INFORMATIQUE

I.LA SECURITE INFORMATIQUE

1. Assurer la protection de son pc : le pare feu (firewall)

Le pare-feu est un système permettant de protéger un ordinateur ou un réseau d'ordinateurs des intrusions provenant d'un réseau tiers.
Il permet de filtrer les paquets de données échangées avec le réseau.

2. Politique de sécurité

Soit on autorise uniquement les communications ayant explicitement autorisées. (Tout ce qui n'est pas explicitement autorisé est interdit) ou soit on empêche les échanges qui ont été explicitement interdits. La première méthode est la plus sûre.

3. Assurer la protection contre les virus

C'est un logiciel malveillant écrit dans le but de se dupliquer sur d'autres ordinateurs. Il peut nuire ou perturber le PC. Il peut se répandre à travers tout moyen d'échange de données numériques comme l'Internet, mais aussi les disquettes, les Cd Roms, et les clés USB.

Les différents types de virus :

- Les TSR (Terminate & Stay Resident) ou virus d'application
- Les vers (worms) ou virus réseaux
- Les chevaux de Troie (Trojan Horses) ou troyens

Comment en guérir?

L'antivirus est composé :

- D'un scanner
- D'un gardien (c'est le plus important)
- D'un module de mise à jour

L'antivirus scanne ou surveille les fichiers de l'utilisateur et s'il détecte une signature de virus connue alors il peut en fonction de la stratégie de l'utilisateur :

- Désinfecter
- Mettre en quarantaine
- Supprimer le fichier (Cette action peut détruire des fichiers contenant des informations très importantes).

Prévention et prudence

Lors de la réception d'un e-mail contenant un fichier en pièce jointe : il faut se poser la question
➔ Est-ce que je connais l'expéditeur ?
Si c'est le cas, le contenu du mail lui-même me permet-il d'être sûre que c'est bien lui qui a rédigé ce courrier.
Il faut faire une analyse de la pièce jointe à l'aide du scanner.

4. Assurer la protection contre les mouchards (spywares)

Bien qu'à première vue anodine, le marché de la publicité sur Internet représente des sommes colossales qui expliquent cet acharnement à proposer aux annonceurs des services adaptés. La fin justifiant les moyens, les sociétés éditrices de spywares n'hésitent pas à sacrifier la vie privée et la confidentialité des données des internautes sur l'autel du profit.

Les spywares ont pour but l'espionnage, de récolter un maximum d'informations et les envoyer vers un serveur où elles seront compilées et traitées.

Le spyware se charge en mémoire vive au démarrage du PC et rapporte les moindres faits et gestes de l'internaute à son centre de manière totalement invisible pour celui-ci.

Les différents types de spyware :

- Les BHO (Browser Helper Objects)
- Les Hijackers
- Les cookies (Il existe une politique de gestion des cookies)

Lutter contre les spywares :

Spybot-Search-and-Destroy

5.Se préserver des nuisances

Les pourriels ou les spams :

C'est un courrier électronique non sollicité ou indésirable.
Il ne représente pas réellement de danger mais ils ont une nuisance qui prend de plus en plus d'ampleur chaque jour.
C'est un courrier envoyé à l'utilisateur sans son consentement. Dans la majorité des cas, il a un but promotionnel ou publicitaire.
Les spanneurs utilisent des robots qui scannent les pages web et recensent toutes les adresses électroniques aléatoires, puis vérifier celles qui sont valides.

Les canulars :

C'est une fausse information ou rumeurs. C'est une forme particulière de spams puisqu'il se base sur le courrier électronique. Il utilise la crédulité des utilisateurs pour se propager, en faisant circuler des informations qui apparaissent à l'utilisateur comme essentielles.
Pour vérifier, si c'est un canular ou pas ➔ Hoaxbuster sur Google
Exemple : la fausse chaîne de solidarité

Stop aux canulars !
Conséquences :

- Désinformation : le moyen de diffusion que représente Internet
- Il engorge les réseaux et les boîtes aux lettres

Vérifier l'information sur www.hoaxbuster.com avant de l'envoyer.

II.UN RESEAU SANS FIL

Un réseau sans fil (en anglais wireless network) est un réseau dans lequel au moins deux terminaux peuvent communiquer sans liaison.

Ils sont basés sur une liaison utilisant des ondes radio-électriques en lieu et place des câbles habituels.

Il existe plusieurs technologies se distinguant par la fréquence d'émission.

