# Conférence de Richard Stallman à Bruxelles, le jeudi 27 septembre 2012

# Vers une société numérique libre

**EN CONSTRUCTION**



Voir http://www.bxlug.be/rms2012. Les liens vers les fichiers son de la conférence sont placés en bas de cet article.

L'orateur, Richard Stallman, est anglophone, mais s'exprime suffisamment bien en français que pour donner ses conférences dans cette langue devant un public francophone. Dans ces conditions, son discours est teinté d'hésitations, de légères imperfections, de tournures inusitées que nous avons préféré conserver pour la plupart, parce qu'elles ne nuisent pas à la compréhension des idées développées, et parce qu'elles constituent aussi une partie de sa signature.

## Mot d'introduction de Nicolas Pettiaux :

Bonjour, plutôt bonsoir, merci d'être venus nombreux à cette conférence organisée par le Bxlug, le groupe Bruxellois des utilisateurs de Gnu Linux et de logiciels libres, pour donner la parole à Richard Stallman.

Pour commencer, je voudrais remercier toutes les institutions et les personnes qui ont permis que cette conférence ait lieu, à commencer par l'hôte de ce soir, l'Université Libre de Bruxelles. Les autres institutions sont l'école nationale supérieure des arts visuels de La Cambre, l'école supérieure d'informatique, la fédération Wallonie Bruxelles, la commission communautaire française, la ville de Bruxelles, et l'union des anciens étudiants de l'Université. A titre individuel, toutes les personnes qui ont permis de rendre cette activité possible sont : Alain, Michel, Anthony, Nathalie, Tony, Jean-Claude, Cécile, Émir, Mathieu, Amza, Mina, Dandy, Caroline, Claude, Ramon, François, Fabrice, Marc, Serge, Frédéric, Aurélien, Lionel, Philippe, André, Jean-Paul, Jean-Marie, Catherine, Andrew et Eddy, et je voudrais que vous les applaudissiez, parce que sans eux, il n'y aurait pas d'activité. (NDLR : applaudissements)

Vous avez vu le message qui est au dessus de moi, les photographies sont strictement autorisées, les enregistrements aussi, “mais avec une condition que je dirai quand je commence” (NDLR : cette phrase dite par Richard Stallman). Et sinon, je crois que vous pouvez la lire.

L'Université de Bruxelles a un chant, le semeur, qui a été entonné vendredi dernier à l'occasion de la rentrée académique, et qui termine par ces mots qui je crois introduise bien Richard Stallman que la plupart d'entre vous connaisse, le fondateur du projet GNU, et ce chant et son refrain terminent donc par “et nous n'avons qu'une seule maîtresse, c'est toi liberté !”, je vous donne la parole Richard Stallman, merci beaucoup.

# Conférence de Richard Stallman

Bonsoir, Si tu fais des photos de moi, prière de ne pas les mettre dans Facebook ! (rires et applaudissements de l'assemblée). Facebook est un moteur de surveillance et mettre les photos de quelqu'un dans Facebook lui donne une autre opportunité de le surveiller. On peut discuter si mettre des photos de tes amis dans Facebook est un traitement amical de tes amis, mais cela ne me touche pas. Mais prière de ne pas mettre des photos de **MOI** sur Facebook. Et si tu enregistres la conférence et si tu veux en distribuer des copies, prière de le faire uniquement dans les formats favorables aux logiciels libres, c'est à dire les formats ogg ou webM. Pas dans mp... n'importe quoi, pas dans Flash et pas dans realplayer, windows media player ou quicktime. Et prière d'y mettre la licence creative commons no-derivative, parce que c'est une présentation de mon point de vue. Merci.

Il y a beaucoup de projets qui visent à l'inclusion numérique, c'est à dire à inviter plus de monde à participer dans la société numérique, mais est-ce que c'est un bon but, est-ce qu'il faut chercher l'inclusion numérique ? Cela dépend, selon moi, si la société est juste ou injuste. Si cette société est juste, l'inclusion dans elle est désirable, mais si elle est injuste, il faut chercher plutôt l'extraction numérique de tous les internautes. Donc, je trouve que ce discours de l'inclusion numérique est erroné. il faut d'abord chercher une société numérique juste, et puis nous pouvons inviter des autres à y participer. Mais quelles sont les menaces à la liberté des internautes, des menaces à la société numérique juste. Je vais traiter 9 menaces dans cette petite conférence.

La première est la surveillance. La technologie numérique facilite un niveau de surveillance qui aurait été le rêve pour Staline. Mais Staline ne pouvait pas le faire, bien qu'il ait essayé, mais sans la technologie numérique, c'était impossible mais aujourd'hui c'est possible. Si nous faisons quelque chose par ordinateur, les ordinateurs peuvent prendre note de tous ce que nous faisons, et garder ces notes à jamais, dans un catalogue sous le nom ou le numéro de chacun. Et beaucoup de pays ont imposé des numéros à chacun, ce que je trouve dangereux, parce que des cartes nationales d'identité facilitent la surveillance. Mais les entreprises aussi font de la surveillance, comme par exemple Facebook et beaucoup d'autres. Souvent, la surveillance est faite par nos propres ordinateurs, surtout s'il y a des logiciels non-libres dans l'ordinateur.

