PETITES ASTUCES CONTRE LA CENSURE ET LE CONTROLE D'INTERNET

PAR KORBEN

VERSION 0.1

JUIN 2004

Ce document a été rédigé fin mai 2004 essentiellement sur Pocket PC lors de mes trajets en train.
J'ai voulu rédiger un genre de « mémo » destiné aux débutants qui se sentent perdus dans la jungle de l'informatique et d'Internet. C'est en réalité un recueil de conseils qui vous seront, je l'espère utiles face aux « cyber-délinquants » et surtout face à cette répression et ce contrôle de l'information numérique qui semble de plus en plus présent dans notre quotidien.

1) Introduction

Le 6 mai 2004, la LEN (Loi sur l'Economie Numérique) a été définitivement adoptée par le Sénat. Cette loi liberticide prive les internautes d'un bon nombre de droits fondamentaux.

A cause de cette loi :
(extrait du site **www.odebi.org**)

Les "hébergeurs" devront se substituer à l'autorité judiciaire, juger et censurer les contenus. Ce transfert de l'autorité judiciaire à des groupes privés constitue en pratique une privatisation de la justice complètement contraire à l'état de droit et à la tradition républicaine.

Les acteurs ou les activités, concernés par cette obligation de jugement et de censure ne sont pas précisés, ce qui fait peser un risque sur de nombreux intermédiaires techniques qui ne sauront tout simplement même pas s'ils sont ou non concernés par cette obligation.

Une des dispositions prévoit que, comme elle est par exemple limitée par des considérations d'ordre public, la liberté d'expression des citoyens pourra désormais être limitée par... l'intérêt de l'industrie audiovisuelle, au mépris total de la convention européenne des droits de l'homme. Nul ne peut accepter que les intérêts économiques de ce lobby puissent prévaloir sur la liberté d'expression, droit constitutionnel et rouage essentiel de la démocratie.

- la durée de prescription de la diffamation des contenus publiés en ligne passera de trois mois à compter de leur date de publication (comme dans la presse) à trois mois à partir de leur date de suppression. Le premier effet de cette mesure sera de nuire à la diversification de l'information offerte par Internet, puisque ce média serait désormais soumis à un régime infiniment plus sévère que celui de la presse. Cette disposition ne manquera pas d'entraîner un phénomène d'autocensure a priori ainsi que la suppression a posteriori de contenus publiés. Au-delà de l'atteinte immédiate à la liberté d'expression et d'information, cette disposition va provoquer un appauvrissement considérable des contenus francophones sur internet.

- enfin, la notion de correspondance privée sera supprimée de la définition du courrier électronique, ouvrant ainsi la porte à d'intolérables atteintes au secret des correspondances.

Rajoutez à cela, la nouvelle LIL (Loi Informatique et Libertés) qui est tout aussi liberticide, autorisant par exemple, **les industries culturelles** à constituer des fichiers d'infractions présumées, véritables casiers judiciaires privés.

N'oubliez pas non plus la loi sur les brevets logiciel qui risque de passer très bientôt et qui permettrait à de grosses sociétés américaines pour la plupart, de déposer des brevets sur toutes les technologies qui font d'Internet et des logiciels ce qu'ils sont. En tant que programmeur, je vomis cette loi qui tuerait définitivement la créativité et l'innovation de notre pays en nouvelles technologies. Breveter un logiciel revient à breveter une suite d'idée et non pas une invention ! Cela est intolérable.

N'oubliez pas non plus la guerre ouverte que les majors et le gouvernement ont déclarée aux réseaux p2p et au piratage, nous grignotant petits a petits certaines libertés sous prétexte de combattre les nazis et autres pédophiles.

Nous n'avons plus de liberté réelle depuis longtemps, ne les laissons pas nous prendre notre cyber-liberté. Celle qui permet à tous de s'exprimer sur un site Internet sans être censuré, celle qui permet d'envoyer des mails sans qu'ils soient lus, celle qui permet de créer toujours de meilleurs logiciels évitant ainsi les monopoles des grosses sociétés, et celle qui nous permet de copier la musique qu'on a achetée pour en faire une copie de sauvegarde. Ne nous laissons pas dévorer.

Pour plus d'informations sur les manigances de notre Etat, et les manœuvres des censeurs, je vous recommande chaudement d'aller consulter le site de la ligue Odebi (www.odebi.org). Plusieurs actions concrètes y sont expliquées pour que vous puissiez vous aussi agir à votre niveau.