Il y a des réseaux sans fil qui permettent de relier très facilement des équipements distants d'une dizaine de mètre à quelque kilomètre.

L'installation de tel réseau ne demande pas de lourds aménagements.

Le problème numéro un, c'est que les ondes hertziennes sont difficiles à confiner dans une surface géographique restreinte. Donc les pirates ont facilement accès à ce réseau.

Les catégories de réseaux sans fils :

- GSM, GPRS, 3G pour le téléphone
- WIMAX (Norme mise en place pour palier certains endroits en France qui ne capte pas l'ADSL)
- La WIFI
- Le Bluetooth

1.Présentation de la WIFI

La norme de la WIFI est 802.11.
WIFI = Wireless Fidelity

Il est possible de créer des réseaux locaux sans fil à haut débit pour peu que l'ordinateur à connecter ne soit pas trop distant par rapport au point d'accès.

Il permet de relier des ordinateurs portables, des ordinateurs de bureau, des assistants personnels (PDA) ou tout type de périphérique à une liaison haut débit sur un rayon de plusieurs dizaine de mètre en intérieur.

Les opérateurs commencent à mettre des bornes un peu partout (gare, aéroport, trains). Ces zones sont appelées « hot spots ».

Les différentes normes WIFI :

- IEEE 802.11 est la norme initiale offrant des débits de un ou deux Mbps.
- Norme 802.11a, 802.11b, et 802.11g (révision apportée à la norme originale)

2.Portées et haut débits

Les normes physiques 802.11a, 802.11b, 802.11g correspondent à des révisions du standard 802.11 et proposent des modes de fonctionnement, permettant d'obtenir différents débits en fonction de la portée.

Standard	Bande de fréquence	Débits	Portée (en mètre)
802.11a	5 GHz	54 Mbit/s	10
802.11b	2.4 GHz	11Mbit/s	100
802.11g	2.4 GHz	54 Mbit/s	100

3. Le manque de sécurité

Les ondes radio-électriques ont une grande capacité à se propager dans toutes les directions avec une portée relativement grande. Il est difficile d'arriver à confiner les émissions d'ondes radio dans un

périmètre restreint.

La propagation des ondes radios doit également être pensé en trois dimensions. Ainsi les ondes se propagent d'un étage à un autre.

La principale conséquence de cette « propagation sauvage » des ondes radios est la facilité que peut avoir une personne non autorisée d'écouter le réseau, en dehors de l'enceinte du bâtiment où les réseaux sans fils sont déployés.

Là où le bat blesse, c'est qu'un réseau sans fil peu très bien être installé dans une entreprise sans que le service informatique ne soit au courant.

4. War-driving

C'est le fait d'écouter des réseaux sans fil.

C'est une pratique venue des EU. Elle consiste à circuler dans la ville avec une ordinateur portable équipé d'un carte réseau sans fil à la recherche de réseaux sans fil (netstumbler). On peut le coupler avec une GPS.

Les cartes établies permettent ainsi de mettre en évidence les réseaux sans fil déployés non sécurisés.

Quelques définitions :

- War chalking : c'est mettre des sigles sur les trottoirs ➔réseau ouvert connecté
  ➔réseau ouvert
  ➔réseau sécurisé

- Le réseau WPA : c'est le réseaux le moins sécurisé
- Le réseau WEP : c'est le réseau le plus sécurisé

5.Les risques en matière de sécurité

- Interception de données : écouter les transmissions
- Détournement de connexion
- Brouillage des transmissions : émet des signaux de radio de telle manière à produire des interférences.
- Dénis de service : réseaux inutilisables envoyant des commandes factices

6. l'interception des données

C'est le fait d'écouter un réseau.

7. L'intrusion réseau

Lorsqu'un point d'accès est installé sur le réseau local, il permet aux stations d'accéder aux réseaux filaires et éventuellement à Internet, si le réseau local est localisé.

Un réseau sans fil présente une aubaine pour le pirate dans le but de mener des attaques sur Internet. Le responsable du réseau peut en être tenu responsable.

8. Le brouillage radio

Les ondes radio sont très sensibles aux interférences, c'est la raison pour laquelle un signal peut être facilement brouillé par une émission radio ayant été proche de celle utilisée.

9. Le dénis de service

Une fois la connexion établit, une station doit s'associer à un point d'accès afin de pouvoir lui envoyer des paquets. Ainsi, les méthodes d'accès au réseau et d'association étant connue, il est facile pour un pirate d'envoyer des paquets demandant la désassociation de la station.

