ampleur presque inimaginable – et absolument illégal – de

surveillance d'Internet de la part des agences de surveillance étatsuniennes. Celles-ci choisissent littéralement au hasard un pays et enregistrent le moindre appel téléphonique passé depuis ce pays, juste pour voir si cela fonctionne et peut être transposé dans d'autres pays. Ils puisent littéralement dans le flux complet d'informations circulant entre les centres de données de Google ou de Yahoo, enregistrant les parcours de navigation/, les e-mails, les discussions instantanées et d'autres choses dont personne ne devrait avoir connaissance chez des milliards de personnes innocentes, y compris des centaines de millions d'Étatsuniens.

Tout cela a modifié les termes du débat sur la vie privée. Tout à coup, les gens ordinaires qui ne se préoccupaient pas de la vie privée s'y sont intéressés. Et ils ont commencé à penser à Facebook et au fait que la NSA avait récolté beaucoup de données par leur biais. Facebook a collecté ces données et les a mises à un endroit où n'importe quel espion pouvait les trouver. D'autres personnes dans le monde y avaient déjà pensé. En Syrie, en Égypte et dans beaucoup d'autre pays, rebelles ou agents du gouvernement ont mis en place des barrages que vous ne pouvez franchir qu'en vous connectant à votre compte Facebook de sorte qu'ils ont accès à votre liste d'amis. Si vous êtes ami-e avec les mauvaises personnes, vous êtes abattu ou emprisonné ou bien vous disparaissez.

Les choses ont été si loin que Marck Zuckerberg – qui avait dit à tout le monde que la vie privée était morte tout en dépensant 30 millions de dollars pour acheter les quatre maisons à côté de la sienne afin que personne ne voie ce qu'il faisait chez lui – a écrit une lettre ouverte au gouvernement des États-Unis pour lui reprocher d'avoir « tout gâché ». Comment avait-il tout gâché ? Ils ont montré au gens d'un seul coup que toutes leurs données privées étaient en train de migrer de leur ordinateur vers ceux de Facebook.

Les enfants savent intuitivement ce que vaut la vie privée.

Mais comme ce sont des enfants, ils ont du mal à comprendre tous les détails. C'est un long processus que d'apprendre à bien la gérer, car il se passe beaucoup de temps entre le moment où on commence à négliger la protection de sa vie privée et celui où les conséquences de cette négligence se font sentir. C'est un peu comme l'obésité ou le tabagisme. Dans les cas où une action et ses conséquences sont clairement distinctes, c'est une relation que les gens ont beaucoup de peine à comprendre. Si chaque bouchée de gâteau se transformait immédiatement en bourrelet de graisse, il serait bien plus facile de comprendre quelle quantité de gâteau était excessive.

Les enfants passent donc beaucoup de temps à réfléchir sur leur vie privée préservée de leur parents, des enseignants et de ceux qui les tyrannisent, mais ils ne se demandent pas à quel point leur vie privée sera protégée vis-à-vis de leurs futurs employeurs, de l'administration et de la police. Hélas, au moment où ils s'en rendent compte, il est déjà trop tard.

Il y a toutefois de bonne nouvelles. Vous n'avez pas à choisir entre une vie privée et une vie sociale. De bons outils sont disponibles pour protéger votre vie privée, qui vous permettent d'aller sur Internet sans avoir à livrer les détails intimes de votre vie aux futures générations d'exploitants de données. Et parce qu' il y a des millions de personnes qui commencent à avoir peur de la surveillance – grâce à Snowden et aux journalistes qui ont soigneusement fait connaître ses révélations – de plus en plus d'énergie et d'argent sont utilisés pour rendre ces outils plus faciles à utiliser.

La mauvaise nouvelle, c'est que les outils propices à la vie privée tendent à être peu pratiques. C'est parce que, avant Snowden, quasiment tout ceux qui se sentaient concernés par l'adéquation entre leur vie privée et la technologie étaient déjà experts d'un point de vue technologique. Non pas parce

que les nerds ont besoin de plus de vie privée que les autres, mais parce qu'ils étaient les plus à même de comprendre quel genre d'espionnage était possible et ce qui était en jeu. Mais, comme je le dis, cela change vite (et les choses ne font que s'améliorer).

L'autre bonne nouvelle c'est que vous êtes des « natifs numériques », au moins un peu. Si vous commencez à utiliser des ordinateurs étant enfant, vous aurez une certains aisance avec eux, là où d'autres auront à travailler dur pour y parvenir. Comme Douglas Adams l'a écrit :

1. Tout ce qui existe dans le monde où vous êtes né est normal et ordinaire, et ce n'est qu'un rouage dans le mécanisme naturel du système.

