

Les Anonymous doivent-ils laisser tomber le masque ?

Une traduction un brin polémique autour du fameux masque symbolisant les [Anonymous](#).

Aussi joli soit-il, il pose quelques problèmes qui peuvent effectivement contrarier la posture et brouiller le message des actions de cet étrange et fuyant collectif.

Le masque fait référence à [Guy Fawkes](#), personne historique anglais du XVIIe siècle, mais il a pour auteur le dessinateur contemporain [David Lloyd](#) de [V pour Vendetta](#). Il est devenu célèbre après l'[adaptation de la BD au cinéma](#). Film produit par [Time Warner](#) qui détient les droits à l'image sur le masque et à qui on doit payer une obole à chaque exemplaire du masque vendu (légalement).

Premier problème, le masque est sous copyright classique. Deuxième problème, il appartient à l'une de ces multinationales souvent prises pour cible par les Anonymous. Et, dernier problème, il semblerait qu'il soit produit dans les pires conditions du capitalisme mondialisé, c'est en tout cas ce que le laisse croire [cette photo](#) qui a semé le trouble et provoqué l'article très critique ci-dessous.

On aurait aimé qu'il fut dans le domaine public. Chiche qu'on demande tous à Time Warner combien ils veulent pour qu'il en soit ainsi et qu'on monte un crowdfunding dans la foulée pour récolter la somme □

,



L'hypocrisie des Anonymous a été dévoilée. Et maintenant ils font des pieds et des mains pour se défendre.

[Anonymous have been exposed as hypocrites. Watch them try to wriggle out of it](#)

Martha Gill – 6 novembre 2013 – The Telegraph (blog)

"(Traduction : lyn, Eiyeron, MFolschette, Catalaburro, Sky, M0tty + anonymes)"

Anonymous est une organisation définie surtout par ce que ses membres ont choisi de se mettre sur la tête, le fameux masque de V pour Vendetta. Mais depuis hier le masque a connu quelques problèmes techniques. Il semblerait qu'il défigure celui qui le porte.

Le jour de Guy Fawkes, juste à temps pour l'opération [Million Mask March](#), [cette photo](#) de Reuters est apparue en page d'accueil de Reddit. Elle montre les masques fabriqués en masse dans une usine au Brésil. Ce n'est peut-être pas un atelier clandestin, mais c'est pourtant le mot que beaucoup ont à la bouche actuellement (d'autres photographies [en suivant ce lien](#)).

Cela ne correspond guère avec l'image du groupe. Anonymous

lutte contre les effets du capitalisme globalisé – protestant contre de grandes entreprises menant la vie dure aux ouvriers. Et pourtant, on peut voir ces ouvriers, dans de mauvaises conditions de travail, fabriquant les masques des protestataires. Par ailleurs, on sait depuis pas mal de temps que Time Warner, une des plus grandes entreprises audiovisuelles au monde, [fait du bénéfice](#) chaque fois qu'un de ces masques est vendu.

Tout cela n'est-il pas légèrement... hypocrite ?

Le compte pro-Anonymous @youranoncentral a essayé de calmer Twitter : « Ecoutez tous, nos masques ont été fabriqués dans un pays en voie de développement. Nous sommes les seuls hypocrites. »

Et plusieurs personnes partagèrent des points de vue similaires à [sayheykid24](#) sur Reddit : « Comment les gens pensent que ces masques ont été faits ? Pensaient-ils qu'ils étaient fait à la main et avec amour par des artisans opposés au grand capital ? »

En effet, que croyions-nous ? Il serait plus simple, plus économique et plus efficace pour les Anonymous de faire fabriquer des masques à la chaîne dans des pays en voie de développement. C'est généralement comme ça que de tels objets sont fabriqués. Cela serait également beaucoup demander à Anonymous que de s'assurer qu'aucune grande entreprise ne tire profit de leurs protestations. Et forcément, étant donné qu'Anonymous est un petit groupe faisant face à de grosses organisations sans scrupules, ils voudront réaliser l'opération la plus percutante possible, quitte à être aussi sans scrupules. Ils peuvent difficilement se permettre de ne pas l'être.

Mais si nous pensions cela nous aurions tort. Ces pressions économiques sont la raison pour laquelle l'industrie du disque a réprimé le piratage numérique et aussi pourquoi Mastercard

et Visa ont mal agi envers certains clients – tous des ennemis, tous des Anonymous attaqués pour ces mêmes raisons. Étant donné qu'Anonymous demande aux entreprises de prendre une position inconfortable mais morale contre le système auquel elles sont soumises, si eux-mêmes n'y parviennent pas, ils sont alors eux-mêmes hypocrites. (Fabriquer un masque de Guy Fawkes est plus simple à réaliser chez soi, non ?)

Est-ce important ?

Bien sûr que ça l'est. C'est vrai que les Anonymous ne sont pas les seuls hypocrites. Mais tous les hypocrites ne sont pas entièrement dépendants de leur posture morale. Le fait de punir le mauvais comportement d'autrui fait partie intégrante du message des Anonymous – ils suggèrent de les rejoindre pour être de côté des gentils. Cela signifie que le groupe repose uniquement sur son intégrité morale – et s'ils ne peuvent se permettre de jouer selon leurs propres règles, ils ne peuvent certainement pas non plus se permettre de les enfreindre.

Le dernier problème avec le masque recensé à cette date a montré son (pas si vilain) visage hier. Il s'avère que, bien que cet accessoire soit pratique pour les vendettas masquées, il l'est moins pour se mettre publiquement en valeur. Que se passe-t-il quand la marche organisée, basée sur la notion d'anonymat, attire une célébrité tel que [Russel Brand](#) parmi ses rangs ? Brand a résolu le problème [en tweetant des photos de lui-même portant son masque](#). Encore une fois, quelle ironie...

Framasoft et Smile unis dans

un mécénat de compétences

Nous nous sommes engagés avec la société [Smile](#), spécialisée dans l'intégration de solutions libres, dans un **mécénat de compétences** autour de la refonte de notre annuaire de logiciels libres, appelé désormais « Framalibre ». Sa mise en œuvre et son suivi seront assurés par Cyrille Assire pour Smile (ci-dessous à droite) et Alexis Kauffmann pour Framasoft (à gauche).



L'[annuaire de logiciels libres](#) est le premier projet du réseau Framasoft. C'est celui pour lequel tout a commencé pour nous et même s'il côtoie désormais une vingtaine d'autres projets, il demeure encore le plus fréquenté. Mais force est de constater qu'il a pris la poussière avec le temps, dans le fond comme dans la forme. Il continue à rendre ses services au quotidien mais il a grand besoin d'être mis à jour. Smile va ainsi participer à la refonte ergonomique et graphique du site

en nous aidant à repenser globalement le projet et proposer une interface plus fonctionnelle et aboutie.