Les programmes non libres contiennent souvent des fonctionnalités malveillantes, y compris les fonctionnalités de surveiller l'utilisateur et transmettre des données sur lui à quelques serveurs. Nous avons trouvé des fonctionnalités spécifiques de surveillance dans Windows, dans les Ithink d'Apple, dans Flashplayer, le kindle d'Amazon, dans la plupart des téléphones portables. Donc c'est assez commun. Mais une défense contre la surveillance faite au travers de ton ordinateur est d'utiliser uniquement du logiciel libre, parce que le logiciel libre est sous le contrôle de l'utilisateur. S'il ne veut pas être surveillé, il peut changer le programme. Et dans la communauté d'utilisateurs d'un programme libre, il y en aura assez qui ne veulent pas être surveillés, donc quelqu'un le fera. C'est presque sûr que d'autres le feront, et tu ne devras pas travailler dessus. Parce qu'il suffit d'éliminer cette fonctionnalité malveillante une fois pour tout le monde.

Mais ce n'est pas la seule manière de nous surveiller par la technologie numérique. La surveillance se fait aussi dans les sites web que nous visitons. Beaucoup envoient les données de chaque visiteur à Google pour le service Google Analytics qui fait de la statistique sur toutes les visites. Mais c'est à dire que le site donne à Google toutes les données sur les visiteurs. Je crois qu'il ne faut pas le faire, mais ils le font. Il y a aussi la surveillance sur les systèmes qui ne nous appartiennent pas, mais que nous devons utiliser, les services. Par exemple les fournisseurs d'accès internet sont obligés en Europe de garder pour une période toutes les données sur les communications des utilisateurs, avec qui ils communiquent. Ces données doivent être gardées assez longtemps, mais peuvent être gardées

beaucoup plus longtemps. Qui sait ? Les entreprises de téléphonie gardent tous les appels de chaque utilisateur, à qui il envoie des messages, mais aussi où il va. Toutes les quelques minutes, le téléphone dit où il est. Quelqu'un en Allemagne a demandé la liste des données que l'entreprise avait sur lui. Et l'entreprise ne voulait pas le lui livrer, mais enfin elle devait le faire, et il a reçu plus de trente milles positions géographique pour six mois, c'est à dire plus ou moins plus de deux cents par jour. C'est assez souvent. On peut comprendre la vie de quelqu'un seulement à partir de cette liste. Mais c'est vrai que le téléphone participe dans cette surveillance. Il transmet sa position GPS, et avec uniquement des logiciels libres dans le téléphone, nous pourrions éliminer cette fonctionnalité. Mais l'entreprise est capable de localiser le téléphone même sans sa participation, par triangulation du signal entre plusieurs tours (NDLR : antennes). Et ils mettent toujours plus de tours, donc ils ont toujours plus d'exactitude dans la localisation du téléphone, même sans sa coopération, et l'utilisateur n'a pas le moyen de l'éviter.

Il y a aussi des systèmes de surveillance qui n'ont rien à faire avec nos activités. Par exemple en Angleterre, ils ont mis des caméras sur les routes pour reconnaître les immatriculations des autos, de toutes les autos, et de suivre tous les mouvements des voitures dans le pays, en temps réel. Ils sont en train de le faire de manière informelle aux État-Unis aussi. Il mettent pour quelques prétextes des caméras ici et là, et avec des milliers de caméras à la fin, cela ressemble à un système de surveillance complet. Que faire ? La seule manière d'éviter la surveillance faite au travers de nos ordinateurs, c'est par l'action politique. Mais ce qu'ils proposent, même ceux qui essayent de limiter la surveillance, c'est de limiter l'utilisation des données une fois recueillies. Cela ne suffit pas. Les données recueillies conduisent à des abus. C'est normal, c'est presque inévitable. Même si nous supposons que nous pouvons éviter que des policiers abusent des données pour des buts individuels, comment limiter ce que fait l'état avec ces données. Cela ne suffit parce que ce changement est une grande augmentation du niveau de surveillance général. Et même si l'utilisation des données est soumise à des limites comme le besoin d'un ordre d'un tribunal, c'est toujours une augmentation énorme du niveau général de surveillance. Si nous ne croyons pas que le niveau général antérieur de surveillance était un manque, évidemment cette augmentation est trop. Il faut limiter la collection des données, pas seulement leur utilisation. Cette surveillance est très dangereuse pour la démocratie, parce que ces données servent surtout pour attraper les dissidents, souvent appelé terroristes. C'est la nouvelle vague, mais c'était aussi l'ancienne vague d'accuser les dissidents d'être terroristes. Même aux États-Unis, ils le font ! C'est comme cela qu'ils mettent toujours des exceptions dans les limitations de l'utilisation des données pour chasser les terroristes, c'est à dire les dissidents. Donc il faut limiter strictement la collection des données. Par exemple (et je peux donner beaucoup d'exemples), en Angleterre, ils ont utilisé leur système de surveillance des mouvements des voitures pour arrêter des dissidents supposés en route à une manifestation, pour les arrêter avant d'y arriver, avant de rien faire. Mais qu'est-ce qu'ils voulaient faire ? Une manifestation ! La démocratie… C'est à dire un système pour saboter la démocratie. Et pourquoi est-ce qu'ils voudraient le faire ? C'est parce que c'est un gouvernement pour les entreprises qui s'impose au peuple. Ce n'est pas vraiment la démocratie. Cet état a toujours la forme de la démocratie, mais pas la substance. Donc, son but est de maintenir le pouvoir des entreprises, et de réprimer les dissidents. Il faut résister à la surveillance donc !

