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

Vers une société numérique libre

EN CONSTRUCTION

Cette transcription sonore réalisée au sein de l'association LoLiGrUB est sous la licence GNU Free Documentation License 1.3 du wiki du site de l'A.S.B.L. LoLiGrUB.

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

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 niumérique, 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 particuper. 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. Mais 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 ? Et 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. Mais 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 ses buts individuels, comment limiter ce que fait l'état avec ces données. Cela ne suffit parce que ce changement est une grande augmentation dans le 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'il voulait 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'imposent 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.

Mais 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 utilises 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 probléme 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 procés 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 reconnait 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 logiciles 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 quatres 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)

From:
https://www.loligrub.be/wiki/ - **LoLiGrUB**

Permanent link:
https://www.loligrub.be/wiki/conference_richard_stallman_bruxelles_27_septembre_2012?rev=1351205879

Last update: **2014/12/27 08:13**