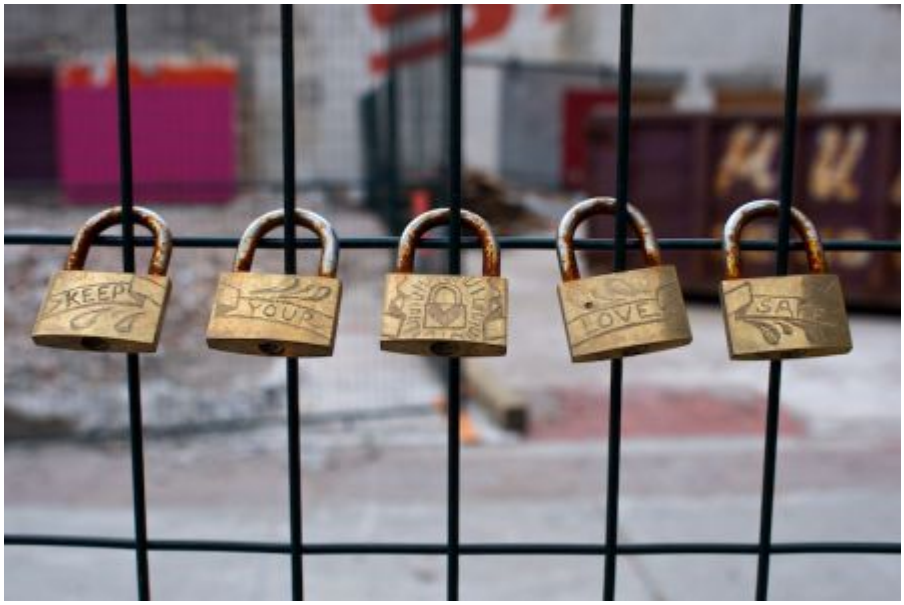
On ferme ! La guerre imminente contre nos libertés d'utilisateurs, par Cory Doctorow

Il y a un mois Cory Doctorow a donné une conférence remarquable et remarquée lors du fameux CCC de Berlin.

Tellement remarquée qu'il a décidé d'en faire a posteriori un *long* mais passionnant article dont nous vous proposons la traduction aujourd'hui (merci @ricomoro)[1].

La guerre contre le copyright préfigure une guerre totale contre les ordinateurs et donc nos libertés d'utilisateurs. C'est pourquoi il est fondamental de la gagner…



On ferme

La guerre imminente contre nos libertés d'utilisateurs

Lockdown – The coming war on general-purpose computing

Cory Doctorow – 10 janvier 2012 – BoingBoing
(Traduction Framalang : Don Rico – Relecture : Goofy)

Cet article reprend une intervention donnée au Chaos Computer Congress de Berlin, en décembre 2011.

Les ordinateurs sont époustouflants. À tel point que notre société ne sait toujours pas très bien les cerner, peine à comprendre exactement à quoi ils servent, par quel bout les prendre, et comment se débrouiller avec. Ce qui nous ramène à un sujet sur lequel on a écrit ad nauseam : le *copyright*.

Mais je vous demande un peu de patience, car je vais aborder ici une question plus importante. La forme que prend la guerre contre le copyright présage d'un combat imminent qui se livrera pour le destin de l'ordinateur lui-même.

Aux débuts de l'informatique grand public, nous achetions les logiciels dans des emballages et nous échangions des fichiers de la main à la main. On trouvait les disquettes dans des sachets hermétiques, dans des cartons, alignées dans des rayons à la façon des paquets de gâteaux et des magazines. Rien n'était plus facile que de les dupliquer, la copie était très rapide et très répandue, au grand dam des concepteurs et des vendeurs de logiciels.

Arrivent les *verrous numériques* (les DRM), dans leurs formes les plus primitives – nous les appellerons DRM 0.96. Pour la première fois, on eut recours à des marqueurs physiques – dégradation délibérée, dongles, secteurs cachés – dont le logiciel contrôlait la présence, ainsi qu'à des protocoles *défi-réponse* qui nécessitaient de posséder des modes d'emploi encombrants et difficiles à copier.