(18:40) Que faire ? Il faut évidemment lutter, mais une chose intéressante est que dans Internet, la censure exige la surveillance. Comment bloquer la transmission de quelque oeuvre, sans savoir si quelqu'un transmet cette oeuvre. Donc, pour vraiment censurer il faut surveiller tout. Il faut noter que des entreprises occidentales ont participé dans le développement des systèmes que ces pays utilisent utilisent pour leur surveillance et leur censure.

Une autre menace à la liberté numérique est dans les formats conçus pour restreindre leurs utilisateurs. Il y a les formats secrets. Par exemple beaucoup d'applications sauvegardent les données

de l'utilisateur dans un format secret pour éviter l'interopérabilité avec d'autres programmes, pour que l'utilisateur ne puisse utiliser ses données hors de ce programme. C'est assez commun chez le logiciel privateur, c'est-à-dire pas libre. Dans un programme libre, aucun format n'est secret. Parce que le code source de ce programme documente le format. Si quelqu'un veut mettre le support de ce format dans un autre programme libre, il peut copier ce code. Et s'il ne veut pas copier ce code, il peut le lire pour comprendre le format et écrire d'autres codes. Donc un format secret est impossible chez le logiciel libre, mais assez commun chez le privateur. Ils utilisent les formats secrets aussi pour la diffusion d'oeuvre pour restreindre l'utilisateur également. Dans ce cas, ils s'appellent des menottes numériques. Et beaucoup de programmes privateurs très utilisés apportent des menottes numériques à l'utilisateur. Par exemple Windows, Mac OS X, ithinks, flash player, le kindle d'Amazon, peut-être des téléphones portables. Je ne sais pas. Il y a plusieurs années il y en avait, maintenant je ne sais pas. Donc c'est assez commun comme problème. Donc j'ai présenté deux sortes de fonctionnalités malveillante : la surveillance et les menottes numériques. Les fonctionnalités pour restreindre l'utilisateur.

Il y a aussi les formats pas secrets, mais brevetés. Par exemple les formats mp sont brevetés, et le problème, ils ne sont pas secrets, donc il y a des logiciels libres capables de gérer ces formats, mais les programmes sont interdits dans plusieurs pays par les brevets, donc dans les distributeurs des systèmes GNU/Linux beaucoup n'osent pas inclure ces programmes parce qu'ils ont peur d'avoir un procès, donc ou ils n'offrent rien pour gérer ces formats, ou ils offrent des programmes privateurs pour gérer ces formats. Mais les utilisateurs ont besoin de ces formats, parce que beaucoup distribuent des oeuvres dans ces formats. Et si l'utilisateur reçoit une copie de GNU/Linux sans support pour le format, il dit “ce système ne marche pas bien”, ne sert pas, parce qu'il ne vient pas avec des supports pour ces formats mp3,... Mais si le système vient avec des logiciels privateurs, il n'est pas complètement éthique. Il y a donc une portion qui n'est pas éthique. D'une manière ou une autre, c'est un problème. c'est pour ça que je ne fais pas de fichiers mp3, jamais ! j'ai du logiciel pour jouer un fichier mp3, mais je ne les fais pas, parce que je ne veux pas ajouter à la somme des fichiers mp3 dans le monde, parce que chaque fichier mp3 pousse les gens à exiger le support pour mp3 et augmente le problème de l'absence de logiciels libres pour le faire dans beaucoup de distributions GNU/Linux. Donc c'est une combinaison des deux facteurs qui crée ce problème : c'est l'utilisation du format généralisé dans la société comme premier facteur, et le brevet et le danger d'avoir un procès sur le brevet comme l'autre facteur, qui rendent dangereux ces formats.

Il y a aussi le cas unique de Flash qui n'est pas secret. Hormis la fonctionnalité de menottes numériques, le reste n'est pas secret. Mais Adobe l'avait changé tant de fois que nous n'avons pas pu implémenter le support pour la dernière version. Nous avons du support pour la version 8, mais Adobe a fait la version 10 ! Que faire ? Il ne faut pas distribuer des oeuvres dans flash, il ne faut pas mettre de flash dans les sites web. Il faut te plaindre si tu visites un site avec Flash, il faut te plaindre à la gestion du site.

