Déontologie, Droit et la bonne utilisation d'Internet

Frédéric Gava (MCF)

gava@univ-paris12.fr

LACL, bâtiment P2 du CMC, bureau 221

Université de Paris XII Val-de-Marne

61 avenue du Général de Gaulle

94010 Créteil cedex

Auteur du texte

- Les textes de ces transparents ne sont pas de moi
- Mais d'un cours de C2i de l'université de Nancy 2 (A. Boyer)
- Ajouts et modifications de quelques éléments par mes soins
- Remise en page et légère re-organisation par mes soins pour la cohérence des cours

Le problème du piratage

Quelques interrogations

- Ai-je le droit de tout faire ?
- Y a t il un vide législatif de l'Internet ?

  (pas de vide juridique)
- Comment puis-je protéger
  - Ma vie privée
  - Mon matériel
- …

Internet sans risque ?

« Plan » général du cours :

- Quelques anecdotes
- Une nuisance : les virus
- Problématique et enjeux de l'Internet
- La réponse par auto ou co régulation
- La réponse juridique

Un exemple célèbre

«le plus important réseau français de contrefacteurs de logiciels, dénommé "étoile noire", démantelé par le service des enquêtes sur les fraudes aux technologies de l'informatique (SEFTI) et BSA»

- Le 22 juin 1999
- 6 mois d'enquêtes et plusieurs perquisitions
- Préjudice estimé à plusieurs millions de francs
- Plaintes de plusieurs éditeurs
- donner accès à un nombre très important de copies illicites
  - Directement via Internet
  - Par des renvois vers des revendeurs de CD ROM piratés

Piratage de logiciels sur Internet

- BSA = Association des principaux éditeurs de logiciels
- Objectif : lutter contre le piratage de logiciels et les copies illicites
  - Traditionnel ou via Internet
  - Atteinte aux droits d'auteurs
- Stratégie :

  1) Information du grand public

  2) Sensibilisation des autorités publiques afin de renforcer les lois protégeant le droit d'auteur

  3) Déclenchement de poursuites à l'encontre des responsables impliqués dans le piratage de logiciels

Et des condamnations ...

- **4 particuliers commercialisant des copies de logiciels sur CD**
  - Tribunal correctionnel de Paris, le 7 mai 1999
  - 3 mois de prison avec sursis
  - Peine d'intérêt général de 100 à 150 heures chacun
  - 65 000 francs d'indemnisation globale
  - Publication dans la presse spécialisée
- **1 étudiant commercialisant des copies de logiciels sur CD**
  - Tribunal correctionnel de Paris, le 22 février 1999
  - 6 mois de prison avec sursis
  - 20000 F d'amende, 50 000 F aux éditeurs de dommages et intérêts
  - Publication dans la presse spécialisée PC direct
  - épouse condamnée à 15 000 F d'amende pour recel de copie
- **1 étudiant pour copie illicite de logiciels sur 11 CD pour son usage**
  - Tribunal correctionnel du Havre, le 8 février 1999
  - 3002 francs de dommages et intérêts aux éditeurs
  - Confiscation de son matériel informatique

Idem dans le domaine musical

- Société Civile des Producteurs de Phonogrammes en France SPPF
- Condamnation d'un internaute récidiviste de 38 ans
  - Le 29 janvier 2004, 31ème chambre du tribunal correctionnel de Paris
- Organisation via son site personnel de vente illicite de CD gravés
  - Reproduisant des fichiers musicaux MP3
  - Téléchargés à partir de sites peer to peer
  - Identification de titres de producteurs indépendants de la SPPF
  - Enquête de la brigade d'enquêtes "fraude aux technologies de l'information"
  - 6 mois de prison ferme
  - 1000 € de dommages et intérêts à la SPPF
  - 300 € au titres 475-1 du code de la procédure pénale
  - Publication du jugement dans Télérama et le Parisien

Les fichiers musicaux

- Condamnation le 2 février 2005
- premier internaute français poursuivi au pénal par les producteurs et les maisons de disques
- contrefaçon pour téléchargement et mise à disposition en P2P
  - 10 000 fichiers musicaux, entre août 2003 et août 2004
- 3.000 euros d'amende avec sursis (annulée au bout de cinq ans) et 10.200 euros de dommages et intérêts