Le mécénat se distingue du parrainage (sponsoring en anglais) en ce qu'il n'y a pas de contrepartie. Si le mécénat financier ou en nature sont connus, le [mécénat de compétences](#) reste un dispositif encore peu répandu. Il permet ici à Smile de mettre à disposition de Framasoft les compétences professionnelles de ses employés pendant leur temps de travail (et sans aucune perte financière). Il donne un nouveau visage au mécénat en le rendant plus solidaire et participatif et permet de faire en sorte que les entreprises et les associations se rencontrent et se rapprochent. Framasoft étant une association reconnue d'intérêt général, Smile va pouvoir déduire de son IS (Impôt sur les Sociétés) 60% des salaires chargés des collaborateurs missionnés, au prorata des heures effectuées pour nous.

Nous vous tiendrons régulièrement au courant des avancées de ce partenariat. Et nous serions ravis de voir d'autres entreprises prendre le sillage de Smile dans le mécénat de compétences parce que ce ne sont pas les besoins qui manquent dans le Libre associatif.

Le logiciel libre a fait de moi l'homme que je suis

Le témoignage simple et percutant d'un développeur qui a visiblement fait le bon choix ☐



L'open source a fait de moi l'homme que je suis

[Open Source made me the man I am](#)

Matteo Spinelli – 6 octobre 2013 – Cubiq.org

(Traduction : Asta, Joseph, GregR, aKa, Cyb, Spanti Nicola, Lydie + anonymes)

De la conception de sites web pour les entreprises nationales au développement d'applications web haut de gamme pour les plus grands acteurs internationaux, tout cela grâce aux logiciels libres.

J'ai longtemps été un (triste) programmeur PHP en freelance ayant quelques compétences en front-end. Je travaillais pour de petites boîtes locales. Mon job le plus sympa en ce temps-là a été avec un distributeur de jeux vidéo, chez moi, en Italie. Le client était sympa, mais le boulot était chiant, et si frustrant parfois.

Je savais que je pouvais donner plus, mais je me sentais pris dans des sables mouvants.

La décision la plus importante que j'ai prise dans ma carrière a été de commencer à développer un logiciel libre et de bloguer sur ce sujet. J'ai commencé avec des trucs un peu stupides, comme un [générateur d'URL épuré](#) en PHP ou la [suppression du délai sur l'évènement onClick](#) et j'ai fini avec [iScroll](#) et l'[ajout de widgets à l'écran d'accueil](#).

J'ai choisi pour eux la licence la plus libre que j'ai pu trouver ([MIT](#)) et les entreprises à travers le monde m'ont contacté pour me demander de la personnalisation et des nouvelles fonctionnalités. Mon tarif horaire était autour de 60 \$ et j'ai dû l'augmenter sur une base à la journée parce que je ne pouvais pas suivre avec l'augmentation des demandes. Maintenant je suis toujours travailleur indépendant mais je travaille pour **Microsoft** et **Google** et mon tarif horaire est de 150 \$.

L'*open source* a augmenté ma visibilité mais ce n'est pas qu'une question *d'audience*. L'*open source* fait généralement de vous un meilleur développeur. Cela vous force à vous comparer vous-même avec d'autres développeurs et c'est le meilleur entraînement pour votre cerveau de codeur.

J'ai plus appris sur le JavaScript des gens postant des suggestions sur le rapporteur de bogues que sur n'importe quel guide, tutoriel ou livre que j'aie jamais lu.

Les logiciels libres m'ont fait également devenir un développeur plus modeste. Je sais comment patcher de petites portions de code et je suis moins sévère quand je remonte des bogues sur les dépôts des autres.

Mais c'est juste une partie de l'histoire.

Vous ne faites pas des logiciels libres juste pour la gloire (et l'argent). Peut-être qu'au début c'était mon intention,

mais une fois que vous êtes impliqué vous comprenez que vous faites bien plus.

Beaucoup de gens utilisent votre code, vous aidez les startups dans leur projet en créant potentiellement de nouveaux emplois. Avec peut-être 48h de votre vie, vous pouvez possiblement aider des dizaines d'entreprises et leurs employés. Une personne a fait un plugin pour WordPress qui était essentiellement une couverture PHP pour mon *Ajouter à l'écran d'accueil* et il a levé 50k\$ de fonds (peut-être plus maintenant). Vous pouvez penser que je suis jaloux de lui, mais je suis en fait heureux pour lui (et tous ses utilisateurs).

En outre, plus je développe du logiciel libre plus j'apprécie les autres logiciels libres et j'en deviens accro. Je comprends ce que signifie coder pour la **sécurité** et, plus particulièrement, l'importance de la **vie privée** de l'utilisateur (et la mienne).

J'étais un fervent utilisateur d'Apple parce que c'est joli et bien rangé et cela fonctionne simplement, mais peut-être qu'il y a des choses plus importantes qu'une interface de qualité et un dégradé parfait de pixels. J'utilise maintenant les produits Apple seulement pour tester et ma plateforme principale est Linux.

Je peux sans hésiter dire que l'*open source* a fait de moi un homme meilleur et je vous encourage à publier votre code sous une licence libre, parce que si ça a marché avec moi, ça marchera probablement avec vous aussi.

Crédit photo : [Beshef](#) (Creative Commons By)

Concurrence déloyale des logiciels libres en Europe ? La réponse de la FSFE

Le groupe de pression « [FairSearch](#) » (Microsoft, Nokia, Oracle...) prétend que Android fausse la concurrence parce qu'il est libre et gratuit et vient s'en plaindre à la Commission Européenne.

Traduite par nos soins, une réponse de la [Free Software Foundation Europe](#) s'imposait.



Les objections de la FSFE aux prétendues pratiques de « prix prédateurs » des logiciels libres

[FSFE objects to claims of 'predatory pricing' in Free Software](#)

(Traduction : Asta, GregR, Kiwileaks, KoS, Rinzin, Scailyna,

Slystone, Tentate, aKa, audionuma, hugo, lamessen, lu, madalton + anonymes)

À :

Commission Européenne

DG Concurrence

B-1049 Bruxelles

Belgique

Juillet 2013

Selon des informations publiées dans un media spécialisé en ligne, la coalition dénommée « FairSearch » (composée de Microsoft, Nokia, Oracle et un certain nombre de fournisseurs de services en ligne) [prétend dans sa dernière demande à la Commission Européenne](#) que la distribution gratuite d'Android, un système d'exploitation libre^[1] pour mobiles développé par Google, constitue une pratique de prix prédateurs. Suggérer que la distribution gratuite de logiciels libres pénalise la concurrence est d'une part faux en soi, et constitue d'autre part un danger pour la concurrence et l'innovation.

Nous exhortons la Commission à examiner les faits comme il se doit avant d'admettre les allégations de FairSearch comme établies. Nous vous écrivons aujourd'hui afin d'expliquer comment la distribution de logiciels libres, qu'elle soit gratuite ou contre rémunération, promeut la concurrence plutôt que de la mettre à mal.

La [Free Software Foundation Europe \(FSFE\)](#) est une organisation associative indépendante et à but non lucratif qui se consacre à la promotion du logiciel libre. La FSFE défend l'idée que les libertés d'utiliser, de partager et d'améliorer les logiciels sont essentielles pour assurer une participation de tous à l'ère informatique. Nous travaillons en faveur d'une compréhension et d'un soutien global vis-à-vis du logiciel libre en politique, en droit et dans la société en général. Nous promouvons également le développement des technologies,

telles que le système d'exploitation GNU/Linux, qui assurent ces libertés à tous les participants de la société numérique. Pour atteindre ces buts, nous avons une longue histoire d'implication active dans les processus de concurrence qui affectent le logiciel libre.