Ces mesures échouèrent pour deux raisons. Premièrement, elles connurent une grande impopularité commerciale, car elles réduisaient l'utilité du logiciel pour ceux qui le payaient. Les acquéreurs honnêtes voyaient d'un mauvais œil que leurs sauvegardes ne soient pas utilisables, n'appréciaient guère de perdre un de leurs ports, déjà rares, à cause des clés matérielles d'autentification, et s'irritaient de devoir manipuler de volumineux modes d'emploi lorsqu'ils souhaitaient lancer leur logiciel. Deuxièmement, ces mesures ne découragèrent pas les pirates, pour qui patcher le logiciel et contourner l'authentification était un jeu d'enfant. L'effet fut nul sur ceux qui se procuraient le logiciel sans le payer.

En gros, cela ce passait ainsi : un programmeur, possédant du matériel et des compétences du même niveau de sophistication que l'éditeur du logiciel, décortiquait le programme par rétro-ingénierie et en diffusait des versions

crackées. Un tel procédé peut paraître très pointu, mais en fait, il n'en était rien. Comprendre le fonctionnement d'un programme récalcitrant et contourner ses défauts constituaient les compétences de base de tout programmeur, surtout à l'époque des fragiles disquettes et des débuts balbutiants du développement logiciel. Les stratégies destinées à combattre la copie devinrent plus inutiles encore lorsque les réseaux se développèrent. À l'apparition des BBS, services en ligne, newsgroups Usenet et listes de diffusion, le résultat du travail de ceux qui parvenaient à surmonter les systèmes d'authentification put être distribué sous forme de logiciel, dans de petits fichiers de crack. Lorsque les capacités du réseau s'accrurent, on put diffuser directement les images disque ou les exécutables crackés.

Vinrent alors les DRM 1.0. En 1996, il devint évident dans les lieux de pouvoir qu'un bouleversement d'envergure allait se produire. Nous allions entrer dans une économie de l'information, sans qu'on sache trop ce qu'était ce machin. Nos élites supposèrent que ce serait une économie où l'on achèterait et vendrait de l'information. La technologie de l'information améliore l'efficacité, alors imaginez un peu les marchés potentiels qui s'offraient à nous ?! On allait pouvoir acheter un livre pour une journée, vendre le droit de visionner un film pour un euro, puis louer le bouton pause pour un centime la seconde. On allait pouvoir vendre des films à un certain prix dans un pays, à un prix différent dans un autre, etc. Les fantasmes de l'époque ressemblaient à une adaptation SF ennuyeuse du Livre des Nombres de l'Ancien Testament, une énumération fastidieuse de toutes les combinaisons possibles de ce qu'on fait avec l'information, et combien chacune allait être facturée.

Hélas pour eux, rien de tout cela n'était possible à moins de pouvoir contrôler la façon dont nous utilisions nos ordinateurs, et les fichiers que nous y transférions. En fait, il était facile d'envisager de vendre à quelqu'un des morceaux de musique à télécharger sur un lecteur MP3, mais plus compliqué d'envisager le droit de transférer une chanson du lecteur vers un autre appareil. Comment en effet en empêcher les acheteurs une fois qu'on leur a vendu le fichier ? Pour cela, il fallait trouver un moyen d'interdire aux ordinateurs d'exécuter certains programmes, d'inspecter certains fichiers et processus. Par exemple, pourquoi ne pas chiffrer le fichier, puis exiger de l'utilisateur qu'il le lise avec un lecteur audio qui ne le déverouillerait que sous des conditions précises ?

Mais là, comme on dit sur internet, *on se retrouve avec deux problèmes*.

Il faut à présent empêcher l'utilisateur d'enregistrer le fichier après qu'il a été déchiffré – ce qui se produira un jour ou l'autre –, et faire en sorte que l'utilisateur ne découvre pas où le programme de déverrouillage entrepose ses clés, ce qui lui permettrait de déchiffrer le média de façon permanente et se débarrasser une bonne fois pour toutes de leur lecteur audio à la con.