Éviter les valeurs par défaut

Un grand nombre d'administrateur en herbe considèrent qu'à partir du moment où le réseau fonctionne, il est inutile de modifier la configuration du point d'accès.

Il faut modifier le nom du réseau par défauts et désactiver la diffusion de ce dernier sur le réseau.

C'est important parce qu'il peut donner aux pirates des éléments d'information sur la marque ou le modèle du point d'accès.

10. Le filtrage des adresses MAC

Chaque adaptateur réseau possède une adresse physique qui lui est propre. Cette adresse est représentée par douze chiffres hexadécimaux groupés par paire et séparés par des tirets.

11.WEP : Wired Equivalent Privacy

Pour remédier aux problèmes de confidentialité des échanges sur les réseaux sans fil.

12. Présentation de la technologie Bluetooth

C'est une technologie de réseau sans fil (noté WPAN pour Wireless Personnal Area Network), c'est-à-dire une technologie de réseaux sans fil d'un faible portée permettant de relier des appareils entre eux sans liaison filaire.

Objectif : transmettre des données ou de la voix

La technologie Bluetooth a d'abord été créé pour les imprimantes, les téléphones portables. Elle a été mise en place en 1994 par Ericsson. Bluetooth veut dire en français « dent bleue ». Sa caractéristique principale et importante c'est son débit (un Méga).

III. DETECTER UN COMPORTEMENT ANORMAL DE SA MACHINE

1. Détecter un comportement anormal : comportement de la machine ou des périphériques

Il faut juger l'activité du disque avec les diodes. Le fonctionnement interne du micro-ordinateur est généralement et intentionnellement caché à l'utilisateur.

Cependant, il existe plusieurs moyens de se faire une idée de l'activité de ses principaux organes vitaux :

- Le temps de réponse de l'ordinateur aux sollicitations de l'utilisateur permet de savoir si celui-ci est plutôt libre ou croule sous les opérations à effectuer.

- Dès lors il peut, grâce à ces indices et ces relevés, juger de l'activité de sa machine, l'utilisateur peut se demander si cette activité est réellement justifiée, compte tenu des opérations qu'il est entrain de réaliser.

2. Réplication des vers ou des virus

Le comportement anormal typique voit l'ordinateur soudainement débordé et incapable de répondre aux commandes de l'utilisateur : on dit qu'il rame.

Il n'y a qu'une seule raison qui peut amener l'ordinateur à cet état : la gestion ou le lancement simultané de plusieurs applications ou d'une seule application « gourmande en ressources ».

Les conséquences sont une surcharge temporaire du processeur allant de pair avec une activité intense des disques durs.

Ce phénomène outre la perte d'interactivité avec le système d'exploitation est facilement identifiable.

La diode rouge sur le boîtier dédiée au disque dur rend compte de l'activité de celui-ci. Un clignotement rapide signifie une forte activité. Généralement le bruit du disque dure permet également d'identifier un régime élevé.

Ensuite, le gestionnaire des tâches du système d'exploitation permet d'apprécier en temps réel l'utilisation du processeur.

Le gestionnaire des tâches du système d'exploitation permet de connaître en temps réel la liste des processus actifs du système et le temps de calcul qu'il nécessite. Il est donc aisé de repérer des processus à l'origine de ce ralentissement soudain et de les identifier.

Lorsqu'une tâche qui monopolise le processeur possède un nom étrange, il peut s'agir d'un vers ou d'un virus. Le site http://www.processlibrary.com/ tient à jour la liste exhaustive de tous les processus de Windows et permet de lever rapidement le moindre doute.

Remarque :

De manière générale, et si les symptômes ne se font pas ressentir, la présence d'un virus actif dans l'ordinateur va se traduire par la présence d'un processus associé. Tuer le processus empêche le virus d'opérer mais celui-ci se relancera automatiquement au prochain démarrage, tant qu'il n'aura pas été éradiqué par un logiciel de désinfection.

3.Propagation des vers et des virus

Un autre comportement anormal est l'accès inexplicable au ressource externe. Le plus facilement repérable est le lecteur disquette pour son bruit peu discret.

Enfin, un 3e comportement anormal est le ralentissement du réseau et plus spécifiquement de la connexion Internet.