- selon la SPPF : "Les juges ont considéré que les utilisateurs des systèmes [P2P] doivent prendre conscience notamment de la nécessaire protection des droits des auteurs, compositeurs ou producteurs des œuvres de l'esprit«
- *En octobre 2006, l'IFPI (Fédération Internationale de l'Industrie Phonographique) a annoncé engager 8000 nouvelles poursuites contre les internautes échangeant des fichiers musicaux sans autorisation par le système P2P (source : « Le mag BNP-Paribas » février 2007)*

- parties civiles : Société des auteurs, compositeurs et éditeurs de musique, Société civile des producteurs phonographiques, Société civile des producteurs de phonogrammes en France, Société pour l'administration des droits de reproduction mécanique

Lu sur LEMONDE.FR | 30.11.06

« A l'automne 2004, l'industrie du disque, exaspérée par la chute vertigineuse de ses ventes (moins 30 % entre 2001 et 2003), décide de frapper les esprits. Sur les 8 millions de Français adeptes de téléchargements via les réseaux P2P, une cinquantaine sont poursuivis en justice pour l'exemple, dont la moitié d'entre eux au pénal. Mineurs, chômeurs, artisans, cadres… M. Tout-le-Monde peut se retrouver au tribunal pour avoir mis des fichiers musicaux à disposition sur Internet."

- Anne-Sophie Lainnemé, 27 ans
- passible de 3 ans d'emprisonnement et de 300 000 euros d'amende
- refuse de payer pour soutenir un modèle économique obsolète
- condamnée le 30/11/2006 par le tribunal correctionnel de Rennes, à 1 200 euros d'amende avec sursis et à la confiscation de son disque dur pour délit de "contrefaçon de droit d'auteur"
- également condamnée à verser 2 225 euros de dommages et intérêts, à la Société des producteurs de phonogrammes en France (SPPF) et à la Société civile des producteurs phonographiques (SCPP)

Piratage de BD sur Internet *Source : 01 net*

"Pour la première fois, un prévenu à été condamné pour piratage de Bande Dessiné sur Internet. Condamné au printemps 2005, il n'a pas fait appel de sa condamnation à un euro symbolique. L'homme était accusé d'avoir mis en ligne quelques 2288 Bandes Dessinées. "

- Possibilité de 300 000€ d'amende et de 3 ans de prison (art. L335-2 du code de la propriété intellectuelle)
- le syndicat du livre, partie civile, a demandé une condamnation symbolique

Une stratégie similaire

- Information du grand public
  - Catastrophisme
  - Avertissement
- Sensibilisation des autorités publiques
- Renforcement des lois sur le droit d'auteur
- Déclenchement de poursuites
  - Condamnations
  - Publicités

NOUVELOBS.COM | 15.02.04

"Microsoft a annoncé jeudi soir que des extraits du code source de Windows protégés jalousement ont été publiés à son insu sur internet"

- Ouverture par le FBI d'une enquête pour identifier et arrêter l'internaute

- Porte-parole du bureau de la sûreté fédérale (Seattle) :

"cette affaire est confiée à une cellule opérationnelle chargée de combattre la criminalité en informatique. Elle comprend des représentants du FBI, des services du Trésor, des impôts, et de la police locale et de l'Etat de Washington"

Au sujet des enseignes

Le problème ne se pose pas qu'avec le piratage de logiciels ou de fichiers:

FNAC/R.G. et Auslese die Buchhandlung

- Fnac.de : site trilingue (allemand, anglais, français) référencé sur *yahoo.fr* !
- La *Fnac* : titulaire d'une marque française et d'une marque communautaire
- condamnation du libraire allemand
  - *Question de la légalité des actions posée ici. On est toujours à la limite.*

Premier constat

- Ne pas s'approprier le travail ou la propriété d'autrui
- Protéger son travail et ses productions

Les hackers = les pirates

- Admirés pour leur maîtrise de la technologie autonome et indépendante des pouvoirs établis
- Décriés comme « cyberterroristes » ou « cybercriminels » en puissance
- Leur savoir faire et leur façon de faire frappent les imaginations
- Leur credo :
  - partage et liberté de l'information
  - Milite pour "un accès aux ordinateurs illimité et total , sans considération de frontières ou de propriétés, avec comme ambition la connaissance«
- Il n'y a qu'à lire la presse !