Voilà donc un *troisième* problème : il faut empêcher les utilisateurs qui parviennent à déchiffrer le fichier de le partager. Un *quatrième* problème se pose alors, car ces utilisateurs qui réussissent à arracher leurs secrets aux programmes de déverrouillage, il faut les empêcher d'expliquer à d'autres comment procéder. S'ajoute au tout un *cinquième* problème, parce que les utilisateurs qui comprennent comment extraire ces secrets, il faut les empêcher de les dévoiler à d'autres !

Ça fait un paquet de problèmes. Mais en 1996, on trouva la solution. L'Organisation mondiale de la propriété intellectuelle des Nations Unies signa le Traité de l'OMPI sur le droit d'auteur. Ce traité engendra des lois qui rendaient illégal d'extirper les clés secrètes des programmes de déverrouillage, d'extraire des fichiers média (tels que des chansons ou des films) de ces programmes de déverrouillage lors de leur fonctionnement. On vota des lois qui rendaient illégal d'expliquer à ses pairs comment extirper les clés secrètes des programmes de déverrouillage, ainsi que d'héberger ces mêmes clés ou des œuvres placées sous copyright. Grâce à ce traité, on mit également en place un procédé bien ficelé et fort commode qui permet de faire retirer du contenu d'internet sans avoir à se coltiner avocats, juges, et tous ces emmerdeurs.

Après quoi, la copie illégale fut éradiquée, l'économie de l'information s'épanouit pour devenir une fleur splendide qui apporta la prospérité au monde entier. Comme on dit sur les porte-avions, « Mission accomplie ».

Non. Ce n'est pas ainsi que l'histoire se termine, bien sûr, car presque tous ceux qui maîtrisaient les ordinateurs et les réseaux comprirent que ces lois allaient créer plus de problèmes qu'elles ne pourraient en résoudre. Après tout, ces lois rendaient illégal le fait de regarder dans le ventre de son ordinateur pendant qu'il exécutait certains programmes. À cause d'elles, il était illégal de raconter à d'autres ce qu'on avait découvert sous le capot, et plus facile que jamais de censurer des fichiers sur internet sans devoir justifier d'une infraction.

En résumé, ces lois soumettaient des exigences irréalistes à la réalité, qui a refusé de s'y plier. Depuis le vote de ces lois, il est au contraire devenu plus *facile* de copier – et cette tendance ne s'inversera jamais. Il ne sera toujours plus *aisé* de copier demain qu'aujourd'hui. Vos petits-enfants vous demanderont : « Raconte-moi encore, papi, comme c'était compliqué de copier des fichiers, en 2012, quand on n'avait pas de disque de la taille d'un ongle sur lequel on peut stocker tous les albums jamais enregistrés, tous les films jamais tournés, tous les textes jamais écrits, toutes les photos jamais prises, absolument tout, et les transférer en un temps si court qu'on ne s'en rend même pas compte ! »

La réalité reprend toujours ses droits. Il existe une comptine dans laquelle une femme gobe une araignée pour attraper une mouche, avale ensuite un oiseau pour attraper l'araignée, et enfin un chat pour attraper l'oiseau. Il en va de même pour ces réglementations, qui semblent très prometteuses sur le papier, mais se révèlent désastreuses une fois appliquées. Chaque régulation en engendre une nouvelle, qui ne vise qu'à colmater ses propres manquements.

La tentation est forte d'interrompre ici mon récit et de conclure que le problème vient des régulateurs, qui seraient soit idiots, soit mal intentionnés, voire les deux à la fois. C'est une voie qu'il ne serait pas satisfaisant d'emprunter, parce qu'il s'agirait au fond d'un aveu d'impuissance. Cela laisserait entendre que nos problèmes ne peuvent être résolus tant que stupidité et mauvaises intentions n'auront pas été écartés des lieux de pouvoirs, autant dire jamais. En ce qui me concerne, j'ai une théorie différente pour expliquer ce qui s'est passé.

