L'Assistance à la Désobéissance Numérique.
So What!

By
Thierno M. SOW
18 décembre 08

Faudrait-il que,
la désobéissance numérique
soit
la révolution majeure au 21em siècle
soit
la désobéissance numérique.
Faudrait-il que.

Thoreau avait-il vu juste au 19em siècle, en posant les fondements théoriques de la désobéissance civile, « le meilleur gouvernement est celui qui gouverne le moins » disait-il (1). Pourtant, dans l'éventualité d'une citoyenneté numérique à assumer il y a nécessairement des droits rattachés à la protection des personnes et des biens numériques que tout gouvernement devrait rendre effectifs. En effet, l'équilibre entre la citoyenneté et les différents types de pouvoir exorbitant est fondamental voire vital pour la bonne cohabitation au sein des sociétés numériques.

Cependant, il ne cesse de se creuser entre les différents acteurs un fossé technologique qui participe de la fragilisation d'un type de citoyenneté au profit de l'autre, entre les **utilisateurs** et les **initiateurs** numériques. En effet, l'élément fondamental qui distingue l'Etat des autres sociétés morales réside dans le monopole par celui-ci de la contrainte organisée. Or, les sociétés numériques pullulent de milices et d'organisations privées qui abusent des moyens de police et agissent en toute impunité. Dés lors, la célèbre assertion de Montalembert en 1840 se vérifie-t-elle encore de nos jours, en ce qu'elle résume parfaitement cet ensauvagement qui aboutit à la situation du « loup libre dans le poulailler libre ». Ainsi, la liberté et l'égalité vont-elles déboucher inéluctablement sur une fraternité dramatique entre le loup et les autres membres de l'écosystème numérique.

Par ailleurs, une formation à la citoyenneté numérique est indispensable au rééquilibrage entre les différents citoyens et l'absence d'initiation à la république numérique est comparable à la situation de nos sociétés avant l'établissement de l'école publique obligatoire selon le modèle de Jules Ferry. Il est d'ailleurs curieux que cette obligation ne soit toujours pas organisée et supportée aussi bien financièrement que techniquement par les constructeurs

et fabricants de matériel (hard) et de logiciel (soft) numériques. La protection des droits d'auteur des fabricants de logiciel doit être assurée par les États à la seule condition que la contre partie sur la sécurité effective des utilisateurs et des citoyens numériques soit assurée. Ainsi, différents abus de pouvoir s'étendent ostensiblement au sein des sociétés numériques.

Des sociétés d'anonymat numérique.
Comme pour la crise des années 1930, l'érection spontanée ainsi que les disparitions subites des sociétés numériques s'intensifient avec la crise financière actuelle. A ce phénomène s'ajoute tout naturellement celui des écrans de fumée et des pièges en tout genre (empoisonnements par DNS, pishing, etc.). Nul ne peut déterminer avec certitude l'authenticité de la page web qui s'affiche à l'écran d'un ordinateur, comme s'il existait un monde numérique parallèle pour combler notre insuffisance de virtualité. A ce titre, le mot écran est révélateur en ce qu'il renferme l'idée même d'une réalité ou d'une supercherie qui se cacherait derrière un rideau en cristaux liquide, en TFT ou en LED. Les enjeux sont colossaux et les dégâts aussi. En effet, à côté des désastres financiers que de telles pratiques occasionnent, il existe le risque permanent que la désinformation vienne ruiner les fondements intellectuels et moraux de la majeure partie de nos concitoyens. Sans s'attarder sur les insuffisances des dictionnaires numériques libres, nous pouvons souligner l'irresponsabilité de telles initiatives d'une part, et l'impossibilité pour les voies autorisées d'y mettre fin, d'autre part. Aussi, l'alibi du renforcement et du partage des connaissances n'est que l'arbre qui cache la forêt économique qui se développe autour des dons et de la publicité. Enfin, l'argument de la contribution citoyenne se pose comme une parade juridique pour parer à toute éventualité d'une poursuite sur le contenu et organise les conditions d'une évaporation numérique préprogrammée. So What !

De l'Impunité et de l'irresponsabilité des industries de la sécurité numérique.
Les utilisateurs sont ponctionnés tous les ans par les fabricants de logiciels de protection numérique; comme s'il fallait dans la réalité que chaque individu recruta un agent pour garantir sa propre sécurité. Or, sans rentrer dans la caricature, nous savons très bien que les meilleurs fabricants de virus sont les fabricants d'anti-virus. De ce fait, s'étend un commerce lucratif de la peur avec l'enrichissement, le nantissement et la multiplication des foyers de diffusion de virus. Par ce biais, l'inventeur d'un virus s'assure un développement professionnel et encourage de ce fait la surenchère au détriment des utilisateurs-cobayes. Aussi, payons-nous tous les ans chez un fabricant d'antivirus, les éventuelles mises à jour pour parer aux virus potentiels auxquels il prétend potentiellement faire face. A notre crédulité s'ajoutent les vices de consentement systématisés. En effet, en cas d'attaque virale, votre fournisseur de protection est hors de cause par l'abus de clause potestative et ne participe en rien à la réparation des dommages occasionnés par le virus. So What !