(31:10) Une autre menace est dans les programmes privateurs, c'est-à-dire les programmes qui ne respectent pas la liberté de l'utilisateur. Chez les logiciels, il y a deux possibilités, ou l'utilisateur a le contrôle du programme, ou le programme a le contrôle de ces utilisateurs. Le premier cas, c'est le logiciel libre, parce que pour avoir le contrôle du programme, les utilisateurs ont besoin de plusieurs libertés. Et ces libertés essentielles définissent le logiciel libre, font les critères pour un programme libre. Et si les utilisateurs ont ces libertés, ils ont le contrôle individuel et collectif, en parallèle. C'est à dire que chaque utilisateur est libre de changer le programme, mais n'importe quel groupe d'utilisateur peut aussi maintenir sa propre version et la changer pour faire ce qu'il veut. Si les utilisateurs ne disposent pas des libertés essentielles, ils n'ont pas le contrôle du programme, donc c'est le programme qui a le contrôle de ces utilisateurs. Mais le propriétaire du programme a toujours

le contrôle du programme. Et au travers ce programme, il exerce du pouvoir sur les utilisateurs, un pouvoir injuste. Donc, nous l'appelons un programme privateur, parce qu'il prive de leurs libertés les utilisateurs. C'est un système de pouvoir injuste, un système de colonisation numérique. Un grand nombre Par conséquent beaucoup de programmes privateurs comprennent des fonctionnalités malveillantes. J'ai déjà mentionné les fonctionnalités de surveillance et les menottes numériques. Il y a aussi les portes dérobées, qui acceptent des commandes de quelqu'un d'autre pour faire quelque chose à l'utilisateur sans lui demander d'autorisation pour le faire.

Comme çà le programme devient l'ennemi actif de son utilisateur. Des portes dérobées ont été trouvées dans Windows, dans les Ithink, dans le kindle et dans la grande majorité des téléphones portables. Dans quelques cas, les portes dérobées vont jusqu'à permettre l'installation à distance des changements de logiciels, par exemple dans Windows. Il y a une porte dérobée par laquelle Microsoft peut imposer n'importe quel changement de logiciel sans l'autorisation de l'utilisateur ou du propriétaire théorique de l'ordinateur. J'ai dit théorique, parce que dans la pratique Windows s'est emparé complètement de cet ordinateur. Microsoft s'en est emparé complètement. Si Windows exécute dans l'ordinateur, cette porte dérobée est universelle parce que n'importe quelle fonctionnalité malveillante qui n'est pas présente dans Windows aujourd'hui peut être imposée par la force demain. Mais les portes dérobées universelles existent aussi dans les téléphone portables, et ont été utilisées pour les convertir en dispositifs d'écoute, qui transmette toute la conversation dans la salle. Pas besoin de parler dans le micro, parce même dans la poche, il écoute et transmet tout.

Pourquoi est-ce que les fonctionnalités malveillantes sont si communes dans les logiciels privateurs ? C'est parce que le propriétaire reconnaît son pouvoir sur l'utilisateur, donc il ressent la tentation de l'abuser. Et s'il est psychopathe, qu'est ce qu'il fera : il utilisera son pouvoir pour gagner quelques avantages sur les utilisateurs, pour vendre quelque chose, juste pour avoir plus d'avantages. Donc il cherche toujours tout pouvoir dont il peut profiter. Mais chez les logiciels libres, il n'y a presque jamais de fonctionnalités malveillantes, parce que les utilisateurs ont le contrôle et les utilisateurs ne désirent pas les fonctionnalités malveillantes et avec les logiciels libres, les utilisateurs reçoivent ce qu'ils veulent. Si quelqu'un mettait une fonctionnalité malveillante dans un programme libre, n'importe quel utilisateur qui sait programmer pourrait le corriger, et les utilisateurs qui savent programmer, il y en a, et de temps en temps, ils étudient le code source pour ajouter quelques fonctionnalités oou corriger quelques erreurs. Comme cela, ils ont la possibilité de reconnaître la fonctionnalité malveillante dans le code, et s'il la reconnaisse, cette fonctionnalité malveillante, qu'est ce qu'ils font ? Ils la coupent, et ils annoncent le scandale : “regardez ce que j'ai trouvé dans ce programme”, et tous les programmeurs peuvent vérifier que c'est vrai, et qui l'avait introduit. Donc pas trop de tentations ! et c'est pour cela que les fonctionnalités malveillantes sont très rares chez le logiciel libre et très communes chez le logiciel privateur.

Mais quelles sont les libertés nécessaires pour que les utilisateurs aient le contrôle du programme ?

Il y en a quatre. La liberté zéro est celle d'exécuter le programme comme tu veux. la liberté un est celle d'étudier le code source du programme et de le changer pour qu'il fasse ton informatique comme tu veux. Et cette liberté nous donne le contrôle individuel à chaque utilisateur, mais le contrôle individuel ne suffit pas. Il faut les deux autres libertés essentielles. La liberté numéro deux est la liberté d'aider les autres, de redistribuer des copies exactes aux autres quand tu veux. La liberté trois est celle de contribuer à la communauté, c'est-à-dire de distribuer des copies de tes versions modifiées quand tu veux. Avec ces deux libertés, n'importe quel groupe d'utilisateurs peut ensemble maintenir sa version du programme, pour sa propre utilisation, ou pour l'utilisation de tout le monde s'il veut.