2) Mise en bouche

Face à cet enfermement de nos droits élémentaires, je vais au travers de ces quelques pages, vous expliquer comment à votre niveau, vous pouvez vous protéger de Big Brother.
Sachez quand même avant toute chose que vous êtes déjà tous dans l'illégalité. Que celui qui n'a jamais téléchargé de mp3 ou gravé un C.D. m'envoie un mail !! Je le féliciterai en personne !

Les techniques et conseils que je vais vous décrire ci-dessous sont tous sortis de mon petit cerveau. Comme ce document n'est pas exhaustif, il sera mis à jour régulièrement suivant les différentes remarques, les corrections et les techniques que vous m'enverrez.

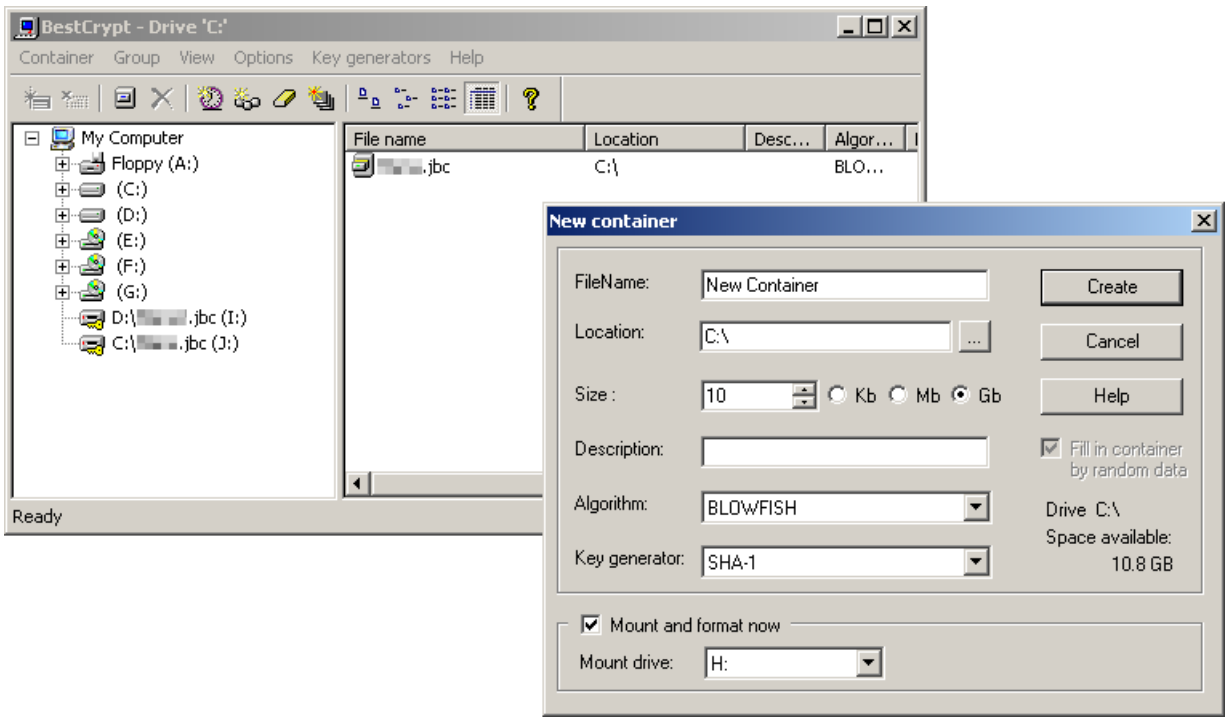
Un des premiers problèmes de l'informatique est la confidentialité de vos fichiers

3) Comment crypter ses fichiers !

Comment protéger des informations confidentielles sur son disque dur ?
Que cela soit des documents top secret ou des mp3 que vous ne souhaitez pas laisser à la disposition de tous, la seule solution envisageable pour vous protéger est le cryptage.

Pour cela, je vous recommande le logiciel BestCrypt (http://www.jetico.com)

Celui-ci va vous permettre de créer un disque crypté virtuel qui ne sera « monté » que lorsque vous aurez tapé le bon mot de passe



Grâce à cela, tous vos documents seront à l'abri d'un piratage ou d'un accès direct a la machine (en cas d'intrusion chez vous)
Note : Pensez à « démonter » les volumes cryptés une fois que vous avez fini de les utiliser. On n'est jamais trop prudent.
Il existe un logiciel de cryptage pour eMule et Kazaa appelé Stegano Secure File qui fonctionne sur le même principe que BestCrypt mais en temps réel pendant les téléchargement. Je l'ai testé. Cela fonctionne mais il y a encore pas mal de bugs.