Le logiciel libre est une question de liberté, pas de prix.

Le terme « libre » dans logiciel libre évoque la notion de liberté, et non celle de prix (*NdT la fameuse ambiguïté sur le mot anglais free*). Plus précisément, le logiciel libre offre aux utilisateurs les [libertés](#) suivantes :

- exécuter le programme, sans limitation ;
- étudier le code source du programme et comprendre comment il fonctionne ;
- partager le programme avec d'autres, que cela soit gratuitement ou moyennant finance ;
- améliorer le programme et distribuer ses améliorations.

Prises ensemble, ces quatre libertés font du modèle du logiciel libre une force puissante et disruptive pour la concurrence. Le logiciel libre a contribué de façon considérable à la rupture d'anciens monopoles construits par les fabricants de logiciels propriétaires tels que Microsoft.

Dans de nombreux domaines, les logiciels libres sont depuis longtemps les applications majeures, ou les alternatives concurrentes les plus puissantes. Cela inclut les serveurs web^[2], la navigation web (Firefox), les suites bureautiques (LibreOffice, OpenOffice), et les systèmes d'exploitation de serveurs. 93% des 500 supercalculateurs mondiaux sont basés sur des systèmes d'exploitation libres.

Le logiciel libre est la norme pour les fabricants de périphériques embarqués, comme les télévisions « intelligentes », les routeurs DSL, et les ordinateurs de

bord des voitures, pour ne citer qu'eux. De nos jours, des entreprises leaders du web, comme Facebook, Amazon et Google, s'appuient fortement sur le logiciel libre pour construire leurs offres. Le logiciel libre fait aussi fonctionner pléthore de startups et de concurrents avec des architectures et des services qui constituent des alternatives aux prestataires établis.

La tendance dans le mobile et ailleurs est irrémédiablement aux logiciels libres

Selon les sources accessibles au public, le fond de la revendication de FairSearch est qu'en « distribuant Android gratuitement », Google empêche les systèmes d'exploitation concurrents d'obtenir un retour sur investissement dans leur concurrence de « la plate-forme mobile dominante de Google ».

La FSFE s'oppose fermement à cette qualification : le logiciel libre est un moyen très efficace de produire et distribuer du logiciel. La vente de licences n'est que l'un des nombreux moyens de monétiser le logiciel.

Android est une plateforme logicielle construite autour du noyau Linux et de Java, par le [fork](#) Dalvik, ce qui est possible parce que Java et le noyau sont disponibles sous licence libre. N'importe qui peut prendre Android et le transformer en quelque chose de meilleur et de plus libre, avec ou sans liens avec Google, et ce aussi longtemps que le code source sera disponible, comme il l'est actuellement. [Replicant](#) et [CyanogenMod](#) sont simplement deux exemples notables, tous deux installés sur des millions de terminaux. L'adoption d'Android par Facebook pour ses propres besoins montre à quel point la plateforme est véritablement ouverte, au point qu'un concurrent peut proposer une interface graphique (GUI) alternative qui est essentiellement destinée aux services d'un concurrent.

En ce qui concerne Java, la Commission a déjà constaté la

forte valeur d'une plateforme non fragmentée et reconnaît qu'il existe de fortes motivations à la prévention de sa fragmentation^[3]. À tout le moins, Android a attiré les critiques du fait que ses conditions de licence et d'ouverture favorisent la fragmentation, contre ses propres intérêts. La fragmentation est une menace liée à la liberté de « forker ». Dans un contexte propriétaire, le contrôle étroit sur le droit d'auteur, les marques et les brevets empêche facilement la fragmentation. À l'inverse, dans un environnement libre, la fragmentation est évitée par le consensus, le l'autorité fondée sur le mérite, et parfois par l'utilisation de marques (Red Hat, Mozilla). Linux, le noyau commun aux systèmes d'exploitation Android et GNU/Linux a échappé jusqu'à présent à la fragmentation non pas parce qu'elle est impossible ou interdite ? elle ne l'est certainement pas ?, mais parce qu'elle ne rimerait à rien. Au sein d'une plateforme, assurer la plus large compatibilité et un haut degré de standardisation est une préoccupation constante de tout projet, et constitue d'une part une incitation forte pour éviter les abus de la communauté, et d'autre part une pression constante sur le ou les chefs de file du projet pour qu'ils avancent par consensus^[4].

Afin de bien illustrer la façon dont le logiciel libre favorise la concurrence, nous faisons remarquer que tous les ajouts récents à la liste des systèmes d'exploitation mobiles sont largement du logiciel libre. Bien que les appareils Android représentent actuellement [aux alentours de 70% des ventes de téléphones portables et tablettes](#), plusieurs autres systèmes d'exploitation mobiles libres basés sur le noyau Linux émergent pour entrer en concurrence avec Android. Les exemples incluent Firefox OS (soutenu par la fondation Mozilla), Jolla (issu des cendres de Maemo, un projet de la société Nokia interrompu suite à l'alignement stratégique de celle-ci sur Microsoft), Tizen (soutenu par Samsung, Intel et plusieurs opérateurs téléphoniques tels que Vodafone et NTT

Docomo), et UbuntuMobile (soutenu par Canonical).

La distribution libre du code n'a rien a voir avec les prix prédateurs

Dans sa demande, la coalition FairSearch affirme que la disponibilité gratuite d'Android rend difficile ou impossible la concurrence sur le marché des systèmes d'exploitation mobiles.

Cependant, la vente de licences n'a jamais été une stratégie importante dans le marché du mobile. À la base, le constructeur de Blackberry, RIM, vendait des appareils et des logiciels et services pour les serveurs dans le secteur des entreprises. Apple a financé son iOS propriétaire grâce à ses services et composants vendu à la fois par Apple et par des entreprises tierces réduisant considérablement les revenus générés par le magasin en ligne iTunes. Nokia a essayé de maintenir deux systèmes d'exploitations différents, tous deux finalement libres (Symbian et Maemo, ensuite renommé en Meego, et maintenant forké par Jolla et son SailFish). Seul Microsoft a réussi à garder une position de vendeur de logiciel indépendant, arguant de l'avantage tiré de l'intégration avec ses services réseaux.

Il semblerait donc que le seul motif envisageable à la plainte de la coalition FairSearch soit que l'existence d'un certain nombre de systèmes d'exploitations mobiles libres, dont Android, rende la tâche plus difficile à Microsoft pour reproduire son modèle économique dans le marché mobile. En soi, la demande de FairSearch à la commission revient à favoriser un modèle économique plutôt qu'un autre. C'est exactement à l'opposé de ce qu'une autorité de concurrence devrait appliquer pour maintenir un marché concurrentiel.

La FSFE a toujours clairement affirmé qu'une licence propriétaire est un système de production de logiciel obsolète et inefficace. De notre point de vu, Google n'a ni l'intention

ni les moyens de monopoliser le marché du système d'exploitation mobile, tout simplement parce qu'il n'y a pas de marché des licences de systèmes d'exploitations propriétaires.