Le problème, ce n'est pas que les législateurs n'entendent rien aux technologies de l'information, parce qu'il devrait être possible qu'un non spécialiste parvienne à rédiger une bonne loi. Parlementaires, membres du Congrès et autres hommes politiques sont élus pour représenter des circonscriptions et des citoyens, pas pour s'occuper de disciplines et de questions pointues. Nous n'avons pas un secrétaire d'État à la biochimie, ni un sénateur issu du magnifique État qu'est l'urbanisme. Pourtant, ces personnes, qui sont des experts de la politique et de l'élaboration des lois, et pas de disciplines techniques, réussissent malgré tout à établir des règles sensées. C'est parce que le gouvernement s'appuie sur l'heuristique : une approche empirique qui permet d'équilibrer les contributions d'experts apportant leur avis sur différents aspects d'une question.

Hélas, il existe un point sur lequel la technologie de l'information est supérieure à

cette heuristique, et la *bat* même à plates coutures.

Il existe deux conditions importantes pour déterminer si une régulation est pertinente : d'abord, il faut savoir si elle sera efficace, et ensuite, si ses effets s'étendront *au-delà de ce pour quoi elle a été conçue*. Si je voulais que le Congrès, le Parlement, ou l'UE préparent une loi réglementant l'usage de la roue, il est peu probable que j'y parvienne. Si je me présentais en avançant que les braqueurs de banque s'enfuient toujours dans un véhicule à roues, et demandais si on peut y remédier, on me répondrait non. Pour la simple raison qu'on ne connaît aucun moyen de fabriquer une roue qui reste utilisable pour un usage licite, mais soit inutilisable pour les bandits. Il est évident pour tous que le bénéfice général des roues est si grand qu'il serait idiot de s'en passer, dans une tentative farfelue d'enrayer les braquages. Même si l'on connaissait une flambée de braquages – et même s'ils mettaient en péril la société –, personne ne songerait que s'en prendre aux roues puisse être un bon point de départ pour résoudre nos problèmes.

En revanche, si je me présentais dans cette même institution, déclarais posséder la preuve irréfutable que les kits mains-libres rendent les voitures dangereuses, et que je demandais une loi les interdisant, il n'est pas impossible que le régulateur prenne ma requête en compte et agisse sur la question.

On pourrait débattre de la légitimité de cette idée, du caractère sensé de mes preuves, mais très peu d'entre nous pourrions avancer que si l'on retire les kits main-libre, *une voiture cesse d'être une voiture*.

Nous sommes d'accord pour dire qu'une voiture reste une voiture si nous en retirons des accessoires. Les automobiles sont des engins à but précis, du moins si on les compare à la roue, et le seul apport d'un kit mains-libres, c'est une fonction supplémentaire ajoutée à une technologie déjà spécialisée.

De manière générale, cette approche empirique est efficace pour le législateur, mais elle devient caduque pour la question de l'ordinateur et du réseau généralistes – le PC et l'internet. Si l'on considère un logiciel comme une fonction, un ordinateur équipé d'un tableur a une fonction tableur, et un autre qui ferait tourner World of Warcraft aurait une fonction MMORPG. En appliquant la méthode heuristique, on pourrait penser qu'un ordinateur ne pouvant exécuter des feuilles de calcul ou des jeux ne constituerait pas davantage une atteinte à l'informatique qu'une interdiction des kits mains-libres ne le serait pour les

voitures.

Et si l'on considère les protocoles et les sites web comme des fonctions du réseau, alors demander à modifier l'internet pour que BitTorrent n'y fonctionne plus ou que The Pirate Bay n'y apparaisse plus, cela n'est pas très différent de vouloir changer la tonalité du signal de ligne occupée, ou de déconnecter la pizzeria du coin du réseau téléphonique, et n'équivaut pas à une remise en question des principes fondamentaux de l'internet.

La méthode empirique fonctionne pour les voitures, les maisons, et tous les autres domaines majeurs des réglementations technologiques. Ne pas comprendre qu'elle n'est pas efficace pour l'internet, ce n'est pas être quelqu'un de mauvais, ni un ignare. C'est faire partie de la grande majorité de la population, pour qui le Turing-complet et le principe de bout-à-bout ne veulent rien dire.