Hacker

- Terme souvent utilisé pour désigner un pirate informatique
- En général des jeunes
- Signification depuis son apparition à la fin des années 50 :
  - à l'origine : programmeurs émérites
  - années 70 : révolutionnaires de l'informatique
    - la plupart devenus les fondateurs de grandes entreprises informatiques
  - années 80 : personnes impliquées dans le piratage de jeux vidéos
    - en désamorçant les protections puis en revendant des copies
  - aujourd'hui : personnes s'introduisant dans les systèmes informatiques “sécurisé” et en général (mas pas toujours) sensible

Des pirates …

- **Les white hat hackers**
  - hacker au sens noble du terme
  - But : aider à améliorer les systèmes et technologies informatiques
  - à l'origine de certains protocoles et outils utilisés aujourd'hui ...
- **Les black hat hackers**
  - couramment appelés *pirates* (ou *crackers*)
  - s'introduire dans les systèmes informatiques dans un but nuisible
- **Les Script Kiddies**
  - *gamins du script*
    - surnommés *crashers*, *lamers*, *packet monkeys* (*singes des paquets réseau*)
  - jeunes utilisateurs du réseau utilisant des programmes trouvés sur Internet généralement de façon maladroite pour vandaliser des systèmes informatiques afin de s'amuser

Toujours des pirates !

- **Les phreakers**
  - pirates s'intéressant au réseau téléphonique commuté (RTC)
  - But : l'utiliser gratuitement grâce à des circuits éléctroniques (les *box*)
- **Les carders**
  - s'attaquent principalement aux systèmes de cartes bancaires
    - pour en comprendre le fonctionnement
    - et en exploiter les failles
- **Les crackers**
  - créer des outils logiciels pour
    - attaquer des systèmes informatiques ou
    - casser les protections contre la copie des logiciels payants
- **Les hacktivistes**
  - contraction de *hackers* et *activistes* (*cybermilitant* ou *cyberrésistant*)
  - motivation principalement idéologique
  - terme largement porté par la presse, aimant à véhiculer l'idée d'une communauté parallèle (exagération, mystification et désinformation typique de la presse…)

Un certain militantisme

- Internet Separatist
  - l'Internet relève d'un ordre juridique à part
  - Transcendant les frontières politiques et l'emprise des états nations
- EEF : Electric Frontier Foundation
  - Créée en 1990 par 2 hackers
  - Promouvoir les droits fondamentaux du cyberespace
  - Liberté d'expression et respect des données personnelles par encryptage
  - Participe notamment à l'échec devant le congrès de la loi sur la lutte contre la pornographie sur le net

Kevin Mitnick, le plus célèbre pirate

- Américain d'environ 40 ans, surnom Condor
  - Arrêté par le FBI à Raleigh, Caroline du Nord
  - le 15 février 1995, après une traque de sept ans
  - Grâce à un ancien pirate reconverti dans la sécurité informatique
- On lui attribue
  - vol sur des réseaux privés le numéro de 20 000 cartes de crédit (dont celles des milliardaires de la Silicon Valley)
  - Introduction dans le système du laboratoire de recherche de la NASA à Pasadena (Californie)
  - visite des centaines de fois les ordinateurs du Pentagone à Washington
- Il passe 5 ans en prison
  - pour avoir volé des logiciels, modifié des données chez Motorola, Nokia, Sun ...
  - A l'époque de son procès, accusé d'avoir causé 10 millions de dollars de dégâts en s'en prenant à plusieurs réseaux d'entreprise
  - libéré en 2000 et jusqu'au 21 janvier 2003, interdiction d'utiliser un ordinateur ou d'être consultant ou conseiller dans tout domaine lié à l'informatique