La pratique de prix prédateurs alléguée par FairSearch est clairement inadaptée à la réalité d'un marché où il n'y a pas de prix, et d'un produit qui, étant un logiciel libre, peut être littéralement pris par n'importe qui et « forké », ce qui est une pratique que la Commission avait déjà abordée précédemment. Il n'y a pas de distribution « à perte » pour le logiciel libre, parce que le prix des copies sur le marché du système d'exploitation mobile dans ces circonstances est précisément de zéro.

Les logiciels sont faciles à copier pour un coût quasi-nul. En termes économiques, cela signifie qu'il n'y a par définition pas de rareté dans les logiciels. Une telle rareté ne peut être introduite qu'artificiellement, l'utilisation d'une licence propriétaire étant le moyen le plus courant.

Au contraire, le logiciel libre crée un bien commun, auquel chacun peut participer, mais que personne ne peut monopoliser. Les logiciels libres créent ainsi de la richesse et augmentent les possibilités de croissance pour nombre de compagnies et de modèles économiques. Par exemple, Red Hat est une entreprise dont le chiffre d'affaire annuel atteint les 1.3 milliards de dollars, uniquement par la fourniture de services autour d'une distribution GNU/Linux. Android a sans nul doute créé un avantage compétitif pour Google ; mais, contrairement à Microsoft, Google ne se focalise pas sur les logiciels et la monopolisation de plateforme, mais sur les services, proposés sur n'importe quelle plateforme utilisée par le consommateur. Au contraire, des analystes estiment que Microsoft [gagne plus d'argent grâce à Android](#) qu'il n'en gagne à partir de Windows pour les appareils mobiles. Après l'engagement d'une politique de licence d'exploitation de ses brevets [agressive](#) à l'égard des fabricants d'appareils Android.

L'avantage compétitif de Google est essentiellement éphémère : la seule voie pour rester devant la concurrence dans les logiciels libres est de concevoir de meilleurs produits ou services et de gagner la confiance des utilisateurs. Le coût à l'entrée dans cette environnement concurrentiel est extrêmement bas. En effet, cette plateforme accepte des marchés d'applications alternatifs. Les différentes fondations du logiciel libre font campagne pour « libérer les Android » (Free Your Android) et sollicite l'adoption d'un marché d'application alternatif appelé F-Droid où sont uniquement proposés des logiciels libres.

Conclusion

Dans cette demande, la coalition FairSearch semble supposer que les régulateurs européens n'ont pas pris conscience des évolutions du marché du logiciel au cours de cette dernière décennie. Au lieu de mettre en évidence une menace réelle à la concurrence dans le marché du mobile, la demande de FairSearch donne l'impression que Microsoft (une entreprise condamnée pour son comportement anti-concurrentiel dans des procès de premier plan sur trois continents) essaye de revenir en arrière. L'entreprise est en fait en train de soutenir que la Commission devrait protéger son modèle économique dépassé dans le marché du mobile par un innovateur plus efficace. Nous nous permettons, avec votre respect, de ne pas être de cet avis.

La qualité d'Android comme ressource commune le rend très précieux pour les fabricants, précisément parce que Google ne peut le contrôler qu'à travers son impulsion, pas à travers une main de fer et un enfermement propriétaire, comme c'est le cas avec les alternatives propriétaires. Ce fait même devrait être considéré comme une grande incitation à la concurrence.

Nous recommandons à la Commission européenne d'écarter ce recours sans même ouvrir formellement de procédure. Éventuellement, si une déclaration de communication des griefs devait être notifiée, elle devrait éviter toute référence à la

licence du logiciel libre comme source d'entrave à la concurrence. En effet, la qualité de logiciel libre d'Android devrait être considérée comme un outil puissant pour réduire les freins à une concurrence libre et améliorée.

À la FSFE, nous continuerons à travailler avec la Commission européenne pour promouvoir le logiciel libre comme un moyen de créer et maintenir la concurrence sur les marchés. Nous nous tenons prêts à assister la Commission dans toutes les affaires qui se rapportent au logiciel libre.

Bien à vous,

Karsten Gerloff, Président
Carlo Piana, Conseil général
Free Software Foundation Europe

Crédit photo : [Laihiu](#) (Creative Commons By)

Notes

[1] Souvent mentionné sous le nom « open source ». « Logiciel libre » est le nom original et plus précis qui reflète tous les aspects de ce phénomène.

[2] Au mois de Juin 2013, pas moins de 68% des sites internet actifs tournent grâce aux logiciels libres Apache et [Nginx](#).

[3] Decision in Case No COMP/M.5529 – ORACLE/ SUN MICROSYSTEMS, paragraph 935.

[4] Decision in Case No COMP/M.5529 – ORACLE/ SUN MICROSYSTEMS, paragraph 655.

Quelle entreprise peut encore faire confiance à Microsoft ?

par Glyn Moody

Le titre se suffit à lui-même ici. On pourrait ajouter aux entreprises, les institutions et les particuliers, bref tout le monde.

Non content d'avoir été accusé par le passé de réserver dans Windows des [portes dérobées](#) à la NSA, non content d'être fortement suspecté de laisser les autorités américaines collecter nos données dans Skype, Microsoft est maintenant soupçonné de différer la publication de ses [patches](#) de sécurité pour en informer d'abord les mêmes autorités américaines !

Tout [DSI](#) normalement constitué(e) devrait lire cet article et en tirer avec sa direction ses propres conclusions.



Quelle entreprise peut encore faire confiance à Microsoft ?

[How Can Any Company Ever Trust Microsoft Again?](#)

*Glyn Moddy – juin 2013 – Open Enterprise (Computer World)
(Traduction : Slystone, Luo, lamessen, Antoine, sinma,
Pouhiou, Sky, Fe-lor, aKa, Asta, audionuma + anonymes)*

Quels que soient les détails des récentes révélations sur l'espionnage de masse de la part des États-Unis fournis par [Edward Snowden](#) dans le Guardian, il y a déjà un énorme bénéfice collatéral. D'un côté, le gouvernement des États-Unis se replie sur lui-même, niant certaines allégations en offrant sa propre version de l'histoire. Cela, et pour la première fois, nous donne des détails officiels sur des programmes dont nous n'étions (au mieux) informés que par fuites et rumeurs, voire pas du tout. De plus, la précipitation indécente et l'histoire sans cesse changeante des autorités américaines est une confirmation, si elle était encore nécessaire, que ce que Snowden a révélé est important – vous ne provoquez pas un tel tapage pour rien.

Mais peut-être encore plus crucial, d'autres journalistes, poussés par la honte et leur culpabilisation, ont finalement posé des questions qu'ils auraient dû poser des années voire des décennies plus tôt. Cela a abouti à une série d'articles extrêmement intéressants à propos de l'espionnage de la NSA, dont beaucoup contiennent des informations auxiliaires qui sont aussi intéressantes que l'histoire principale. Voici [un bel exemple](#) de ce qui est apparu durant le week-end sur le site de Bloomberg.