Remarque :

Si le virus tente d'infecter les disques amovibles et de se propager sur d'autre machine par le

réseau ou par Internet, il est fort probable que le disque dur de l'ordinateur soit totalement infecté.

IV. COMPRESSION : PRINCIPE

1.Compresser / décompresser ses données

Définitions :

Compresser

C'est l'action de réduire la taille d'un fichier en modifiant le codage de l'information. Après la compression, le fichier est donc plus lisible par le logiciel qui a servit à le créer et il change d'extension avant de pouvoir le réutiliser, il faut le décompresser c'est-à-dire lui faire reprendre sa taille et son codage d'origine de façon à reconstruite l'information initiale.
Compression avec perte : mp3,format d'image Jpg

Codec

Abréviation de compresseur/décompresseur. Élément logiciel ou matériel permettant de compresser ou de décompresser des données multimédias numériques.

Pourquoi a-t-on besoin de compresser des données ?

Le besoin de compression apparaît là où la taille du fichier est à caractère critique.

Lors de l'envoi de courrier électronique les fournisseurs d'accès limitent la taille du fichier attachés pour éviter d'encombrer les boîtes aux lettres. La compression permettra de réduire la taille de vos fichiers et donc de pouvoir les envoyer.

La création d'image numérique est très coûteuse en mémoire car pour avoir une image de bonne qualité il faut qu'elle ait une définition importante et une palette de couleur assez grande. Le problème est identique pour les fichiers vidéos ou sonores.

Donc la plupart des formats d'enregistrement des fichiers numériques multimédias sont des formats utilisant la compression.

Film: avi divx MPEG

Lors de la sauvegarde sur un support externe, il est très utile de pouvoir réduire la taille totale des données à sauvegarder afin de gagner en place et temps de sauvegarde.

2.Compresser et décompresser un fichier et/ou un répertoire

Définitions:

Archive : c'est un fichier souvent compressé qui comporte plusieurs autres fichiers et/ou répertoires.

Archiver : signifie que l'on regroupe dans un seul fichier un ensemble de fichier et/ou de répertoires. Lorsque vous ajoutez un répertoire à une archive les fichiers et les sous répertoires qu'il contient sont également ajoutés.

3. Formats de compression

Les divers formats de compression (zip, rar, gzip, tar…)

Définitions

Ces formats de compression utilisent une compression physique sans perte d'information car le but de ces formats de compression est simplement de réduire la taille de l'ensemble des fichiers.

Compression physique

La compression physique agit sur le fichier, sans savoir quel type de données elle manipule. De plus, elle est sans perte d'information.

Compression sans perte

La compression sans perte d'information assure que les données une fois décompressée sera identique à l'originale ayant servi à la compression.

Il existe plusieurs formats de compression, parmi les plus connus : ZIP, et le format RAR qui se veut plus puissant. Tous les formats de compression physique sans perte sont néanmoins basés sur le même principe.

4.La compression des images des sons et des vidéos

Définitions:

La plupart des formats images, sons et vidéos utilisent une compression logique avec une perte d'informations.

Compression logique :

La compression logique utilise un algorithme (procédé) qui agit sur les données de manière spécifique.

En fonction du réglage de l'algorithme, la compression peut se faire avec ou sans perte d'information. Lors de la compression avec perte la donnée reconstruite sera plus ou moins proche de la donnée originale en fonction du taux de compression utilisé. Mais il n'est pas évident qu'une personne puisse faire la différence.

Les formats d'image :

-BMP : fichier bitmap, pas compressé.
-GIF : (Graphic Interchange Format)
-JPEG : Joint Picture Expert Group, compressé permet d'avoir des images de très bonne qualité avec un bon niveau de compression.
-PNG : Portable Network Graphics est un format de fichier graphique.

Les formats audio:

- WAV équivalent audio du format Bitmap est l'équivalent audio du BITMAP. Il reprend le principe de la compression minimale. C'est un format non compressé
- MP3 « MPEG Audio Layer 3 » est un format de compression des données audio par filtrage des données audio. Pour les fichiers musicaux plus longs

Le format mp3 n'est pas illégal car il représente uniquement une façon de compresser des données numériques. Par contre, son utilisation peut l'être, il faut respecter les droits d'auteur. Le principe d'exception de copie privée prévoit qu'il est possible de posséder une copie numériques d'une ouvre musicale a condition que l'on possède l'original.
Attention : les œuvres numérisées sont réservées à un usage privé (cercle familial ou d'amis). La diffusion de ces fichiers en dehors de ce cadre est strictement interdite.