Ehud Tenebaum, le plus discret

- Israélien âgé d'environ 25 ans, surnom l'Analyste
- Entre 1996 et 1998 aurait piraté par jeu plus de 1000 sites sensibles, sans jamais se faire repérer
  - Pentagone, la NASA, le centre américain pour l'armement sous-marin, les archives secrètes de l'armée israélienne, le MIT, le FBI, l'U.S. Air Force et l'U.S. Department of Defense, la Knesset ou encore la Banque d'Israël
  - utilisait les réseaux des universités israéliennes pour se connecter incognito
- En 1998 décide de tout arrêter
  - communique ses programmes et mots de passe à un ami américain
  - L'ami les utilise, se fait arrêter par le FBI pour espionnage (un mot de passe permettait d'accéder à l'un des sites du Pentagone)
  - intervient pour disculper son camarade
    - fournit à un journal israélien des fichiers récupérés dans les ordinateurs du Pentagone
  - Arrêté par la police israélienne le 18 mars 98, relâché après quelques jours
  - effectue son service militaire (enrôlé par le MOSSAD ?)
  - inculpé un an après les faits

Vladimir Levin, auteur du premier e-hold-up

- biochimiste russe de 35 ans environ
- Entre juin et août 94 s'introduit plusieurs fois dans le réseau SWIFT
  - réseau bancaire international pourtant réputé inviolable !
- Assisté de quelques amis pirates
  - perce les coffres-forts électroniques de la Citibank (1ère banque américaine)
  - détourne des fonds vers des comptes en Finlande, Russie, Allemagne, Pays-Bas, Etats-Unis et Israël
  - Montant du butin :
    - plus de 10 millions de dollars selon les autorités judiciaires américaines
    - "seulement" 3,7 millions de dollars selon l'intéressé
- Arrêté par Interpol en mars 1995 à l'aéroport d'Heathrow (Londres)
  - extradé vers les Etats-Unis en septembre 1997
  - jugé en février 1998
  - condamné à 36 mois de prison

Un deuxième constat

- Vol ou effraction sur Internet comme ailleurs
- Ne pas confondre actes délictueux et militantisme

Les escrocs du woueb

Première condamnation en France pour escroquerie par "phishing"

- ZDNet France 27 janvier 2005
- Phishing : usurpation d'identité via un faux site web

"Un internaute (un étudiant) avait détourné 20.000 euros en attirant ses victimes sur un faux site du Crédit lyonnais qu'il avait créé. Il a été condamné à 8.500 euros de dommages et intérêts et un an de prison avec sursis."

- sanction prononcée par le tribunal correctionnel de Strasbourg le 2 septembre 2005 (première condamnation de phishing en France)

Principe

- Obtenir des données personnelles et bancaires
  - grâce à un e-mail factice
  - apparence d'un courrier officiel envoyé par une banque ou un cybermarchand
- repose sur la crédulité
- de moins en moins marginal en France
- environ 1.707 nouveaux faux sites recensés par une organisation américaine (l'APWG) dans le monde en décembre 2004
  - = augmentation de 24% par rapport à juillet 2004

Selon les derniers chiffres publiés par l'association Anti-Phishing Working Group (étude parue dans le Fig. Mag. du 6/01/2007): plus de 28500 attaques de phishing sur le seul mois de juin 2006.

- le plus sûr : respecter des règles simples de prudence
  - ne jamais communiquer de données bancaires en cliquant sur un lien envoyé par e-mail

Protection de la tranquillité : spam

envoi massif et parfois répété, de courriers électroniques non-sollicités à des personnes avec lesquelles l'expéditeur n'a jamais eu de contacts et dont il a capté l'adresse électronique de façon irrégulière

Deux types de spamming

- Avec intention de nuire en produisant un déni de services (mail bombing)
- Marketing indélicat

Les spams: élèments caractéristiques

- des messages adressés sur la base d'une collecte irrégulière de mails
  - *soit au moyen de moteurs de recherche dans les espaces publics de l'internet (sites web, forums de discussion, listes de diffusion, chat...)*
  - *soit cession des adresses sans informer les personnes et sans qu'elles aient été mises en mesure de s'y opposer ou d'y consentir*

- *Le plus souvent,*
  - *pas d'adresse valide d'expédition ou de "reply to"*
  - *adresse de désinscription inexistante ou invalide*

Contre exemples

- *l'envoi de messages par un organisme qui a procédé à une collecte loyale des adresses électroniques*
- *la réception d'une lettre d'information (newsletter) envoyée à partir d'un site sur lequel l'internaute s'est préalablement inscrit*

OUTILS COLLABORATIFS POUR LUTTER CONTRE LE "SPAM"

- A titre d'exemple
  - Spamassassin
  - un logiciel gratuit de lutte contre le spam SpamNet
    - efficacité repose sur le principe de la collaboration de tous les utilisateurs de ce logiciel.
    - Chaque spam est recensé sous une forme codée dans une base de données centralisée
- Pour plus d'information (en anglais) : http://www.spamnet.com.
- Une liste de logiciels également disponible sur http://www.caspam.org/outils_anti_spam.html.