Le deuxième problème est la censure ou plutôt la surveillance dont vous ferez l'objet si vous devez communiquer des informations "sensibles"

4) Transmettre des informations privées

A cause de la répression actuelle des gouvernements, il faut savoir que votre droit de correspondance privée n'existe pratiquement plus.
Alors comment communiquer par mail sachant que tout ce que vous écrirez sera lu ?

La solution vient une nouvelle fois du cryptage
Je vous propose donc 2 méthodes pour faire passer des messages qui ne pourront être décodés par le premier venu.

I) la méthode classique

Il suffit tout simplement de crypter vos mails avec un logiciel tel que PGP (http://www.pgpi.org), fonctionnant sur un système de clé publique - clé privée.
Le principe est le suivant: Chaque personne avec qui vous devez correspondre doit vous transmettre sa clé publique. Votre destinataire doit quand à lui posséder votre propre clé publique. Quand vous envoyez un mail, vous le cryptez avec la clé publique de votre correspondant et votre clé privée. Il sera ainsi le seul à pouvoir l'ouvrir avec sa clé privée et votre clé publique.
Bien sur, il sera flagrant que vous avez crypté vos messages et un interrogatoire musclé de vous ou de votre destinataire en viendra facilement à bout

II) la méthode vicieuse

toujours sur le même principe du cryptage, sauf que cette fois on y rajoute un élément qui est la stéganographie
(petit topo sur la stegano)
Il est alors très amusant d'inventer différentes procédures de "diffusion d'informations confidentielles"

Scénario 1:
Je dissimule mon message crypté dans une photo ou un mp3 puis, je le mets à disposition de tous sur kazaa ou emule.
Si le fichier est équivoque, comme une photo pornographique (avec un nom qui attire l'œil) ou la dernière chanson de tel ou tel artiste du moment, des centaines de personnes le téléchargeront
Votre fichier sera ainsi impossible à contrôler, et personne ne pourra l'intercepter pour le bloquer
Et seul celui qui aura la clé de décodage et qui saura quel fichier télécharger aura connaissance de son contenu.

Scénario 2:
Même chose que ci dessus avec une photo anodine que vous placerez sur un site Internet
Ni vu ni connu, votre message sera transmis sans attirer l'attention.

Scénario 3:
Inventez un mail publicitaire (Spam) ou mieux, remodifiez en un que vous expédierez avec un mail a usage unique ou de façon anonyme, contenant votre message crypté ou votre photo steganographiée.

Il faut bien sur considérer que tout ce qui est crypté sera "décryptable" un jour ou l'autre. C'est pour cela qu'il est très important de choisir un cryptage "fort" (>128 bits) et une clé ou mot de passe le plus long possible, mélangeant toutes sortes de caractères et de chiffres.

5) Rendre une information publique tout en ne prenant aucun risques et en évitant la censure.

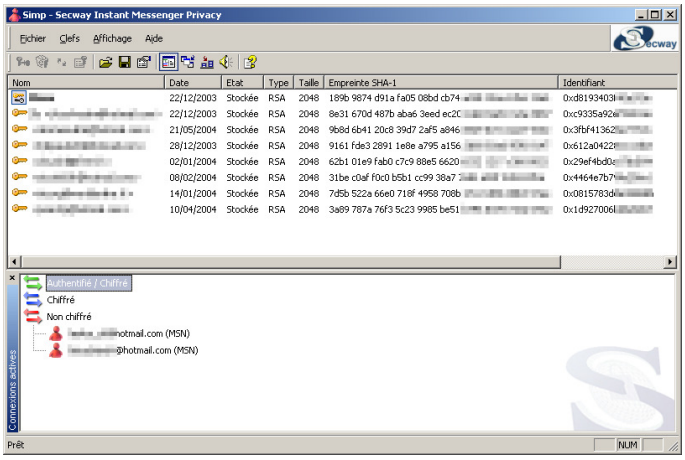
Vous êtes en possession d'une information, d'une technique ou d'un fichier capital qui sera censuré si vous le mettez sur votre site personnel ?
Ne prenez pas le risque. Si vous êtes absolument persuadé que ce que vous possédez doit profiter à la terre entière, même si cela doit nuire à une ou deux entreprises voir même à un gouvernement, mettez tout simplement votre fichier sur les réseaux d'échanges p2p.
Ensuite, de manière anonyme, diffusez le lien sur quelques petits forums de bas étages, laissez les gens le télécharger, supprime le de votre disque dur et attendez. Vous verrez votre information remonter sur d'autre sites et cela se répandra comme une traînée de poudre.