Nos législateurs se lancent donc et votent allègrement ces lois, qui intègrent la réalité de notre univers technologique. Soudain, nous n'avons plus le droit de diffuser certaines séries de chiffres sur internet, il est interdit de publier certains programmes, et pour faire disparaître des fichiers licites du réseau, une simple accusation d'infraction au droit d'auteur suffit. Ces mesures échouent à atteindre l'objectif de la réglementation, car elles n'empêchent personne d'*enfreindre* le copyright, mais de façon très superficielle, elles donnent l'impression que l'on fait respecter le droit d'auteur – elles satisfont au syllogisme de la sécurité : « Il faut prendre les mesures nécessaires, je prends des mesures, donc le nécessaire à été fait. » Résultat, au moindre échec, on peut prétendre que la réglementation ne va pas assez loin, au lieu de reconnaître qu'elle était inefficace depuis le début.

On retrouve ce genre de similarité superficielle et d'opposition sous-jacente dans d'autres domaines. Un de mes amis, autrefois cadre supérieur dans une grosse entreprise de biens de consommation courante, m'a raconté ce qui s'est passé lorsque les membres du service marketing avaient annoncé aux ingénieurs qu'ils avaient trouvé une idée formidable pour une lessive : désormais, ils allaient fabriquer une lessive grâce à laquelle les vêtements sortiraient *plus neufs à chaque lavage* !

Après avoir tenté sans succès d'expliquer au service marketing la loi de l'entropie, ils parvinrent à une autre solution : ils conçurent une lessive contenant des enzymes qui attaquaient les fibres éparses, celles-là mêmes qui donnent un

aspect usé aux vêtements. À chaque machine, le linge paraissait plus neuf. Malheureusement, cela se produisait parce que le détergent digérait les habits. En l'utilisant, on condamnait littéralement le linge à se désagréger.

C'était évidemment l'inverse du but recherché. Au lieu de rajeunir les vêtements, on les vieillissait de façon artificielle à chaque passage en machine, et en tant qu'utilisateur, plus on appliquait cette « solution », plus on devait prendre des mesures radicales pour garder une garde-robe à jour. Au bout du compte, il fallait acheter des vêtements neufs parce que les anciens tombaient en lambeaux.

Aujourd'hui, certains services marketing déclarent : « Pas besoin d'ordinateurs, ce qu'il nous faut, ce sont des appareils électroménagers. Fabriquez-nous un ordinateur qui ne permet pas de tout faire, seulement de lancer un programme qui effectue une tâche spécialisée, comme lire de l'audio en streaming, transférer des paquets, ou jouer à des jeux Xbox, et surtout, il ne doit pas faire tourner un programme que nous n'avons pas autorisé et qui risquerait d'amoindrir nos profits. »

En surface, l'idée d'un programme ne servant qu'à une fonction spécialisée n'a rien de farfelu. Après tout, on peut installer un moteur électrique dans un lave-vaisselle, et installer un moteur dans un mixeur, et peu nous importe de savoir si l'on peut lancer un programme de lavage dans un mixeur. Mais ce n'est pas ce qui se produit lorsqu'on transforme un ordinateur en appareil électroménager. On ne fabrique pas directement un ordinateur qui ne fait tourner que l'application de l'« appareil ». On prend un ordinateur capable d'exécuter tous les programmes, puis, grâce à un ensemble de rootkits, d'espiogiciels et de codes de validation, on empêche l'utilisateur de savoir quels processus sont actifs, d'installer ses propres logiciels, et d'interrompre les processus qu'il ne désire pas. En d'autres termes, un appareil électroménager n'est pas un ordinateur réduit à sa plus simple expression, c'est un ordinateur entièrement fonctionnel bourré d'espiogiels.