1ère condamnation d'un spammeur français 9/06/2004

- Spam : courrier électronique non sollicité
- L´histoire :
  - société de marketing direct du sud de la France abonnée au fournisseur d´accès AOL
  - créait des e-mails sous une fausse identité chez Hotmail
  - utilisait sa connexion AOL pour envoyer les spams depuis une adresse "hotmail.com"
  - a utilisé de fausses identités pour créer de nouveaux comptes et continuer à envoyer des spams malgré la fermeture contractuelle de son compte AOL pouractes de spamming avérés et constatés
  - à l´origine de plus d´un million de spams
- Association de AOL et Microsoft pour la faire condamner
- Condamnation de l'entrepreneur à 22 000 € de dommage et intérêts
- 1 000 euros pour tout nouveau courrier électronique non sollicité qu´il enverrait en dépit de sa condamnation

Howard Carmack dit "Buffalo Spammer"

- Condamné par la justice américaine à 7 ans de prison
- Envoi de 825 millions de spams en utilisant de fausses identités
- Premier prévenu poursuivi en vertu de la nouvelle loi de l´Etat américain sur le vol d´identité
- Inculpé de 14 chefs d´inculpation

3 spammeurs américains condamnés à un milliard de dollars d'amende 29/12/2004

- en 2000 un fournisseur d'accès a vu ses serveurs noyés sous un flot de spams pouvant atteindre jusqu'à 10 millions d'e-mails publicitaires par jour
  - Le spammeur le plus lourdement condamné devra payer 720 millions de dollars
- la moitié des courriers électroniques échangés en 2004 étaient du spam
  - selon les estimations les plus prudentes
  - Prévision de 80 % durant 2005

Les attaques informatiques

(selon le journal du net)

- Rapport ICSA Labs (division société de services en sécurité informatique Cybertrust)
  - étude annuelle relative à propagation et aux conséquences des virus en entreprise
  - panel : 300 organisations de plus de 500 postes, dotés d'au moins 2 connexions distantes et 2 réseaux locaux
  - 3,9 millions d'incidents relatifs à un virus relevés en 2004
- incident majeur chez 112 organisations
  - soit contamination de 25 postes (PC ou serveur) ou plus par un même virus
  - soit un virus ayant causé des dommages financiers significatifs pour l'entreprise
  - Augmentation de 12% par rapport à l'année 2003

Un troisième constat

- Personne n'est à l'abri
- La nuisance peut être importante
  - Impact sur l'entreprise

Un exemple célèbre : Yahoo

- Plainte de 3 organisations antiracistes pour hébergement d'un site de vente aux enchères d'objets nazis
- Légal aux USA
  - Accès par des internautes français
  - Demande que des techniques de filtrage en rendent l'accès impossible
- 20/11/2000, le juge des référés du TGI de Paris
  - 3 mois à Yahoo pour mettre en place une procédure de contrôle
  - sous peine d'astreinte de 100 000 F par jour de retard

Une base de réflexion

- 1er amendement de la constitution américaine

  "le congrès ne votera aucune loi limitant la liberté d'expression ou la liberté de presse"

- Article 9 de la déclaration des droits de l'homme

  autorise "tout citoyen à parler, écrire et imprimer librement" sauf "à répondre de l'abus de cette liberté dans des cas déterminés par la loi"

- Internet espace de liberté
  - Danger dans les pays totalitaires
  - L'État Chinois met en place régulièrement des filtres et demande aux société de moteurs de recherche de ne pas faire apparaître certains sites (Tibet, Tiananmen, etc.)
- Régulation au niveau mondial
  - Monde sans frontières

Un autre exemple (Libération, 16/9/05)

"Shi Tao a été condamné à 10 ans de prison pour avoir transmis une note confidentielle du parti communiste, des consignes à la presse officielle à la veille de l'anniversaire du massacre de la place Tiananmen.