L'inexistence de recours prompt et efficient.

Pour ce troisième point, il est désastreux de constater que la plainte d'un citoyen lambda pour intrusion informatique et vols de données (voir les articles 323-1 et suivants du code pénal) n'aboutisse sur une enquête sérieuse et sur une condamnation. Pourtant, lorsqu'une personnalité est victime de piratage, des moyens exorbitants sont aussitôt déployés pour identifier les coupables. Devant ce laxisme, les hackers transforment nos espaces numériques de travail en terrain de jeu à partir desquels ils perpétuent leurs crimes à notre insu. Imaginons un seul instant, qu'à chaque fois qu'un citoyen quitte son domicile pour se rendre à son lieu de travail ou vaquer à ses occupations, qu'un intrus s'y installe confortablement. Dans le cas en l'espèce, les hackers ne se gênent même plus pour laisser les traces de leur passage ou de leur séjour qui sur le long terme se termine en résidence numérique secondaire. So What !

L'émergence d'une contre morale numérique.

Ce qui est inadmissible dans la sécurité des citoyens au sein de la république épouse les formes d'une pratique banale voire normale. L'on nous reprocherait presque de ne pas installer d'antivirus sur nos espaces numériques de travail. En effet, nos fournisseurs d'accès Internet ne s'estiment en aucune façon responsables de notre exposition à la cybercriminalité, les vendeurs de système d'exploitation déclinent leur responsabilité face aux victimes et pertes causées par leur propre insuffisance. Dés lors, l'assurance numérique se retrouve du côté des hackers dont l'identité est doublement protégée par le système. En effet, une victime de piratage informatique se voit refuser l'accès à ses logs de connexion. En terme plus clair, si vous demandez à votre fournisseur d'accès de vous communiquer l'origine des intrusions informatiques dont vous êtes victimes, il vous fera savoir que seule la police a le droit d'accéder à ces informations. En gros : « enterrer vos morts et la police gardera en lieu sûr les noms des assassins. Dans un registre plus dramatique, lorsqu'un mineur est exposé aux contenus dangereux et criminels sur Internet, la réponse proposée se résume à la sensibilisation de l'entourage donc à la culpabilisation des parents. Nom de Dieu ! Comment de tels contenus peuvent-ils circuler librement sur un espace numérique public ? Le service public c'est la conjonction et la convergence de trois principes régaliens : la sécurité, la salubrité et la tranquillité. Trois principes totalement inexistants sur Internet. So What !

L'arme de la diffamation massive

N'importe qui peut s'inscrire sur un forum public en usurpant l'identité d'un tiers et diffuser en son nom toute une série d'informations diffamatoires qui portent atteinte à l'honneur d'un honnête citoyen. L'exercice d'une citoyenneté numérique est incompatible avec l'abus d'anonymat. La guerre économique, les jalousies méprisables et la déloyauté usent de la diffamation massive comme arme de concurrence pour nuire aux intérêts d'autrui. Dans le cas où le citoyen ne dispose d'aucun moyen financier, pour solliciter le concours de cabinets spécialisés et organiser sa propre défense, il ne lui reste que ses yeux pour pleurer. Même dans l'éventualité que son innocence soit ultérieurement prouvée, le mal est déjà fait et toute recherche associée à son nom sur les moteurs de recherche révèleront indéfiniment cette fausse

information. So What !

L'apparition de nouveaux fichiers de police a soulevé un mouvement de conscience citoyenne un peu partout dans le monde et pourtant le fichage permanent par les moteurs de recherche produit le même résultat, les mêmes marges d'erreurs et les mêmes stocks d'informations erronées sur les citoyens numériques. Nul ne peut nier l'importance d'un contrôle d'Etat sur les espaces numériques, mais lorsque la police détient un pouvoir exorbitant de contrôle, il y a le risque d'un abus de pouvoir dans l'accès et l'utilisation d'une technologie publique à des fins d'investigations privées. Il n'existe aucune différence entre la problématique des fichiers politiques et l'utilisation politique des moyens d'infiltration numérique. Cependant, le droit est entrainé de plus en plus à la dérive par les détenteurs des pouvoirs numériques exorbitants dans la législation et le renforcement des contraintes juridiques à leur profit exclusif. Le lobby numérique n'existe pas de fait mais plusieurs faisceaux d'indices concourent à son expression derrière le voile de la morale et tentent d'inverser le rapport de force en brandissant l'exercice libre de la citoyenneté numérique comme une forme de parasitage et une menace à l'intégrité de l'économie numérique. La conséquence immédiate de cette absence de « balance » renforce les moyens d'asservissement des utilisateurs numériques et garantit la survie des mauvais initiateurs et des mauvaises pratiques numériques.
Les argumentations avancées sont toujours les mêmes, banales et généralistes : faut-il lutter contre le terrorisme et la pédophilie ? Yes, So What !