6) Les réseaux d'échanges cryptés

Les réseaux FastTrack (Kazaa) ou eDonkey ne sont pas des réseaux sécurisés. Evitez aussi Bittorrent car son système de tracker « .torrent » permet de retrouver rapidement les releasers (personnes qui sont à l'origine du fichier original)
Des réseaux décentralisés plus ou moins sécurisés commencent a faire leur apparition. Le plus célèbre est Waste (http://sourceforge.net/projects/waste/), un système crypté de p2p fonctionnant sur le principe de communauté dont le père n'est autre que le père de Winamp.
Le programme est open-source, il ne cesse donc de s'améliorer de jour en jour.
les autres clients p2p garantissant une sécurité plus ou moins fiable sont:

- Mute (http://mute-net.sourceforge.net/)
- Freenet (http://www.freenetproject.org/index.php?page=news)
- KDrive (http://www.kdrive.com/)

7) Les messageries instantanées



Il existe pour tout les logiciels de discussion comme ICQ, MSN ou AIM, des modules de cryptage instantané qui vous permettront de discuter avec votre interlocuteur en toute tranquillité vu que le flux qui passera entre vos 2 machines et qui peut facilement sniffé sera crypté.
Utilisant essentiellement MSN, je vous recommande "Simp" de Secway qui vous garantira le cryptage de vos conversations .

Ensuite ne faites confiance à personne
Méfiez vous des questions qu'on vous posera et des réponses que vous donnerez
N'acceptez non plus aucun fichier qu'un inconnu (ou peu connu) voudrait vous envoyer
Il peut s'agir d'un programme parfaitement anodin (comme une animation flash) qui installera un logiciel espion sur votre pc

8) Les indispensables

J'attaque maintenant un chapitre primordial, dans lequel je vais vous montrer les solutions existantes pour vous protéger d'à peu près tout les dangers d'internet.

je vous recommande donc d'utiliser:

- ***un antivirus***

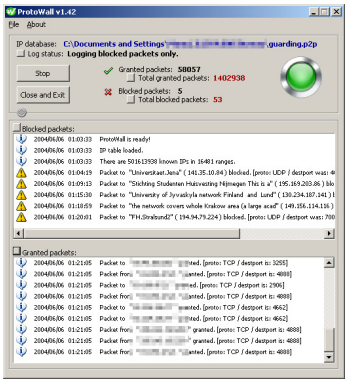
Nul n'est a l'abri d'un virus ou d'un trojan
Le plus souvent, celui ci se diffuse a l'insu de l'expéditeur mais parfois quelqu'un de mal intentionné peut vous envoyer ce genre de petit cadeau pour vous nuire, ou prendre le contrôle de votre machine
Un bon antivirus est donc de rigueur
Personnellement, je vous conseille Kaspersky Antivirus (et vous déconseille Norton ou Mc Affee) (www.kaspersky.com)

Pensez à programmer les mises à jour au moins une fois par jour.
Je vous recommande aussi de faire un scan de votre système de temps en temps avec un antivirus en ligne. Il trouvera peut être des parasites oubliés par votre antivirus local. Je vous recommande le site www.pandasoftware.com/activescan/ de Panda Software.

- ***un firewall***

Un bon firewall vous protégera essentiellement des intrusions mais aussi des "sorties" suspectes
En effet, parfois un programme installé sur votre pc essayera de transmettre des informations vers Internet (vers le site de l'éditeur du logiciel par exemple, Microsoft est friand de ce genre de procédé)
Certains firewalls surveillent aussi la version des logiciels qu'il filtre et vous informera en cas de modification de celui-ci (lors d'une mise a jour si c'est volontaire, ou d'une infection si quelqu'un a remplacé un de vos programme par un autre de son cru)
Je vous conseille Kerio Personnal Firewall (http://www.kerio.com/) qui utilise très peu de ressource tout en étant très efficace.