Nul ne sait concevoir un ordinateur généraliste capable de faire fonctionner tous les programmes sauf ceux qui déplaisent au constructeur, sont interdits par la loi, ou font perdre de l'argent à une entreprise. Ce qui s'en approche le plus, c'est un ordinateur bardé d'espiogiciels, une machine sur laquelle des parties tierces décident de limitations sans que l'utilisateur en soit averti, ou malgré les objections du propriétaire de la machine. Les outils de gestion des droits numériques s'apparentent toujours à des logiciels malveillants.

À l'occasion d'un incident qui a fait couler de l'encre (un vrai cadeau pour ceux qui partage mon hypothèse), Sony a dissimulé des installeurs de rootkits sur six millions de CDs audio, lesquels exécutaient subrepticement des programmes qui surveillaient toute tentative de lire les fichiers sons du CD et les interrompaient. Les rootkits cachaient aussi leur existence en poussant le noyau de l'ordinateur à mentir sur les processus en activité et les fichiers présents sur le support. Et ce n'est pas le seul exemple de ce genre. La 3DS de Nintendo profite des mises à jour de son firmware pour procéder à un contrôle d'intégrité, et vérifier que l'ancien firmware n'a subi aucune altération. Au moindre signe qu'on a mofifié le programme, la console devient inutilisable.

Des défenseurs des droits de l'homme ont tiré le signal d'alarme concernant U-EFI, le nouveau programme d'amorçage des PC, qui restreint votre ordinateur de sorte qu'il n'exécute que les systèmes d'exploitation « homologués », faisant valoir que des régimes répressifs allaient vraisemblablement refuser l'homologation des systèmes d'exploitation qui ne permettraient pas des opérations de surveillance furtives.

En ce qui concerne le réseau, les tentatives de le modeler pour qu'il ne puisse servir à enfreindre le droit d'auteur rejoignent toujours les mesures de surveillance mises en place par des régimes répressifs. Prenons par exemple SOPA, la proposition de loi pour la lutte contre le piratage, qui interdit des outils inoffensifs tels que DNSSec (une suite de sécurité qui authentifie les informations envoyées par un nom de domaine) parce qu'il pourrait servir à contrecarrer des mesures de blocage de DNS. SOPA proscrit également Tor, un outil d'anonymat en ligne soutenu par le Naval Research Laboratory *(NdT : laboratoire de recherche de la Marine des États-Unis)*, et utilisé par les dissidents dans les régimes totalitaires, parce qu'il permet de contourner des mesures de blocage d'adresse IP.

La Motion Picture Association of America *(NdT : MPAA, l'organisme qui défend les intérêts de l'industrie cinématographique)*, un des partisans de SOPA, a même fait circuler un mémo qui citait des recherches avançant que SOPA *pourrait fonctionner* parce qu'elle s'appuie sur des mesures éprouvées en Syrie, en Chine et en Ouzbékistan. On y expliquait que, ces procédés étant efficaces dans ces pays, ils le seraient aussi aux États-Unis !

On pourrait avoir l'impression que SOPA *(NdT : quand ce billet a été écrit,*

SOPA/PIPA n'avaient pas encore été ajournées suite au blackout) siffle la fin de partie au terme d'une longue lutte au sujet du copyright et d'internet, et l'on pourrait croire que si nous parvenons à faire rejeter SOPA, nous serons en bonne voie pour pérenniser la liberté des PC et des réseaux. Mais comme je l'ai précisé au début de cette intervention, le fond du sujet, ce *n'est pas* le copyright.

La bataille du copyright n'est que la version bêta d'une longue guerre qui va être menée contre l'informatique. L'industrie du divertissement n'est que le premier belligérant à prendre les armes, et dans l'ensemble, on peut penser qu'elle remporte de belles victoires. En effet, nous voici face à SOPA, qui est sur le point d'être votée, prête à briser les fondements de l'internet, le tout pour protéger les tubes du Top 50, les émission de télé-réalité et les films d'Ashton Kutcher.