Entre autres choses, il s'agit de Microsoft, et d'évaluer dans quelle mesure ils ont aidé la NSA à espionner le monde. Bien sûr, cette crainte n'est pas nouvelle. Dès 1999, [il était déjà dit](#) que des portes dérobées avaient été codées dans Windows :

Une erreur d'inattention de programmeurs Microsoft a révélé qu'un code d'accès spécial préparé par l'agence nationale de sécurité étasunienne (NSA) avait été secrètement implémenté dans Windows. Le système d'accès de la NSA est implémenté sous toutes les versions de Windows actuellement utilisées, à l'exception des premières versions de Windows 95 (et ses prédécesseurs). La découverte suivait de près les révélations survenues un peu plus tôt cette année concernant un autre géant du logiciel étasunien, Lotus, qui avait implémenté une trappe « d'aide à l'information » pour la NSA dans son système Notes. Des fonctions de sécurité dans d'autres logiciels systèmes avaient été délibérément paralysées.

Plus récemment, il y eut des craintes au sujet de Skype, [racheté par Microsoft](#) en mai 2011. En 2012, il y a eu des [discussions](#) pendant lesquelles on s'est demandé si Microsoft avait changé l'architecture de Skype pour rendre l'espionnage plus facile (l'entreprise a même un brevet sur l'idée). Les récentes fuites semblent confirmer que ces craintes étaient bien fondées, comme le [signale](#) Slate :

Le scoop du Washington Post sur PRISM et ses possibilités présente plusieurs points frappants, mais pour moi un en particulier s'est démarqué du reste. The Post, citant une diapositive Powerpoint confidentielle de la NSA, a écrit que l'agence avait un guide d'utilisation spécifique « pour la collecte de données Skype dans le cadre du programme PRISM » qui met en évidence les possibilités d'écoutes sur Skype « lorsque l'un des correspondants utilise un banal téléphone et lorsque deux utilisateurs du service réalisent un appel audio, vidéo, font du chat ou échangent des fichiers. »

Mais même cela devient dérisoire comparé aux [dernières informations](#) obtenues par Bloomberg :

D'après deux personnes qui connaissent bien le processus, Microsoft, la plus grande compagnie de logiciels au monde,

fournit aux services de renseignement des informations sur les bogues dans ses logiciels populaires avant la publication d'un correctif. Ces informations peuvent servir à protéger les ordinateurs du gouvernement ainsi qu'à accéder à ceux de terroristes ou d'armées ennemies.

La firme de Redmond basée à Washington, Microsoft, ainsi que d'autres firmes œuvrant dans le logiciel ou la sécurité, était au courant que ce genre d'alertes précoces permettaient aux États-Unis d'exploiter des failles dans les logiciels vendus aux gouvernements étrangers, selon deux fonctionnaires d'État. Microsoft ne demande pas et ne peut pas savoir comment le gouvernement utilise de tels tuyaux, ont dit les fonctionnaires, qui ne souhaitent pas que leur identité soit révélée au vu de la confidentialité du sujet.

Frank Shaw, un porte-parole de Microsoft, a fait savoir que ces divulgations se font en coopération avec d'autres agences, et sont conçues pour donner aux gouvernements « une longueur d'avance » sur l'évaluation des risques et des [mitigations](#).

Réfléchissons-y donc un moment.

Des entreprises et des gouvernements achètent des logiciels à Microsoft, se reposant sur la compagnie pour créer des programmes qui sont sûrs et sans risque. Aucun logiciel n'est complètement exempt de bogues, et des failles sérieuses sont trouvées régulièrement dans le code de Microsoft (et dans l'open source, aussi, bien sûr). Donc le problème n'est pas de savoir si les logiciels ont des failles, tout bout de code non-trivial en a, mais de savoir comment les auteurs du code réagissent.

Ce que veulent les gouvernements et les compagnies, c'est que ces failles soient corrigées le plus vite possible, de manière à ce qu'elles ne puissent pas être exploitées par des criminels pour causer des dégâts sur leurs systèmes. Et

pourtant, nous apprenons maintenant que l'une des premières choses que fait Microsoft, c'est d'envoyer des informations au sujet de ces failles à de multiples agences, en incluant sans doute la NSA et la CIA. En outre, nous savons aussi que « ce type d'alerte précoce a permis aux U.S.A. d'exploiter des failles dans les logiciels vendus aux gouvernements étrangers »

Et rappelez-vous que « gouvernements étrangers » signifie ceux des pays européens aussi bien que les autres (le fait que le gouvernement du Royaume-Uni ait [espionné](#) des pays « alliés » souligne que tout le monde le fait). Il serait également naïf de penser que les agences de renseignement américaines exploitent ces failles « jour 0 » seulement pour pénétrer dans les systèmes des gouvernements ; l'espionnage industriel représentait une partie de l'ancien [programme de surveillance Echelon](#), et il n'y a aucune raison de penser que les U.S.A. vont se limiter aujourd'hui (s'il y a eu un changement, les choses ont empiré).

Il est donc fortement probable que les faiblesses des produits Microsoft soient régulièrement utilisées pour s'infiltrer et pratiquer toutes sortes d'espionnage dans les gouvernements et sociétés étrangères. Ainsi, chaque fois qu'une entreprise installe un nouveau correctif d'une faille majeure provenant de Microsoft, il faut garder à l'esprit que quelqu'un a pu avoir utilisé cette faiblesse à des fins malveillantes.

Les conséquences de cette situation sont très profondes. Les entreprises achètent des produits Microsoft pour plusieurs raisons, mais toutes supposent que la compagnie fait de son mieux pour les protéger. Les dernières révélations montrent que c'est une hypothèse fautive : Microsoft transmet consciencieusement et régulièrement des informations sur la manière de percer les sécurités de ses produits aux agences américaines. Ce qui arrive à ces informations plus tard est, évidemment, un secret. Pas à cause du « terrorisme », mais parce qu'il est presque certain que des attaques illégales

sont menées contre d'autres pays (et leurs entreprises) en dehors des États-Unis.

Ce n'est rien d'autre qu'une trahison de la confiance que les utilisateurs placent en Microsoft, et je me demande comment un responsable informatique peut encore sérieusement recommander l'utilisation de produits Microsoft maintenant que nous sommes presque sûrs qu'ils sont un vecteur d'attaques par les agences d'espionnage américaines qui peuvent potentiellement causer d'énormes pertes aux entreprises concernées (comme ce qui est arrivé avec Echelon).

Mais il y a un autre angle intéressant. Même si peu de choses ont été écrites à ce sujet – même par moi, à ma grande honte – un nouvel accord législatif portant sur les attaques en ligne est en cours d'élaboration par l'Union Européenne. Voici [un aspect](#) de cet accord :

Ce texte demandera aux États membres de fixer leur peine maximale d'emprisonnement à au moins deux ans pour les crimes suivants : accéder à ou interférer illégalement avec des systèmes d'informations, interférer illégalement avec les données, intercepter illégalement des communications ou produire et vendre intentionnellement des outils utilisés pour commettre ces infractions.

« Accéder ou interférer illégalement avec des systèmes d'informations » semble être précisément ce que le gouvernement des États-Unis fait aux systèmes étrangers, dont probablement ceux de l'Union Européenne. Donc, cela indiquerait que le gouvernement américain va tomber sous le coup de ces nouvelles réglementations. Mais peut-être que Microsoft aussi, car c'est lui qui en premier lieu a rendu possible l'« accès illégal ».