Les formats vidéos:

- AVI
- MPG, MPEG 2 format qui compresse un peu comme ipeg , MPEG4
- DIVX format compressé

Tous ces fichiers sont compressés.

Remarque :

Pour comprendre la compression d'image, il faut d'abord savoir comment est codée une image : une image est constituée d'un ensemble de points appelés pixels (pixel est une contraction de PICTURE ELEMENT)

V. LOGICIELS

1.Logiciel libre

Il ne faut pas confondre les logiciels libres avec les logiciels gratuits (freewares), ni avec les sharewares, ni avec des logiciels tombés dans le domaine public. La notion de logiciel Open Source établie par l'Open Source Initiative est en revanche très proche de celle de logiciel libre.

2.Freeware

Un graticiel ou gratuiciel est un logiciel qui est mis gratuitement à disposition par son créateur, mais qui est soumis à certaines contraintes quant à sa diffusion. Les gratuiciels sont soit des logiciels complets, soit des logiciels commerciaux qui sont diffusés de manière bridée en terme de fonctionnalités (version réduite). Ils sont parfois financés par la publicité qu'ils contiennent (Adware).

3.Shareware

Un partagiciel ou shareware est un logiciel propriétaire protégé par le droit d'auteur, dont l'usage peut être limité dans le temps ou dans les fonctionnalités, à moins d'en rétribuer l'auteur.

4.Domaine public

En droit de la propriété intellectuelle, le domaine public est un statut sous lequel sont placées les biens intellectuelles (œuvre, invention…) pour lesquelles, au terme de leur durée de protection, il n'est plus nécessaire de demander une autorisation d'exploitation quelconque.
On dit alors qu'ils sont « tombés dans le domaine public »

5.Open source

Le terme open source correspond à une licence de logiciel obéissant à une définition très précise établit par l'open source initiative, dont voici les principaux critères nécessaires:
-La libre redistribution
-Un code source disponible
-Les travaux dérivés possibles

Le fait de disposer les sources d'un logiciel ne suffit pas a dire qu'il est open source. Dans tous les cas, on se référera à la licence d'utilisation du logiciel.

6.Logiciel libre

Pour être qualifié de logiciel libre, un logiciel doit être disponible sous une licence répondant à des critères strictes. La free software Foundation et le projet DEBIAN étudient avec soin chaque licence pour déterminer si elle est libre.

La Free Software Foundation maintient une définition du logiciel libre basée sur quatre libertés:

Liberté 0 : La liberté d'exécuter le programme pour tous les usages
1 La liberté d'étudier le fonctionnement du programme
2 La liberté de redistribuer les copies
3 La liberté d'améliorer le programme et de publier ses améliorations.

7.Qualités des logiciels libres

Inconvénients et limitations des logiciels libres : on identifie plus facilement les failles, problème de sécurité du logiciel (libre accès) .
On accès a la source fait qu'on arrive a voir plus facilement les failles.

8.Linus

Ou GNU/ linux est un système d'exploitation libre, multitâche, multi plate forme et multi-utilisateur de type Unix.

Il tire son nom d'une de ses parties, à savoir de son noyau, initié par Linus TORVALDS en 1991. Il s'agit d'un composant central et de bas niveau (composant qui va passer avant tout) qui s'occupe de fournir aux logiciels une interface pour communiquer entre eux et avec le matériel.

Pour l'utilisateur final, GNU/linux se présente sous la forme d'une distribution Linux, commercial ou non c'est-à-dire d'une solution prête a être installée comprenant une sélection complète est cohérente de logiciels, des programmes d'installations et d'administrations de

l’ordinateur, ainsi qu’un mécanisme facilitant l’installation et la mise à jour des logiciels.

Linux est aujourd'hui utilisé sur de nombreuses plate formes, du plus puissant super ordinateur aux systèmes embarqués tels que les téléphones portables, lecteur vidéo Divx en passant par les ordinateurs personnels, PC et Mac sur lesquelles il peut être installé seul ou en parallèle avec Microsoft Windows ou Mac OS.

Linux s'est d'abord imposé dans le domaine des serveurs informatiques grâce à des logiciels tels que le serveur Web Apache ou le serveur de fichier Samba. Qui permet de partager des fichiers avec un réseau d'ordinateurs sous microsoft Windows.