Pour être adéquate, ces libertés doivent s'appliquer à toutes les activités de la vie, y compris le commerce, parce que le commerce est une activité légitime, et ce n'est pas juste que l'informatique

d'une entreprise soit sous le pouvoir d'autres entreprises. Il faut réglementer le commerce, il faut réglementer les entreprises pour qu'elles ne puissent pas abuser tout le reste de la société, mais c'est autre chose. Ces réglementations doivent être imposées démocratiquement par l'état, et pas par les préférences d'autres entreprises. Donc les quatre libertés sont pour tout utilisateur, y compris les entreprises, mais aucune n'est obligatoire. La liberté zéro dit que tu peux exécuter le programme comme tu veux, mais si tu es masochiste, tu peux l'exécuter comme tu ne veux pas. Tu as aussi l'option de ne pas l'exécuter. Avec la liberté un tu peux étudier et changer le code source du programme, mais ce n'est jamais obligatoire et le cas usuel est de recevoir le programme et de l'utiliser sans regarder le code, parce que personne n'a tant de temps, et tout le monde a d'autre travail à faire, donc tu lis le programme quand tu veux, pour quelque raison. Avec la liberté deux tu peux faire des copies et les distribuer mais dans aucun cas il n'est obligatoire de le faire. Nous n'imposons pas que tu coopères avec quelqu'un, mais tu dois être libre de le faire quand tu veux. Par la liberté trois, si tu as fait une version modifiée, tu peux en distribuer des copies, mais ce n'est pas obligatoire, tu peux l'utiliser dans ta vie privée sans distribuer des copies, jamais, si c'est ta préférence. En ce cas, ta version est un programme privé. Pas privateur, privé est autre chose. Un programme privé, tu l'utilises dans ta vie privée. Si tu as les quatre libertés, ce programme est libre, ta copie de ce programme est libre. Un programme privateur se distribue de manière à priver les autres de leur liberté, et voici l'injustice.

J'ai lancé le mouvement des logiciels libres à l'année 83 et j'ai commencé en 84 le développement du système d'exploitation censé être complètement de logiciels libres, c'est à dire chaque programme serait libre. Le système entier n'aurait aucune, pas une seule ligne de code privateur, c'était le but. Et le système s'appelle GNU, ce qui veut dire GNU is Not Unix, c'est un acronyme récursif ! Nous avons travaillé beaucoup d'années dans le développement des centaines de composants nécessaires pour avoir un système semblable à Unix. Unix était privateur, mais avait beaucoup d'avantages techniques donc j'ai suivi la même conception technique mais il fallait remplacer chaque composant parce que nous ne pouvions pas utiliser les composants de Unix qui était privateur.

(44:30) A l'année 92 nous avions presque tous les systèmes : il manquait un seul composant important et essentiel, c'était le noyau. Le noyau du système est le composant qui fournit les ressources de la machine aux autres programmes et nous avions commencé le développement du noyau à l'année 90. Mais ce noyau, le “herd” c'est-à-dire “troupeau”, ne marche pas bien. Il fallait six ans pour avoir une version initiale. C'est dommage mais ce n'était pas un désastre car il ne fallait pas l'attendre à l'année 92. Mr Torvalds qui avait développé le noyau privateur dans l'année 92, a décidé de le libérer. En février 92 il a publié le code de Linux sous une des licences de logiciels libres, spécifiquement la licence public général de GNU, ou GPL de GNU, qui était une des licences libres qui s'utilisait à l'époque, mais pas la seule. C'est une confusion assez répandue, mais incorrecte : il y a d'autres licences libre, par exemple les deux licences BSD sont des licences libres, et beaucoup d'autres. Nous aurons un répertoire GNU.org/licences qui donne davantage d'information sur les licences libres et identifie aussi des licences qui ne sont pas libres. L Donc, la combinaison du système presque complet GNU et le noyau Linux était un système complet et libre. Pour la première fois, il était possible d'acheter un pc et l'utiliser en liberté avec ce système. Mais par confusion, ceux qui ont combiné ce noyau Linux avec les composants du système qui attendait d'être le système GNU ont appelé la combinaison comme un système Linux, qui n'était pas juste envers nous, et c'est comme ça que des millions utilisent le système GNU et ne le savent pas. Prière de les informer. Quand vous parlez de ce système, prière de l'appeler GNU et linux. Donnez-nous la reconnaissance égale. Et pourquoi GNU et pas FNU, SNU, ANU ? parce que GNU est un mot a d'autres significations, sans autre signification qui n'est pas un jeu de mots. donc j'ai choisi GNU parce que c'est un mot, c'est le nom de cet animal qui vit en Afrique et c'est aussi le mot le plus chargé d'humour de la langue anglaise. Parce qu'il s'utilise dans beaucoup de jeux de mots, parce que souvent dans le

dictionnaire le “g” est muet et le mot se prononce “NU”. C'est-à-dire “nouveau”. Donc chaque fois que tu veux écrire le mot “NEW” tu peux l'écrire GNU et c'est un jeu de mot. Peut-être pas très bon, mais il y en a beaucoup.