Et il y a un autre aspect. Supposons que les espions américains utilisent des failles dans les logiciels de Microsoft pour entrer dans un réseau d'entreprise et y

espionner des tiers. Je me demande si ces entreprises peuvent elles-mêmes se trouver accusées de toute sorte d'infractions dont elles ne savaient rien ; et finir au tribunal. Prouver son innocence ici risque d'être difficile, car en ce cas les réseaux d'entreprise seraient effectivement utilisés pour espionner.

Au final, ce risque est encore une autre bonne raison de ne jamais utiliser des logiciels de Microsoft, avec toutes les autres qui ont été écrites ici ces dernières années. Ce n'est pas uniquement que l'open source est généralement moins cher (particulièrement si vous prenez en considération le prix de l'enfermement livré avec les logiciels Microsoft), mieux écrit, plus rapide, plus sûr et plus sécurisé. Mais par-dessus tout, le logiciel libre respecte ses utilisateurs, les plaçant solidement aux commandes.

Cela vous ôte toute crainte que l'entreprise vous ayant fourni un programme donne en secret à des tiers la possibilité de retourner contre vous ce logiciel que vous avez payé assez cher. Après tout, la plupart des résolutions des bogues dans l'open source est effectuée par des codeurs qui ont un peu d'amour pour l'autorité verticale, de sorte que la probabilité qu'ils donnent régulièrement les failles à la NSA, comme le fait Microsoft, doit être extrêmement faible.

Crédit photo : Cambodia4kids.org (Creative Commons By)

**Quand l'industrie culturelle
US veut attaquer les**

« pirates » à l'artillerie lourde !

Une [nouvelle](#) traduction de Cory Doctorow

L'industrie américaine du divertissement au Congrès : autorisez-nous légalement à déployer des [rootkits](#), des mouchards, des logiciels rançonneurs et des chevaux de Troie pour attaquer les pirates !

[US entertainment industry to Congress: make it legal for us to deploy rootkits, spyware, ransomware and trojans to attack pirates!](#)

Cory Doctorow – 26 mai 2013 – [BoingBoing.net](#)

(Traduction : Mowee, ehsavoie, audionuma, Asta)

La « Commission sur le Vol de la Propriété Intellectuelle Américaine », qui porte bien comiquement son nom, a finalement rendu son [rapport](#) de 84 pages complètement folles. Mais dans toute cette folie, il y a une part qui l'est encore plus que le reste : une proposition pour légaliser l'usage des logiciels malveillants afin de punir les personnes soupçonnées de copies illégales. Le rapport propose en effet que ce logiciel soit chargé sur les ordinateurs et qu'il détermine si vous êtes un pirate ou non. S'il soupçonne que c'est le cas, il verrouillera votre ordinateur et prendra toutes vos données en otage jusqu'à ce que vous appeliez la police pour confesser vos crimes. C'est ce mécanisme qu'utilisent les escrocs lorsqu'ils déploient des [logiciels rançonneurs](#) (NdT : *ransomware*).

Voilà une preuve supplémentaire que les stratégies en terme de réseau des défenseurs du copyright sont les mêmes que celles

utilisées par les dictateurs et les criminels. En 2011, la MPAA (Motion Picture Association of America) a dit au Congrès qu'ils souhaitaient l'adoption de la loi SOPA (Stop Online Piracy Act). Selon eux, cela ne pouvait que fonctionner vu que [la même tactique](#) est utilisée par les gouvernements en « Chine, Iran, Émirats Arabes Unis, Arménie, Éthiopie, Arabie Saoudite, Yémen, Bahreïn, Birmanie, Syrie, Turkménistan, Ouzbékistan et Vietnam. » Ils exigent désormais du Congrès que soit légalisé un outil d'extorsion inventé par le crime organisé.

De plus, un logiciel peut être écrit de manière à ce que seuls des utilisateurs autorisés puissent ouvrir des fichiers contenant des informations intéressantes. Si une personne non autorisée accède à l'information, un ensemble d'actions peuvent alors être mises en œuvre. Par exemple, le fichier pourrait être rendu inaccessible et l'ordinateur de la personne non autorisée verrouillé, avec des instructions indiquant comment prendre contact avec les autorités pour obtenir le mot de passe permettant le déverrouillage du compte. Ces mesures ne violent pas les lois existantes sur l'usage d'Internet, elles servent cependant à atténuer les attaques et à stabiliser un cyber-incident, pour fournir à la fois du temps et des preuves, afin que les autorités puissent être impliquées.

De mieux en mieux :

Alors que la loi américaine interdit actuellement ces pratiques, il y a de plus en plus de demandes pour la création d'un environnement légal de défense des systèmes d'informations beaucoup plus permissif. Cela permettrait aux entreprises de non seulement stabiliser la situation, mais aussi de prendre des mesures radicales, comme retrouver par elles-mêmes les informations volées pouvant aller jusqu'à altérer voire détruire ces dernières dans un réseau dans lequel elles n'ont pourtant aucun droit. Certaines mesures

envisagées vont encore plus loin : photographier le hacker avec sa propre webcam, infecter son réseau en y implantant un logiciel malveillant ou même désactiver voire détériorer physiquement le matériel utilisé pour commettre les infractions (comme son ordinateur).

Source : [La Commission sur le Vol de la Propriété Intellectuelle Américaine recommande les malwares !](#)

Éducation : priorité au logiciel libre ou respect de la « neutralité technologique » ?

On commence à connaître la chanson et elle est emblématique de l'époque actuelle : le *privé* qui s'alarme et demande au *public* de le soutenir sur le dos des *biens communs*.

Ici nous sommes dans le secteur sensible de l'éducation et pour refuser la priorité aux logiciels libres on est prêt à tout, comme sortir du chapeau la notion pour le moins vague et floue de « neutralité technologique » (sans oublier le [FUD](#) sur l'innovation, la croissance, la destruction d'emplois, toussa...)

Le Sénat a en effet examiné cette semaine le [projet de loi](#) sur la refondation de l'école de la République. Parmi les dispositions introduites par la commission de la culture, de l'éducation et de la communication, on trouve une modification apportée à l'article 101 **qui donne la priorité au logiciel**

libre et aux formats ouverts dans le futur service public du numérique éducatif.

Pour ceux (comme [l'April](#) ou [l'Aful](#)) qui se battent depuis des années, voire des décennies, pour qu'il en soit ainsi, c'est déjà un grand pas en avant.

Un pas en avant clairement non partagé par le [Syntec Numérique](#) et l'[AFINEF](#) (Association Française des Industriels du Numérique dans l'Education et la Formation) qui ont publié dans la foulée un communiqué de presse que nous avons reproduit ci-dessous.