Il a également atteint depuis peu une certaine maturité sur le poste de travail grâce aux interfaces conviviales que représentent GNOME et KDE ainsi qu'au succès de logiciel comme la suite bureautique OPEN office.org ou le navigateur internet Mozilla Firefox

La mascotte de Linux est un manchot qui a pour nom Tux.

Gnu, l'acronyme de GNU's Not Unix est le nom du système complet de logiciels compatible Unix qui est écrit pour pouvoir le donner librement à tous ceux qui en auraient besoin. De nombreux bénévoles aident en contribution en temps, en argent, en logiciels et en matériel.

Les logiciels du projet GNU et le noyau Linux forment la base d'un système d'exploitation depuis complété par les apports de nombreuses communautés du logiciel libre :
Mozilla Firefox
openoffice. Org

C'est la principale originalité de Linux par rapport à d'autres systèmes d'exploitation concurrents comme Microsoft Windows, MAC os, ou les autres Unix.

Un logiciel libre n'est pas nécessairement un logiciel gratuit, et inversement tout logiciel non commercial n'est pas forcément libre. Ce ne sont pas non plus des logiciels libres de droits.

Certaines licences sont basées sur le principe de copyleft, c'est a dire de réciprocité : une œuvre dérivée d'un logiciel sous copyleft doit à son tour être libre. C'est le cas de la licence libre la plus utilisée, à commencer par le noyau Linux lui même:

9.Interopérabilité

les logiciels sont libres cela permet d'avoir des standards.

10.Communautés

De nombreuses associations, connues sous le nom de Linux Users Group, groupe d'utilisateurs Linux, cherchent à promouvoir Linux et par extension, les logiciels libres, par le biais des rencontres ou des démonstrations de Linux sont faites, des formations, et pour ceux qui le souhaitent des installations sur leur ordinateur.
De nombreuses communautés existent sur Internet afin d'aider les débutants et le professionnels.

11.Les distributions Linux

red hat
suse
ubuntu
mandriva
debian

La distribution Linux est une solution prête à être installée par l'utilisateur final comprenant un noyau Linus, des programmes d'installations et d'administration de l'ordinateur, un mécanisme facilitant l'installation et la mise à jour des logiciels comme RPM ou dpkg ainsi qu'une sélection de logiciels produits par d'autres.

12.Choisir une distribution

La diversité des distributions permet de répondre à des besoins divers :
-à but commercial ou non
-orienté serveur, bureautique ou embarqué
-orienté grand public ou public averti
-généraliste ou spécialisée pour un usage spécifique
-d'autres sont certifiés sur un matériel donné (par exemple telle gamme de portable HP)

13.Live Cd

dont la plus célèbre est Knoppix :démarrer un système a partir du Cd sans installation préalable sur le disque dur et sans altérer son contenu. Support très populaire

14. Succès de Linux:

- tout le monde utilise Linux sans le savoir
-apprécié pour sa fiabilité, sa résistance aux attaques des pirates informatiques sur les réseaux

VI.VIE PRIVEE SUR INTERNET

Avec l'avènement des blogs et des réseaux sociaux, internet emmagasine toujours plus de données privées sur chacun.

Aujourd'hui, on peut être vu, entendu, et même suivi avec la géolocalisation, à notre insu. C'est une atteinte a la liberté d'expression et de circulation.

Selon une étude publié en aout 2009, près de la moitié des employeurs questionnent le web pour trouver des informations sur les candidats à l'embauche.

Plus d'un tiers des recruteurs avouent avoir éliminé des candidats à cause de photographies ou de propos « déplacés » dénichés sur la toile.

1.Fans de Facebook: vie privée et Internet,est-ce compatible?

C'est le numéro un des réseaux sociaux en ligne en France. Dans le monde, il compte 175 millions de membres.

Mais s'il fait couler autant d'encre, c'est pas seulement pour son audience
-il dépasse régulièrement les bornes en matière d'utilisation des données personnelles de ses membres.
-face à la croissance fulgurante du site, ses couts de fonctionnement grimpent aussi
fort d'un réseau de 175 millions d'utilisateurs, le site cherche à tirer profit tous azimuts des quantités d'informations personnelles que ces derniers livrent et échangent.

-voila la vraie richesse du site car ces informations représentent une manne considérable pour les publicitaires qui peuvent ainsi s'adresser personnellement à leurs cibles selon leurs centres d'intérêts, leurs ages, les gens et lieux qu'ils fréquentent.