2. Tout ce qui est inventé entre le moment de vos quinze ans et celui de vos trente-cinq est nouveau, excitant et révolutionnaire et vous pourrez probablement y faire carrière.

3. Tout ce qui sera inventé après vos trente-cinq ans est contraire à l'ordre naturel des choses.

Si j'étais un enfant aujourd'hui, je saurais tout au sujet des sécurités opérationnelles. J'apprendrais à me servir d'outils pour garder mes affaires entre moi et les personnes avec qui j'aurais décidé de les partager. J'en ferais une habitude, et j'inciterais mes amis à adopter cette habitude aussi (après tout, ça ne change rien si tous vos e-mails sont chiffrés mais que vous les envoyez à des idiots qui les gardent tous sur les serveurs de Google sous une forme déchiffrée, là où la NSA peut venir y fourrer son nez).

Voici quelques liens vers des outils de sécurité pour vous y initier :

- Tout d'abord, téléchargez une version de Tails (pour « The Amnesic Incognito Live System »). Il s'agit d'un

système d’exploitation que vous pouvez utiliser pour démarrer votre ordinateur sans avoir à vous soucier si le système d’exploitation installé est exempt de tout virus, enregistreur de frappe ou autre logiciel-espion. Il est fourni avec une tonne d’outils de communication sécurisés, ainsi que tout ce dont vous avez besoin pour produire les contenus que vous souhaitez diffuser de par le monde.

- Ensuite, téléchargez une version du Tor Browser Bundle, une version spéciale de Firefox qui envoie automatiquement votre trafic à travers quelque chose appelé TOR (The Onion Router, le routeur en oignon, à ne pas confondre avec Tor Books, qui publie mes nouvelles). Cela vous permet de naviguer sur Internet avec beaucoup plus d’intimité et d’anonymat que vous n’en auriez normalement.
- Apprenez à utiliser GPG, qui est une excellente manière de chiffrer vos courriers électroniques. Il existe une extension pour Chrome qui vous permet d’utiliser GPG avec GMail et une autre pour Firefox.
- Si vous appréciez les messageries instantanées, procurez-vous OTR (« ’’Off The Record messaging’’ »), un outil pour sécuriser ses conversations en ligne, incluant des fonctionnalités telles que « l’inviolabilité des messages passés » (une façon de dire que même si quelqu’un arrive à le casser demain, il ne pourra pas lire les conversations interceptées aujourd’hui).

Une fois que vous aurez maîtrisé ce genre de choses, mettez-vous à réfléchir à votre téléphone. Les appareils sous Android sont de loin plus faciles à sécuriser que les iPhones d’Apple (Apple essaie de verrouiller ses téléphones pour que vous ne puissiez pas y installer d’autres logiciels que ceux de leur logithèque, et en raison de la loi DMCA de 1998, il est

illégal de créer un outil pour les déverrouiller (''jailbreaker''). Il existe de nombreux systèmes d'exploitation concurrents d'Android, avec des niveaux variables de sécurité. Le meilleur point de départ est Cyanogenmod, qui vous facilitera l'utilisation d'outils de confidentialité sur votre mobile.

Il existe également des quantités de projets commerciaux qui traitent la vie privée bien mieux que le tout-venant. Je suis par exemple consultant de l'entreprise Wickr, qui reproduit les fonctionnalités de Snapchat mais sans moucharder à tout moment. Wickr a cependant beaucoup de concurrents, il vous suffit de regarder dans votre logithèque préférée pour vous en convaincre, mais assurez-vous d'avoir bien lu comment l'entreprise qui a conçu l'application vérifie que rien de louche ne vient interférer avec vos données supposées secrètes.

Tout ceci est en constante évolution, et ce n'est pas toujours facile. Mais c'est un excellent exercice mental que de chercher comment votre usage d'Internet peut vous compromettre. C'est aussi une bonne pratique dans un monde où des milliardaires voyeurs et des agences d'espionnage hors de contrôle essayent de transformer Internet en l'outil de surveillance le plus abouti. Si vous trouvez particulièrement pénible que vos parents espionnent votre historique de navigation, attendez que tous les gouvernements et toutes les polices du monde en fassent autant.

Notes

[1] Lisez ses très bons romans, notamment Little Brother

[2] Lien direct vers le téléchargement de cet essai au format PDF, en anglais : http://www.danah.org/books/ItsComplicated.pdf

[3] …et non Danah Boyd, c'est elle qui insiste pour ne pas

mettre de capitales à ses nom et prénom, dit sa page Wikipédia