En réalité, si la législation sur le copyright va aussi loin, c'est parce que les politiciens ne prennent pas la question au sérieux. C'est pourquoi, au Canada, les Parlements successifs n'ont eu de cesse de présenter des propositions de loi plus calamiteuses les unes que les autres, mais en contrepartie, ces mêmes Parlements n'ont jamais été capables de les voter. C'est pourquoi SOPA, une proposition de loi composée de *stupidité à l'état pur* et assemblée molécule par molécule pour former une sorte de « Stupidium 250 » que l'on ne trouve normalement que dans le noyau des jeunes étoiles, a vu son examen reporté au beau milieu des vacances de Noël – pour que les législateurs puissent participer à un débat national enflammé sur une question autrement *importante*, l'assurance chômage.

C'est pourquoi l'Organisation mondiale de la propriété intellectuelle se fait duper et promulgue des lois délirantes et d'une ignorance crasse ; parce que lorsqu'une nation envoie une mission à l'ONU de Genève, ce sont des experts en eau, pas en copyright. Des experts de la santé, pas du copyright. Des experts en agriculture, et toujours pas du copyright, parce que c'est loin d'être aussi important.

Le parlement canadien n'a pas soumis ces propositions de loi au vote parce que, parmi les inombrables sujets que le Canada doit traiter, les problèmes de copyright arrivent très loin derrière les urgences sanitaires dans les réserves indiennes, l'exploitation de la nappe pétrolière d'Alberta, l'intervention dans les frictions sectaires entre francophones et anglophones, la résolution des crises dues aux ressources de pêche, et des tas d'autres problèmes. À cause du caractère anodin du copyright, une chose est sûre : dès que d'autres secteurs de l'économie évinceront les inquiétudes au sujet de l'internet et du PC, on se rendra

compte que la question du copyright n'était qu'une escarmouche, pas une guerre.

Pourquoi d'autres secteurs risquent-ils de s'en prendre aux ordinateurs comme c'est déjà le cas de l'industrie du divertissement ? Dans le monde d'aujourd'hui, tout est ordinateur. Nous n'avons plus de voitures, mais des ordinateurs qui roulent. Nous n'avons plus d'avions, mais des machines sous Solaris qui volent, agrémentées d'un tas de dispositifs de contrôle industriels. Une imprimante 3D n'est pas un appareil ménager, c'est un périphérique qui ne fonctionne qu'en étant connecté à un ordinateur. Une radio n'a plus rien du poste à galène d'antan, c'est un ordinateur généraliste qui utilise un logiciel. Le mécontentement que soulèvent les copies non autorisées du dernier best-seller à la mode sera insignifiant comparé aux appels aux armes que créera bientôt notre réalité tissée d'ordinateurs.

Prenons l'exemple de la radio. Jusqu'à présent, la réglementation concernant les radios se fondait sur l'idée que les propriétés d'une radio sont fixées à la fabrication, et qu'il est difficile de les modifier. Il ne suffit pas d'actionner un interrupteur sur votre babyphone pour capter d'autres signaux. Mais des radios logicielles puissantes peuvent servir d'interphone pour bébé, de répartiteur pour services d'urgence ou d'outil de contrôle aérien, simplement en chargeant et en exécutant un logiciel différent. C'est pourquoi la Federal Communications Commission (FCC) *(NdT : Commission fédérales des communications)* s'est intéressée à ce qui allait se produire lorsque les radios logicielles seraient disponibles, et a organisé une consultation pour savoir si elle devait imposer que toutes les radios logicielles soient enchâssées dans des machines d'« informatique de confiance ». En définitive, la question est de savoir si les PC devraient être verrouillés, de telle sorte que leurs programmes puissent être strictement contrôlés par des autorités centrales.

Là encore, ce n'est qu'un avant-goût de ce qui nous attend. C'est cette année seulement que sont apparues des *limes* open source pour transformer des fusils AR-15 en armes automatiques. C'est cette année qu'on a créé pour la première fois du matériel libre et financé collectivement destiné au séquençage génétique. Tandis que l'impression 3D donnera lieu à des tas de plaintes sans importance, des juges du Sud des États-Unis et des mollahs iraniens piqueront une crise quand des habitants de leur circonscription modèleront des sex-toys. Ce qu'il sera possible de fabriquer avec les imprimantes 3D, qu'il s'agisse de labos à méthemphétamine ou de couteaux céramiques, provoquera de véritables

protestations.