Près de 22 millions d'internautes français ont visité un réseau social en décembre 2008 enregistrant un bond de 45% par an.
Il détrône Skyrock

2. La CNIL

CNIL : commission nationale de l'informatique et des libertés est une institution indépendante chargée de veiller au respect de l'identité humaine, de la vie privée et des libertés dans un monde numérique.
Mondialisation des échanges de données, vagues incessantes d'innovations technologiques, exigence de sécurité collective: quelles réponses?
L'actualité de la CNIL et de la protection des données personnelles, en France et dans le monde.
Pour enraciner une culture de l'informatique dans le respect des libertée, la CNIL s'appuie sur de nombreux relais: parlementaires, élus locaux, partenariats, correspondants..

3.la sécurité des fichiers

Les utilisateurs de données personnelles ont des obligations:
-parce qu'un traitement de données personnelles n'est pas un fichier comme les autres
-parce que ca peut concerner la vie privée

Tout responsable de traitement informatique de données personnelles doit adopter des mesures de sécurité physiques (sécurité des locaux), logiques (sécurité des systèmes d'information) et adaptées à la nature des données et aux risques présentés par le traitement.
La non respect de l'obligation de sécurité est sanctionné de 5 ans d'emprisonnement et de 300000 euros d'amende. (art 226-17 code pénal)

4.la confidentialité des données

Seules les personnes autorisées peuvent accéder aux données personnelles contenus dans un fichier. Il s'agit des destinataires explicitement désignés pour en obtenir régulièrement communication et des « tiers autorisés » ayant qualité pour les recevoir de façon ponctuelle et motivée (ex: police, fisc).
La communication d'informations à des personnes non autorisées est punie de 5ans d'emprisonnement et de 300000 euros d'amende.

5.La durée de conservation des informations

Les données personnelles ont une date de péremption.
Le responsable d'un fichier fixe une durée de conservation raisonnable en fonction de l'objectif du fichier
le code pénal sanctionne la conservation des données pour une durée supérieure a celle qui a été déclarée de 5 ans d'emprisonnement et de 300000 euros d'amende.(art 226-20 du code pénal)

6.L'information des personnes

Le responsable d'un fichier doit permettre aux personnes concernées par des informations qu'il détient d'exercer pleinement leurs droits. Pour cela, il doit leur communiquer : son identité, la finalité de son traitement, le caractère obligatoire ou facultatif des réponses; les destinataires de l'information, l'existence des droits; les transmissions envisagées.
Puni 1500 euros par infraction constatée et 3000 en cas de récidive.

7.L'autorisation de la CNIL

les traitements informatiques de données personnelles qui présentent des risques particuliers d'atteinte aux droits et aux libertés doivent, avant leur mise en œuvre, être soumis à l'autorisation de la CNIL.
Le non accomplissement des formalités auprès de la CNIL est sanctionné de 5 ans d'emprisonnement et de 300000 euros d'amende.

8.La finalité des traitements

Un fichier doit avoir un objectif précis.
Les informations exploitées dans un fichier doivent être cohérentes par rapport à son objectif.

9.Hadopi

le terme Hadopi (haute autorité pour la diffusion des œuvres et la protection des droits sur Internet)
la loi « création et internet » ou « hadopi » vise à réprimer le partage d'œuvres culturelles sur Internet. Préparée par le gouvernement français, elle met en œuvre le dispositif de « riposte graduée » à l'issue duquel peut être prononcée une suspension de la connexion Internet des personnes soupçonnées d'actes et de partage.

L'autorité administrative (HADOPI) crée par ce texte agit sur dénonciation d'acteurs privés représentant les industriels du divertissement (syndicats professionnels, enquêteurs privée). Elle est chargée, en se basant sur des preuves sans valeur, d'envoyer des courriers d'accusation menaçant les utilisateurs de sanctions s'ils ne cessent de partager des œuvres culturelles sur Internet. Initialement, le texte prévoit que en cas de récidive, HADOPI puisse prononcer une coupure de la connexion Internet pour une durée allant jusqu'à un an (le paiement de l' abonnement restant à la charge des abonnés sanctionnés pendant cette période).

Le projet de loi Hadopi 2 examiné au cours de l'été 2009 cherche à contourner la censure du conseil constitutionnel en confiant ce pouvoir de sanction à un juge unique, généralisant au passage une procédure judiciaire expéditive et irrespectueuse des droits fondamentaux.