Durant la guerre froide, et tout récemment encore, il était fréquent de lire dans la presse l'arrestation en territoire étranger d'espions ou d'agents du renseignement. Or, de nos jours, n'importe quel citoyen numérique travaille à son insu au profit de tous les services de renseignement du monde entier. En effet, par le micro, la caméra, les terminaux à fréquences hertziennes ainsi que le GPS de son ordinateur et de son téléphone portables, l'utilisateur numérique fournit toutes les informations privées sur sa personne et sur son entourage et devient de ce fait un parfait agent infiltré. Seulement, à partir du moment où le traçage numérique ne permet pas d'anticiper sur les actions criminelles quelles relèvent du terrorisme de la pédophilie ou du crime organisé, il est amer de constater que le renseignement opère une mutation vers le journalisme de faits divers en ce qu'il n'use de moyens numériques exorbitants que pour remonter *a posteriori* des faits antérieurs et des crimes déjà commis.

De cette situation, découle une relation de manipulations et d'intoxications permanente entre les journalistes et les agents de renseignement. Cette nouvelle forme de journalisme sur Internet constitue la matrice d'un phénomène qui porte le nom de « Buzz ». En effet, le Buzz précède à l'information destinée à le démentir ou à le confirmer. La lutte contre le terrorisme et la cybercriminalité ne doit pas aboutir à un renversement des rôles qui userait de moyens et de pratiques terroristes et criminelles sous prétexte de les combattre ou pour atteindre des opposants politiques. Ainsi, plusieurs questions permettent de souligner l'importance dans l'équilibrage

entre les objectifs supposés et les moyens pour éviter la disproportion et les procédures abusives : Doit-on fouiller le sac de toutes les demoiselles à chaque coin de rue ? La police et tous les serruriers doivent-ils s'introduire chez les citoyens à leur insu ? Tous les écrivains doivent-ils envoyer une copie des mises à jour de leurs manuscrits à la censure ? So What !

Si la fouille au corps est une éthique professionnelle quelconque (médicale, professorale, styliste, miss monde, aviation civile) que **les seuls assermentés se doivent rigoureusement d'appliquer sur eux-mêmes**, depuis quand un code déontologique vaut le code pénal et depuis quand un code déontologique d'une profession s'applique aux non-professionnels. So What !

Si tous les moyens de police avaient été braqués sur les banques et les bourses, nous aurions assurément évité la crise financière internationale. Le cas échéant, les Etats sont-ils doublement acteurs et complices de la délinquance au col blanc. Yes, So What ! Sous ce rapport il apparaît qu'à la différence de la citoyenneté « naturelle », le citoyen numérique apparaît comme un délinquant anonyme jusqu'à preuve du contraire.

Pourtant, la citoyenneté numérique nous semble-t-il acquise à des individus plus et mieux éduqués que l'homme de l'Agora. Alors en quoi le numérique nous désarme-t-il face à toutes ces formes d'abus contre lesquels nous avons bâtis les principes fondateurs des civilisations du 21em siècle.

De nos jours, le numérique mobilise notre attention plus de 02 heures par jour. Nous consacrons plus de temps à nos activités numériques qu'à d'autres sociales et humaines. La citoyenneté numérique n'est donc pas une figure de style ou un artifice de modernité, c'est une réalité numérique et non virtuelle. Nos outils numériques contiennent plus de confidences et d'informations sensibles et personnelles que nous en sachions sur nous-mêmes. A chaque fois, qu'un citoyen s'équipe numériquement, il cède une part de ses droits et de ses libertés. A chaque fois, qu'un citoyen ouvre un espace numérique, il crée les conditions de sa propre incarcération numérique.

A la question du rôle de l'Etat, rappelons que Thoreau n'a jamais été un antigouvernemental mais en tant que citoyen réclamait-il : « non une absence immédiate de gouvernement, mais *immédiatement* un meilleur gouvernement ». En effet, la gouvernance numérique doit être un principe de constitutionalité pour tous les Etats modernes au 21em siècle et reste un idéal républicain contre les abus et les erreurs du passé. Ainsi, à l'insistance d'un disciple qui demandait : « qu'est-ce que gouverner ? » Confucius répétait plusieurs fois : "gouverner, c'est rectifier".

Cependant, si la démocratie numérique est un processus et un long cheminement, tout porte à croire que malgré tout ce qui lui arrive, notre citoyen continu d'entretenir la survie d'un système dont il est le seul à même de stopper. Seulement, tant qu'il n'aura pas atteint la majorité numérique et

reçu le kit de l'assistance à la désobéissance numérique, il ne sera pas encore apte à exercer pleinement sa qualité de citoyen numérique.
Yes, So What!

Thierno M. SOW
Expert Consultant
Cabinet One-Zero Consulting
10@one-zero.eu
www.one-zero.eu

1/ Henry David Thoreau, *civil disobedience*,1849.