Dans la mesure où les communiqués de l'April, de l'Aful et du Syntec ne proposent pas d'espace de discussion sous article, **nous invitons toutes celles et ceux que le sujet intéresse à intervenir dans les commentaires.**

PS : Rappelons à l'occasion l'article de Richard Stallman : [Pourquoi les écoles devraient utiliser le logiciel libre et l'enseigner.](#)



Numérique éducatif et pédagogique : les professionnels du numérique interpellent le Gouvernement sur le respect de la neutralité technologique

CP du Syntec Numérique et l'AFINEF (22 mai 2013)

[URL d'origine du document](#)

Syntec Numérique et l'AFINEF interpellent le Gouvernement sur la mention favorisant de manière prioritaire l'utilisation de logiciels libres pour le service public du numérique éducatif, dans le projet de loi en débat ce mercredi 22 mai au Sénat sur la Refondation de l'Ecole de la République. Syntec Numérique, le syndicat professionnel des industries et métiers du numérique, et l'Association Française des Industriels de l'Education et de la Formation (AFINEF) interpellent le Gouvernement sur les dispositions modifiées du Projet de Loi de Refondation de l'Ecole de la République issues du travail en commission au Sénat, **donnant la priorité à l'utilisation de logiciels libres pour le service public du numérique éducatif.**

Malgré un avis défavorable du Gouvernement en commission, la rédaction retenue à l'alinéa 7 de l'article 10, « *Ce service public utilise en priorité des logiciels libres et des formats ouverts de documents* », **porte atteinte au principe de neutralité technologique** qui est la règle notamment pour la commande et l'achat publics.

Par ailleurs, le rapport annexé à la Loi à l'article 1er, définissant les moyens et les orientations de la refondation de l'école de la République mentionne que « *L'incitation au développement de ressources numériques se fera notamment en faveur de contenus et de services numériques dits « libres »* ».

Les professionnels du numérique regrettent que **ces deux**

dispositions contredisent la circulaire du premier ministre du 19 septembre 2012 sur les modalités de l'utilisation des logiciels libres dans l'administration tout **en portant atteinte au pluralisme** des ressources informatiques.

En effet, au moment où le Gouvernement engage une politique d'aide à la création d'une filière d'acteurs français du numérique éducatif et pédagogique, ces dispositions, si elles sont définitivement adoptées, handicaperont gravement les efforts de développement de la plupart des entreprises déjà présentes sur cette filière qui n'a pas encore trouvé sa consolidation et dissuaderont de nouveaux acteurs innovants de s'y engager.

Pour les acteurs du numérique, **le pluralisme et la neutralité technologique, adossés à l'interopérabilité, sont les conditions sine qua none** afin de s'engager dans le développement des produits et supports technologiques pour répondre à l'enjeu essentiel de la modernisation du service public éducatif et à l'accompagnement des enseignants dans leur investissement pédagogique.

Ils souhaitent par ailleurs alerter les pouvoirs publics sur **les conséquences que ces dispositions auraient sur la lisibilité de l'offre e-éducative française à l'international**, notamment en direction de continents où le pluralisme et la neutralité technologique conditionnent la pénétration des marchés.

Ils soulignent enfin que ces dispositions évidemment inconstitutionnelles, augmenteront **le risque de recours contentieux** entre les opérateurs privés du secteur et les administrations. En effet, ces dispositions rentrent en contradiction avec les principes d'égalité de traitement et de liberté d'accès à la commande publique, rappelés à l'article 1er du Code des marchés publics et qui ont acquis valeur constitutionnelle (Cons. Const. 26 juin 2003) : « *Les marchés publics et les accords-cadres soumis au présent code*

respectent les principes de liberté d'accès à la commande publique, d'égalité de traitement des candidats et de transparence des procédures. Ces principes permettent d'assurer l'efficacité de la commande publique et la bonne utilisation des deniers publics. Ces obligations sont mises en œuvre conformément aux règles fixées par le présent code ».

Force est de constater que ces dispositions vont en effet à l'encontre du principe de neutralité du droit des marchés publics, qui ne permet aucunement de favoriser des opérateurs économiques au détriment d'autres. Au contraire, les règles de la commande publique ont pour objet de permettre au pouvoir adjudicateur de sélectionner l'offre économiquement la plus avantageuse, correspondant à ses besoins, après une mise en concurrence. Ainsi, écarter la fourniture de certaines solutions, en imposant un type de logiciels, violerait les principes fondamentaux de la commande publique consacrés tant au niveau français qu'europpéen et jamais démentis.

Syntec Numérique et l'AFINEV en appellent ainsi à la sagesse de la Haute Assemblée et au respect de la feuille de route numérique du Gouvernement, afin de soutenir une filière qui a besoin d'être stimulée par un environnement législatif et juridique stable, et non par des mesures discriminatoires infondées, pour donner la mesure de tout son potentiel, en termes d'innovation, de croissance et de création d'emplois.

Crédit photo : [Sashomasho](#) (Creative Commons By-Sa)

Attention danger !

Restrictions numériques et physiques sur nos propres appareils

Nous devons craindre de nous réveiller un jour dans un monde où non seulement les contenus numériques seront sous contrôle mais également les appareils qui permettent de les consulter...



Restrictions numériques et physiques sur votre propre appareil

[Digital and physical restrictions on your own device](#)

Erik Albers – 3 mai 2013 – FSFE Blog

(Traduction : goofy, hugo, Eijebong, ProgVal, Rudloff, Tony, Rogdham, Asta, KoS + anonymes)

À propos des restrictions numériques

Aujourd'hui, 3 mai 2013, on célèbre la [Journée internationale contre les Mesures Techniques de Restriction](#) (Digital

Restrictions Management)^[1], promue par la [Fondation pour le Logiciel Libre](#) (Free Software Foundation, FSF). En général, le terme [Digital Restrictions Management](#) (DRM) se réfère à différentes restrictions que les entreprises – ou tout autre fournisseur de contenu – imposent sur les données et contenus numériques. Ces restrictions sont là pour permettre aux fournisseurs de décider ce que vous pouvez faire avec vos données et contenus, et ce que vous ne pouvez pas faire. Ainsi, ils vous empêchent d'être en pleine possession de vos données. Ces données sont défectueuses par nature (defective by design) – quel que soit le prix que vous soyez prêt-e à y mettre.

Et cela nous mène à un monde [où l'on « n'achète » rien d'autre qu'une « licence d'utilisation »](#).

Les restrictions comme celles-ci évoluent, jusqu'au jour où la personne détenant les droits peut légalement décider de soudainement [supprimer tout ce que vous avez acheté](#) – à distance !

Cette année, la journée contre les DRM se concentre sur une nouvelle menace globale contre tout ce que ce que nous connaissons du World Wide Web : le World Wide Web Consortium (W3C) réfléchit à un projet de spécification d'Extension de Contenus Chiffrés (Encrypted Media Extensions proposal, EME), qui vise à avaliser le support des DRM dans HTML5. HTML est le cœur de ce qu'est le Web (*NdT: « de ce qu'est Internet » (sic) dans la version originale*). Établir les DRM au sein d'HTML pourrait devenir une terrible menace pour la liberté de l'Internet, les navigateurs libres et la liberté des utilisateurs en général.

J'espère que beaucoup de personnes dans le monde vont [rejoindre la FSF ou la FSFE](#) (FSF Europe), ou [s'aligner avec d'autres organisations](#) dans leur combat contre les DRM dans HTML5. S'il vous plait, [signez la pétition](#) et [faites le plus de bruit possible](#) pour que d'autres personnes se rendent

compte de ce développement [captieux](#).