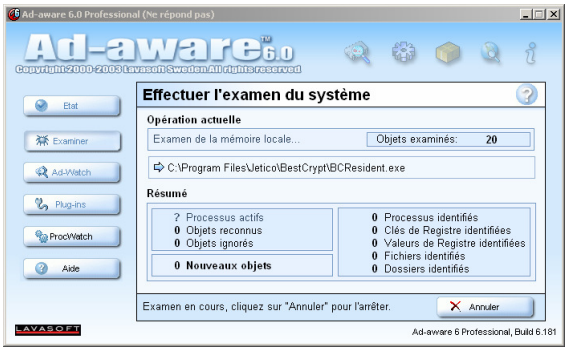
- Un filtre d'IP



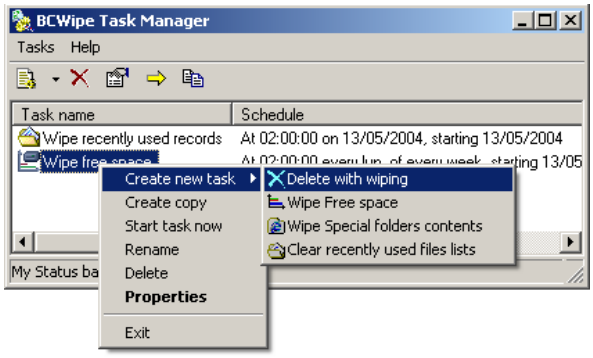
Protowall (http://www.bluetack.co.uk/pwhelp/) fonctionne un peu comme un firewall mais celui-ci filtre les connexions en se basant sur une base d'IP "interdites" telles que celles de la RIAA ou organismes de même acabit. Il est le complément indispensable à un bon firewall. Idéal si vous utilisez des logiciels d'échanges p2p. Je vous recommande Protowall. Pensez a mettre la liste d'IP régulièrement à jour.

- ***Un anti-spyware***

De nombreux logiciels et sites web vous espionnent ou vous bombardent de publicités sans que vous ne l'ayez voulu. Qui ne s'est jamais retrouvé avec un moteur de recherche roumain comme page de démarrage et des dizaines de popup (petites fenêtres) publicitaires impossibles à enlever ?
Ajouter a cela quelques cookies mal faisant et des plug-ins Internet explorer comme Hotbar ou Gator et votre pc n'en pourra plus. Pour se débarrasser de tout Cela, il faut vous munir d'un anti-spyware. Celui ci scannera votre système et délogera les intrus. Je vous conseille Ad-aware (la version freeware) (http://www.lavasoftusa.com/)



- ***Un destructeur de fichiers***



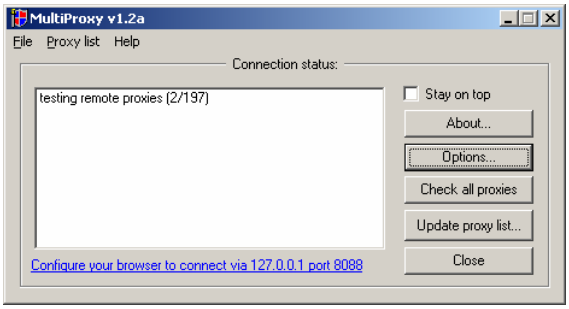
Quand vous supprimez un fichier de votre disque dur, celui ci n'est pas réellement effacé et peut être rapidement récupéré avec un logiciel comme easy recovery d'Ontrack. (www.ontrack.com)

Pour éviter ce genre de petit soucis et vous débarrasser efficacement de vos documents personnels, je vous recommande d'utiliser un shredder comme Bcwipe (fournit avec Bestcrypt). Celui ci supprimera vos fichiers en cryptant plusieurs fois de façon aléatoire son "résidu" empêchant ainsi toute récupération . (http://www.jetico.com)

- ***un "cleaner" de traces***

Lorsque vous surfez, ou que vous utilisez Word ou Excel, des traces sont enregistré sur votre ordinateur comme les derniers fichiers ouverts ou l'historique des sites consultés. Il existe de très Bons "nettoyeurs", et en installer un ne vous fera pas de mal. Je vous recommande «Internet Cleaner » (http://www.softneoweb.com/), qui est payant mais très complet.

- ***logiciel multi-proxy***



Chaque fois que vous surfez sur le net, le serveur sur lequel vous vous promenez apprend un nombre considérable de Choses sur Vous dont Votre IP. (site de la CNIL)
Passer par des Proxys anonymes successifs vous assurent une certaine sécurité. Un Proxy est un serveur qui jouera le rôle d'intermédiaire entre vous et le site web que vous consultez. Ainsi les serveurs ne connaissent plus votre identité (IP) réelle.