Donc le système nous rend possible l'utilisation d'un ordinateur sans logiciels privateurs, mais seulement si nous avons des pilotes pour les périphériques de l'ordinateur. Aujourd'hui nous avons un problème que nous n'avions jamais à l'année 1994. C'est-à-dire que le mode d'emploi du périphérique peut être secret. Ils te vendent le produit, mais ils ne te disent pas comment l'utiliser. Au lieu de te le dire, ils t'offrent un programme privateur pour le faire et c'est la seule manière d'utiliser leur produit. C'est injuste et cela doit être illégal. Mais c'est assez commun donc pour résoudre ce problème, il faut du génie inverse (NDLR : retro-engineering) pour comprendre le mode d'emploi du produit et pour ensuite écrire un programme libre pour le gérer. Donc si tu veux contribuer à quelque chose de très important par le travail technique, fais du génie inverse. C'est très important. Mais aujourd'hui nous avons d'autres problèmes. Des ordinateurs “tyrans”, qui ne permettent pas l'installation de logiciels modifiés. Beaucoup de produits Android sont tyrans. C'est-à-dire qu'ils viennent avec une version d'Android préinstallée, et l'utilisateur peut obtenir une version libre d'Android, mais ne peut pas installer cette version dans son ordinateur. En ce cas, le code source peut être libre, mais l'exécutable est privateur. Parce que l'utilisateur dispose avec ce code source des quatre libertés : il peut le changer, il peut en faire des copies, mêmes changées. Mais ce qu'il ne peut pas faire c'est utiliser sa propre version dans son propre ordinateur à lui. En ce cas, l'exécutable dans l'ordinateur n'est pas libre bien que son code source soit libre. Tu auras entendu parler du terme “open source”, pourquoi est-ce qu'ils disent cela au lieu de “logiciel libre” ? Parce qu'ils ne veulent pas dire “libre”, ils ne veulent pas poser la question de la liberté, poser la question de justice. Donc ils ont cherché une manière de présenter le sujet en oubliant complètement l'éthique, faisant uniquement attention aux valeurs pratiques. Si tu écoutes le discours de ceux qui disent “open source”, tu verras le manque de questions éthiques dans ce discours. Et l'absence complète de l'idée que les programmes privateurs sont injustes. Que le pouvoir du développeur sur les utilisateurs est injuste. Cela ils ne le mentionnent jamais. Parce que ils veulent coopérer avec les développeurs ou les vendeurs de logiciels privateurs, donc ils ne veulent pas les critiquer, donc ils ont construit le discours. Et les gens motivés par ce discours, par l'idée d'“open source” ont développé les programmes libres utiles, parce que l'utilité d'une contribution technique est indépendante de la philosophie derrière la contribution. Mais cette philosophie est faible quand la liberté est menacée, ce qui se fait souvent. Pour la maintenir il faut la défendre, mais pour la défendre il faut la valoriser et pour la valoriser il faut comprendre le concept de la liberté et voici ce qu'il manque. Donc quand il y a beaucoup d'utilisateurs d'un programme libre qui ne valorisent pas la liberté donc ils disposent, ils sont aptes à la perdre. Sur n'importe quel prétexte : quelqu'un leur offre un programme privateur attractif comme remplacement de ce programme libre, ils ne voient pas pourquoi le rejeter. S'ils n'apprécient pas la liberté comme telle. Donc pour établir une liberté durable il ne suffit pas de donner en cadeau la liberté à tout le monde, il faut les enseigner à valoriser la liberté pour la défendre après. Et voici la faute d'“open source”, c'est pour cela que je ne participe jamais dans des activités qui portent le drapeau d'open source. Uniquement les activités des logiciels libres. Parce que je veux que mon travail diffuse l'appréciation de la liberté, en même temps que n'importe quelle activité pratique. Il y a trop à faire dans ce champ, je ne peux pas faire tout. J'ai besoin, nous avons besoin, parce que je ne suis pas seul, (NDLR : pointant une personne) voici un autre activiste de la liberté, et il y en a des milliers, mais nous ne sommes pas assez. Nous avons besoin de tonnes d'aide. Et donc si tu choisis les activités qui disent “logiciels libres” et liberté de préférence, tu peux contribuer de deux manières à la fois.

Bon, autre menace, ça paraît de l'eau gazeuse

fichier son 2 (00:00)

c'est pour sa participation dans le système de surveillance d'Amesys, qui a été installé en Tunisie, et

aussi en Lybie pour Khadafi.

Maintenant, tu peux facilement utiliser des programmes privateurs sans le savoir, parce qu'ils viennent dans beaucoup de pages web. Beaucoup de pages web contiennent des programmes en javascript, et installent d'autres programmes en javascript, et pour la plupart ces programmes sont privateurs, ils s'installent dans le navigateur sans rien dire. Et donc, pour l'éviter, que faire ? Nous avons développé un programmes libreJS. Pour analyser le code javascript dans les pages, pour voir si le code est ou trivial, ou libre. Et dans ces deux cas, le programme s'exécute, mais si le programme n'est ni trivial ni libre, libreJS dit “cette page contient du code javascript non libre”, et bloque l'exécution ! Il offre une fonctionnalité de te plaindre facilement parce que le programme cherche où te plaindre. Tu n'as pas besoin de chercher dans le site comment te plaindre, parce que le programme le fait pour toi. Il suffit de dire “oui je veux me plaindre” et voici la fenêtre pour taper le texte de plainte. C'est très important d'envoyer beaucoup de plaintes, parce que nous devons faire pression sur la gestion des sites pour changer cette pratique.