À présent, je voudrais utiliser cette journée pour faire le point sur un autre problème. Quelque chose auquel les DRM ne sont pas forcément reliées ; mais, qui y est effectivement relié : la propriété de vos propres appareils.

À propos de la propriété de votre appareil

De plus en plus souvent, nous voyons comment les entreprises et les fabricants vendent des appareils bridés qui sont en fait des (mini) ordinateurs – mais sont artificiellement bloqués pour que vous ne puissiez pas vous en servir comme des ordinateurs universels. Les fabricants sont créatifs lorsqu'il s'agit de restreindre vos appareils et sont déjà prêts à s'attaquer aux ordinateurs universels classiques avec [une restriction appelée Secure Boot](#). Mais, l'amère vérité est que de telles restrictions sont déjà valables pour des appareils « mobiles » – téléphones et tablettes – ce qui remet fondamentalement en cause de ce que l'on appelle propriété.

Note : Ce que je vais expliquer est tout à fait vrai pour beaucoup d'appareils sur le marché – mais comme je connais mieux le système Android et les restrictions qui viennent avec celui-ci, je vais me concentrer sur les téléphones Android. À propos, si vous voulez en savoir plus sur la façon de débloquent son chargeur de démarrage (bootloader), changer votre système d'exploitation et utiliser du Logiciel Libre sur votre appareil mobile, vous pourrez trouver plus d'informations sur <http://www.freeyourandroid.org>.

Si aujourd'hui vous achetez un appareil Android, vous achetez le matériel d'un fabricant qui vient avec un système d'exploitation préinstallé développé par Google, Android. Ce système d'exploitation vient souvent avec son lot d'inconvénients, comme des applications que vous n'êtes pas autorisé-e à désinstaller. Ainsi, ils vous vendent un système d'exploitation bloqué. Malheureusement, le même matériel vient

souvent avec un chargeur de démarrage bloqué, donc vous n'êtes pas capable de remplacer le système d'exploitation. À part quelques applications, en quoi est-ce mal ?

Tout d'abord, c'est une restriction artificielle de votre appareil. Ils ne veulent pas que vous l'utilisiez comme vous l'entendez – que vous souhaitiez utiliser le système préinstallé ou non. Ils appellent souvent cela un « produit fini », ce qui devrait être littéralement compris comme la fin de votre liberté.

Ensuite, leur but est de vous lier aux intérêts du fabricant. Et leur intérêt est d'augmenter le nombre d'appareils vendus chaque année au lieu d'assurer la maintenance de ceux déjà vendus. Comment ? Si vous achetez un téléphone Android et qu'ensuite Google publie une nouvelle version, vous ne pourrez pas installer cette nouvelle version car votre chargeur de démarrage est bloqué. Autrement dit, peu importe que votre appareil soit capable de fonctionner sur un nouveau système d'exploitation, ils restreignent simplement la possibilité de le faire.

Heureusement, il y a une façon de vous réapproprier votre appareil et d'installer le système de votre choix, quel qu'il soit : débloquer le chargeur de démarrage. Mais comme ce n'est pas l'intérêt de votre fabricant – tel que je l'ai expliqué plus haut – ils vont probablement déclarer votre garantie nulle si vous le faites. Ce qui est juridiquement incorrect. Comme [Carlo Piana et Matija Šuklje l'ont fait remarquer](#) – ainsi qu'une [association de consommateurs allemande](#) – ce n'est pas légal suite à la [Directive Européenne 1999/44/EC](#) (NdT: *la garantie est due par le vendeur, voir Code de la consommation, L.211*). Malheureusement, ils essayent toujours de vous faire peur. Cela ne peut pas être vu que comme une mauvaise habitude. L'intention est d'éviter que les utilisateurs ne se réapproprient leurs propres appareils. C'est pourquoi ils continuent de le faire – même si ce n'est pas sur une base légale.

Les constructeurs ont différentes politiques concernant la possibilité de débloquent votre chargeur de démarrage. Dans le pire des cas, ils vont feront signer un contrat juridique avant que vous n'obteniez le code spécifique pour débloquent votre chargeur de démarrage. Dans ce contrat, que vous devez signer, ils vous forcent souvent à renoncer à votre garantie – qui est un transfert de vos droits en tant que consommateur, comme expliqué plus haut. Mais, pire encore, il y a le contrat que vous devez signer pour débloquent votre appareil Motorola^[2] :

Les appareils qui ont été débloquentés sont pour votre utilisation personnelle uniquement. Une fois que vous avez débloquenté votre appareil, vous ne pouvez l'utiliser que pour votre utilisation personnelle et ne pouvez pas le vendre ni même le céder.

Pardon ? Vous n'êtes plus autorisé à **vendre** votre appareil ? Celui que vous avez acheté ?

Où allons nous ?

Le contrôle à distance et la gestion des restrictions de vos données numériques sont quelque chose dont nous devons nous soucier. Mais, de plus en plus d'entreprises ont déjà imposé des restrictions numériques sur l'usage physique de nos appareils – tel que l'interdiction d'installer les logiciels que vous voulez sur votre propre appareil. Ou, comme on l'a déjà vu, la limitation sur les conditions de vente de votre propre matériel. C'est un développement négatif contre lequel nous devons agir et essayer de changer ces pratiques. Si nous échouons à le faire et laissons tomber nos droits en tant que consommateurs et nos libertés civiles, nous devons craindre de nous réveiller un jour dans un monde où non seulement le contenu numérique sera hors de contrôle de la société, mais également le contrôle physique de la technologie.

De nos jours, Google nous donne un parfait exemple de comment cela peut être fait : les [Google Glass](#) vont être du matériel qui sera vendu par Google et qui est actuellement en beta test sous le nom de *Google Glass Explorer Edition*. À cause de la licence d'utilisation que vous devez signer pour devenir un beta testeur, vous ne serez pas autorisé à vendre l'appareil ou même le prêter à un ami. Certes, cela peut être vu comme une mauvaise habitude ou une restriction compréhensible pour un test. Ce n'est pas mon propos. Je veux dire que cela devrait concerner tout le monde : [si vous ne respectez pas les conditions de Google, ils désactiveront votre matériel à distance](#).

Cela se rapproche de l'étape finale : l'intégration par le constructeur d'une option pour détruire à distance votre matériel, laissant chaque utilisateur sans contrôle de sa propre technologie informatique, de ce qui lui appartient. Si le futur est dans le contrôle à distance, la société perdra le contrôle de la technologie et de son contenu. À partir de là il est facile d'imaginer la censure, la supervision et le contrôle de la société par des monopoles d'une manière encore jamais vue.

Crédit illustration : [Brendan Mruk et Matt Lee](#) (Creative Commons By-Sa)

Notes

[1] Lire à ce sujet ces deux billets du Framablog : [Mobilisons-nous ! Pas de DRM dans le HTML5 et les standards W3C](#) et [DRM dans HTML5 : la réponse de Cory Doctorow à Tim Berners-Lee](#).

[2] C'est seulement un exemple, j'en suis conscient. Il y a peut être d'autres entreprises qui agissent de la sorte, je n'en sais rien.