Pas la peine d'être auteur de science-fiction pour comprendre que les régulateurs auront des suées à l'idée que l'on puisse modifier le firmware des voitures sans conducteur, limiter l'interopérabilité dans les systèmes de contrôle aérien, ou tout ce qui serait possible d'accomplir avec des assembleurs et séquenceurs moléculaires. Imaginez ce qui se passera le jour où Monsanto décrétera qu'il est *primordial* de s'assurer que les ordinateurs ne puissent exécuter des programmes grâce auxquels des périphériques produiraient des organismes modifiés qui, *littéralement*, concurrenceraient leur gagne-pain.

Qu'il s'agisse selon vous d'inquiétudes légitimes ou de peurs insensées, elles restent néanmoins la monnaie politique de lobbies et de groupes d'intérêt beaucoup plus puissants que Hollywood et l'industrie du divertissement. Tous finiront par formuler la même requête : « Fabriquez-nous donc un ordinateur grand public qui exécute tous les programmes, sauf ceux qui nous effraient et nous déplaisent. Fabriquez-nous un internet qui transmet des messages, sur tous les protocoles, d'un point à une autre, sauf si ça nous dérange. »

Parmi les programmes qui tourneront sur des ordinateurs grand public et leurs périphériques, cerains me ficheront les jetons à moi aussi. J'imagine donc sans mal que les partisans d'une limitation de ces ordinateurs trouveront une oreille réceptive. Mais comme cela s'est produit avec la guerre du copyright, interdire certaines instructions, certains protocoles et messages sera un moyen de prévention ou un remède tout aussi inefficace. Comme nous l'avons vu au cours de la guerre du copyright, toute tentative de contrôler les PC mènera à l'installation de rootkits, et toute tentative de contrôler l'internet débouchera sur la surveillance et la censure. Ces questions sont importantes, car depuis dix ans, nous envoyons nos meilleurs joueurs combattre ce que nous prenions pour le dernier boss du jeu, mais il s'avère que ce n'était qu'un boss secondaire. Les enjeux seront toujours plus importants.

Appartenant à la génération Walkman, je me suis résolu au fait que j'aurai besoin d'un appareil auditif pour mes vieux jours. Cela étant, ce ne sera pas un simple sonotone ; en réalité, ce sera un ordinateur. Quand je monterai dans ma voiture – un ordinateur dans lequel je place mon corps – équipé de mon aide auditive – un ordinateur que je place dans mon corps –, je veux donc être certain que ces technologies ne sont pas conçues pour me cacher des informations, ou

m’empêcher de mettre fin à un processus qui œuvre contre mon intérêt.

L’année dernière, le secteur scolaire de Lower Merion, dans une banlieue aisée de Philadelphie, s’est trouvé au centre d’un scandale. On a découvert que les établissements distribuaient aux élèves des ordinateurs portables rootkités qui permettaient de procéder à une surveillance furtive et à distance, via la webcam et la connexion réseau. Les machines ont pris des milliers de photos des adolescents, chez eux et en cours, de jour ou de nuit, vêtus ou nus. Dans le même temps, la dernière génération de technologie de surveillance légale peut activer secrètement les caméras, les micros et les émetteurs-récepteurs GPS des PC, tablettes et appareils mobiles.

Nous n’avons pas encore perdu, mais si nous voulons que l’internet et les PC restent libres et ouverts, nous devons d’abord gagner la guerre du copyright. À l’avenir, afin de préserver notre liberté, nous devrons être en mesure de contrôler nos appareils et d’établir des réglementations sensées les concernant, d’examiner et d’interrompre les processus logiciels qu’ils exécutent, et enfin, de les maîtriser pour qu’ils restent d’honnêtes serviteurs de notre volonté, au lieu de devenir des traîtres et des espions à la solde de criminels, de bandits et de maniaques du contrôle.

Notes

[1] Crédit photo : Francis Mariani (Creative Commons By-Nc-Nd)