Je suis à une chose de plus sur le logiciel libre. L'éducation doit enseigner uniquement le logiciel libre, c'est-à-dire à tous les niveaux d'écoles, même les universités. Les autres activités éducatives doivent enseigner uniquement les logiciels libres, et pas pour les économies, c'est un bienfait secondaire. Il y a des raisons éthiques pour rejeter le logiciel privateur dans l'éducation. Par exemple les écoles ont une mission sociale d“éduquer des bons citoyens d'une société capable, forte, solidaire, indépendante et libre. Dans l'informatique ça veut dire former des utilisateurs habitués aux logiciels libres, mais enseigner l'utilisation d'un programme privateur, et imposer la dépendance à une entreprise, il ne faut pas le faire, ne jamais le faire. Pourquoi est-ce que des développeurs de logiciels privateurs offrent aux écoles des copies gratuites, c'est comme les marchands de drogues qui offrent une dose gratuite, pour attirer, pour rendre dépendant les gens. Les développeurs de logiciels privateurs veulent que les écoles participent dans le projet de rendre dépendants les élèves, en leur enseignant l'utilisation de ce programme privateur, et après sa graduation, il ne reçoivent pas d'offres de copies gratuites. Ils travaillent peut-être pour des entreprises. Les entreprises ne reçoivent pas d'offres de copies gratuites.

(04:45) Donc l'école doit se souvenir de sa mission sociale et refuser les logiciels privateurs que ce soit gratuits ou pas. Mais il y a une autre raison plus profonde pour l'éducation des meilleurs programmeurs. Parce qu'il y a des jeunes qui ont le talent de programmer, qui sont des programmeurs-nés, et, pour apprendre à écrire bien le code, que doivent-ils faire ? Ils doivent lire beaucoup de code et écrire beaucoup de code. Mais uniquement les logiciels libres offrent l'opportunité de lire beaucoup de code, de grands programmes, comme nous utilisons. Et puis ils doivent écrire beaucoup de code, c'est-à-dire écrire du code dans des grands programmes, mais uniquement le logiciel libre leur offre l'opportunité d'écrire des changements parce que au commencement on est pas capable d'écrire tout un grand programme. Il faut commencer par le petit, c'est-à-dire des petits changements dans grands programmes déjà existants. Et seulement le logiciel libre offre cette opportunité. N'importe quelle école peut offrir aux programmeurs-nés l'opportunité de maîtriser leur talent mais seulement d'être une école de logiciels libres. Mais la raison la plus profonde est pour l'éducation morale dans la citoyenneté. Parce que l'école doit enseigner pas seulement des faits et des méthodes, elle doit enseigner l'esprit de bonne volonté, c'est-à-dire la coutume d'aider les autres. Donc chaque classe doit avoir cette règle. Les élèves, si tu apportes un programme à la classe, tu ne peux pas le garder pour toi, tu dois partager des copies avec le reste de la classe. Y compris le code source du programme pour le cas où quelqu'un veut apprendre, parce que cette classe est le mieux pour partager les connaissances. N'importe quel programme incorpore des connaissances. Si le programme est privateur, elles sont liées aux étudiants, mais si le programme est libre, ses connaissances sont offertes aux étudiants. Donc apporter un programme

privateur à la classe n'est pas permis. Uniquement des logiciels libres. Mais l'école doit suivre sa propre règle. L'école doit apporter uniquement des logiciels libres et partager les copies du code source, avec des exécutables bien sur. Avec tous les étudiants dans la classe.

(8:05) Avec l'utilisation des services du réseau viennent deux autres menaces à la liberté. D'abord la menace d'abuser tes données et aussi la menace d'abus de prendre le contrôle de ton informatique. La première est assez connue. On sait maintenant que les services font beaucoup de surveillance, mais ils demandent aussi beaucoup de données que l'utilisateur donne consciemment, mais dans tous les deux cas le site peut abuser ces données pour les montrer à quelqu'un d'autre. Et le site peut les montrer à quelqu'un pas autorisé par l'utilisateur. Sauf dans la cas où l'utilisateur utilise le site pour publier quelque chose, parce que si tu publies quelque chose, ça veut dire que tout le monde est invité à le voir. Il n'y a personne qui ne soit pas autorisé en ce cas. Mais dans les autres cas, si le site possède des données privées, en ce cas le site peut les abuser. Et si le site appartient à une entreprise américaine, c'est presque certain que le site abusera tes données, parce que, selon une loi, l'entreprise doit livrer, même sans ordre du tribunal, toutes les données qu'il possède sur toi au FBI, sans te le dire. Donc, évidemment tu ne dois jamais faire confiance à une entreprise américaine avec tes données.