Je vous conseille le très bon stegano anonymiser qui vous baladera selon vos réglages de Proxys en Proxys semant ainsi la confusion chez les personnes qui voudraient vous tracer. Il existe aussi un logiciel qui se nomme Multi Proxy dont les listes de Proxys sont régulièrement mises a jour ici http://www.multiproxy.org

- ***email crypté ou a l'étranger***

Se créer une adresse email sur un webmail à l'étranger (hors usa et Europe) vous mettra hors de porté des lois liberticides qui violent votre correspondance privées . je vous recommande Mail.ru, entièrement en russe mais extrêmement sympathique. (version en anglais ici: http://eng.mail.ru)

Sinon, je vous recommande aussi d'utiliser un email crypté comme le Célèbre Hushmail (le seul du genre je crois) (http://www.hushmail.com)

9) quelques recommandations avant de vous quitter

- Ne gravez plus
  Il n'y a plus aucun avantage a stocker des tonnes de CD gravés contenant des mp3 ou des DivX. Cela peut vous coûter cher si un jour vous avez des ennuis avec la justice mais aussi, cela coûte cher en cd vierges. Considérez plus votre ordinateur comme une radio ou un télévision plutôt qu'une usine à contrefaçons.

- Ne vous vantez pas de choses plus ou moins illégales et surtout, NE VENDEZ JAMAIS un cd, même pour dépanner quelqu'un. La justice est aveugle et à besoin de "faire des exemples". Donc méfiance...

- Utilisez des pseudos (ou nickname)
  « Bah oui j'ai pas compris, j'avais mis mon numéro de téléphone et mon vrai nom dans la case "pseudo" de Kazaa et me voilà en prison :-) »

- Utilisez des connexions publiques (Wifi par exemple) Quelle invention géniale ! c'est gratuit, haut débit et anonyme !

- N'enregistrez pas vos mots de passe par exemple avec Internet explorer. N'importe qui utilisant votre pc aura ainsi accès a vos emails..

- Pensez a mettre un mot de passe efficace à votre ordinateur et bloquez votre cession lorsque vous vous absenterez.

- Webmasters: décentralisez vos sites, vos fichiers et vos emails a l'étranger en vous offrant ces services dans des pays assez peu coopératifs avec votre pays d'origine comme la chine, ou les pays de l'est (hors Europe de préférence)
  Si vous devez mettre a disposition des fichiers, n'ayez plus le réflexe FTP mais plutôt le réflexe eMule ou Bittorrent. C'est beaucoup plus pratique, et cela ne vous coûtera plus rien en espace web

- Lisez les news, tenez vous en permanence au courant de l'actualité ayant un rapport avec les nouvelles technologies (législation, sécurité, nouveaux moyen de communications...etc.), c'est un bon moyen d'avoir une longueur d'avance sur tout le monde (news google)

- Devenez parano ;-) On n'est jamais trop prudent !

- Et pour finir, ne restez pas les bras croisés, et aidez la communauté du net a garder sa liberté (si vous programmez, faites le pour la gloire et la satisfaction d'apporter votre pierre a l'édifice, faites le pour que chacun puisse conserver ses libertés individuelles et pour qu'Internet reste un lieu de liberté d'expression et d'échange plutôt qu'un terrain de profit pour majors ou politiciens.

9) Conclusion

J'espère que ce petit tour d'horizon vous aura servi.
Ce texte est totalement libre, vous pouvez le citer partiellement et complètement où bon vous chante.
Vous pouvez même appuyer sur DEL une fois que vous l'aurez lu ;-)
Sachez toutefois qu'à l'heure actuelle, Internet tel que nous le connaissons est réellement menacé par des gens sans scrupules qui vous traqueront et vous attaqueront sans pitié si vous vous écartez du rang.
Il faut combattre ces politiciens et ces lobbys de grosses entreprises qui veulent prendre le contrôle d'Internet et nous priver de nos droits.
Les médias traditionnels (journaux, télévision) font l'impasse sur ces problèmes, et c'est comme cela que des lois liberticides sont votées chaque jours sans que nous nous en doutions une seule seconde.
N'abandonnez pas, continuez de vous battre, chacun a votre niveau pour sauvegarder cet espace de liberté.

Je vous remercie d'avoir consacré un peu de temps a la lecture de ce document. Si vous désirez y apporter des modifications, des corrections et surtout des ajouts sur des thèmes que j'aurais omis, je me tiens a votre disposition par mail (korben_@mail.ru) si vous voulez participer a l'écriture de ce texte.

La version mise à jour sera consultable sur mon site : http://www.korben.tk

Merci

Korben