L'autre menace est moins connue. Si tu utilises un service pour faire ta propre informatique, tu en perds le contrôle. C'est comme utiliser un programme privateur. Et ce cas s'appelle le “logiciel comme service”. C'est quand un site fait ce qu'un programme approprié aurait pu faire.

(10:54) avec le logiciel comme service, l'utilisateur fait sa propre informatique, pas en exécutant sa copie de programme, avec les données qu'il a dans son ordinateur à lui, mais au lieu de cela, il envoie toutes les données pertinentes au serveur de quelqu'un d'autre, qui fait son informatique et lui envoie le résultat, ou agit directement pour lui. Comme ça, qui a le contrôle de cette informatique ? Pas l'utilisateur, c'est le propriétaire du service qui a le contrôle de comment se fait le logiciel de l'utilisateur ! C'est le même résultat que d'avoir utilisé un programme privateur. Le même problème, mais c'est encore pire, parce que beaucoup de programmes privateurs contiennent des fonctionnalites de surveillance qui transmettent des données à quelques serveurs mais si l'utilisateur utilise le logiciel comme service, il doit envoyer toutes les données pertinentes au serveur, et c'est le même résultat, le serveur possède ses données, et qui sait ce qu'il fera avec après. Mais il est encore pire, j'ai mentionné les portes dérobées que beaucoup de programmes privateurs contiennent. Il y a même les portes dérobées universelles par lesquelles quelqu'un a le pouvoir de changer comment se fait l'informatique de l'utilisateur sans lui demander l'autorisation. Avec le logiciel comme service, le propriétaire du serveur peut à n'importe quel moment changer le logiciel dans le serveur et donc changer comment se fait l'informatique de l'utilisateur sans lui demander l'autorisation. Le logiciel comme service est donc l'équivalent d'utiliser un programme privateur avec des fonctionnalités de surveillance et une porte dérobée universelle, c'est à dire d'utiliser du malware. Il faut rejeter le logiciel cimme service comme il faut rejeter le logiciel privateur. Heureusement, le logiciel comme service est assez rare toujours. Si nous considérons tous les seveurs web du monde, presque tous ne font que présenter l'information. Et si tu regardes cette information, ce n'est pas faire ta propre informatique, donc ce problème ne se pose pas. Mais si nous considérons les serveurs qui offrent des services pas triviaux. La grande majorité font des services de communication, qui ne font pas ta propre informatique, donc ce sont très peu qui offrent de faire ta propre informatique, et ce service, le logiciel comme service, si tu peux imaginer d'avoir un programme qui fait la même informatique, fait la même chose que ce service, en ce cas, le service fait du logiciel comme service. Et quand je dis ta propre informatique, il s'agit de faire des computations avec les données que tu possèdes, sans interaction avec les autres utilisateurs. Quand il s'agit d'interagir avec les autres, il ne s'agit plus de ta propre informatique, mais d'une informatique collective, ou conjointe, et c'est autre cas. Tu ne pourrais pas le faire dans ton ordinateur sans communiquer avec personne. Donc s'il s'agit de

l'informatique de quelques uns ensemble, tu ne peux pas prévoir avoir le contrôle complet de cette informatique. Il ne t'appartient pas uniquement. C'est quand c'est ta propre informatique que tu peux avoir complètement le contrôle et donc dans ce cas perdre le contrôle est une injustice.

(16:34) Autre menace à notre liberté est le vote numérique. Il ne faut pas faire confiance aux ordinateurs dans les élections publiques. Parce que, si les ordinateurs comptent les votes, comment vérifier qu'ils ont fonctionnés correctement ? C'est impossible ! Il ne reste que les totaux. Et si pendant l'élection le programme fonctionne mal, peut-être délibérément, peut-être quelqu'un l'a changé pour faire une fraude, comment le savoir ? Même si des experts ont étudié d'avance le programme qui doit tourner pendant l'élections et ont dit ce programme paraît fonctionner correctement, comment savoir si le programme dans l'ordinateur pendant l'élection était le même ? Peut-être quelqu'un a pu installer une version modifiée le matin, pour que ce candidat gagne, et remplacer par la version correcte le soir. L'idée des systèmes électoraux pour le vote secret est que tout le monde puisse comprendre le fonctionnement du système pour que les actions de tous les participants, sauf le voteur, peuvent être surveillés par des autres participants, pour assurer que personne ne peut faire de fraude. Qui sait surveiller le fonctionnement correct de l'ordinateur ? Presque personne, seulement des experts, et cela ne suffit pas. Donc, il faut rejeter le vote numérique. Il faut noter aussi que ce n'est pas une question technique. Il y en a qui proposent des systèmes sophistiqués d'encryption qui supposément garantissent le résultat correct. Mais ce n'est pas un problème de la mathématique. Un système électoral est un système social aussi. Trouver les points faibles dans ce système n'est pas un exercice de la mathématique. Il faut des années d'expériences pour savoir si le système est vulnérable.

Autre menace à notre liberté est la guerre contre le partage. (20:20)