Reporter sans frontière révèle que Yahoo avait livré aux autorités le détenteur de l'adresse et du téléphone d'où est parti le message.

Jerry Yang, co-fondateur de Yahoo se défend : pour faire des affaires en Chine ou n'importe où dans le monde, nous devons respecter les lois locales."

en Chine

- environ 100 millions d'internautes
- contrôle sur Internet : une cyberpolice identifie les cyberdissidents
- une soixantaine d'internautes en prison pour délit d'opinion

Un quatrième constat

- L'anonymat n'existe pas sur Internet
- Importance de garantir ses droits et libertés fondamentales

Les virus informatiques

Une forme de criminalité = les attaques sur Internet

- Les virus !

  Fini le temps des hackers solitaires qui envoyaient des virus capables d'effacer le contenu du disque dur dans le seul but de se faire remarquer de la communauté informatique et trouver un emploi dans une grosse compagnie. Désormais: nouvelle génération de hackers avec le crime organisé (but financier: récolté le plus d'argent avec le moins de risques possibles) d'où nouvelle génération de virus plus subtils chargés de récolté des donnée personnelles et confidentielles (identifiants, mots de passe, codes de carte bancaire…)

Cf. *étude publiée dans le Fig. Mag. du 6/01/2007.*

Origines ?

- Incertaine !
- Forcer la maintenance
- Protéger son emploi
- Garantir les droits
- Concurrence
- Créer un business
- Un jeu
- ….

Histoire (1)

- Le premier pas vers les virus : Core War
  - début des années 60
  - création d'un jeu par 3 informaticiens de la société Bell
  - lâcher 2 programmes de combat dans la mémoire vive de l'ordinateur
  - but : détruire le premier son adversaire ou être celui dont le nombre de copies restantes, après un temps déterminé, est le plus grand
- techniques de combat très simples : bombarder la mémoire de "1" (valeur binaire) ce qui modifiait le programme et le détruisait
- réservé à quelques initiés : pas de grand danger.

Histoire (2)

- Quelques années plus tard : presque un virus
  - Perfectionnement des programmes d'attaque par 2 italiens
  - ajout d'une procédure de copie du programme sur la mémoire de masse
  - abandon du projet
- premier virus :
  - par Fred Cohen, étudiant informaticien à l'Université de Californie
  - créer un programme parasite (comparable aux virus biologiques) capable de se reproduire et de pervertir les programmes
  - but : créer une sorte de vie artificielle autonome, sans la moindre volonté négative
- idée reprise dans le but de nuire
  - solution contre la copie pour des éditeurs de logiciel avant l'adoption de lois strictes sur les virus
  - exemple : virus pakistanais, distribué largement avec les copies pirates de logiciel vendues au Pakistan (pays sans loi de concernant les droits d'auteur)

Les virus (1)

"programme capable d'infecter un autre en le modifiant de façon à ce qu'il puisse à son tour se reproduire"

- véritable nom : CPA soit Code Auto-Propageable
- petit programme autoreproducteur situé dans un autre programme

Les virus (2)

- Objectifs : du canular sans conséquence à la destruction criminelle

- de simplement irritants à totalement paralysants
  - Wazzu
    - insère le mot «wazzu» dans les documents Word
    - modifie des chaînes aléatoires de mots
  - Worm.ExploreZip
    - se propage par le mail
    - prend le contrôle du système de messagerie
    - répond automatiquement à tous les messages entrants
    - envoie des pièces jointes destructrices qui peuvent effacer certains types de fichiers

Principe

- rien d'autre qu'un programme
  - indispensable : le sous programme de reproduction
  - parfois d'autres sous-programmes : partie destructrice, protection contre les anti-virus
- Reproduction :
  - recherche de nouveaux fichiers ou zones d'action sur le disque
  - s'assure qu'il n'a pas déjà infecté le fichier choisi
  - accroche le virus au fichier sélectionné
  - partie suffisante pour avoir un virus
- possède en général une signature
  - suite d'octets qui ne varient pas
  - permet de l'identifier grâce à une séquence d'octets consécutifs
  - méthode la plus utilisée par les anti-virus
  - Seulement le virus doit être connu
  - et d'autres sont polymorphes, leurs signatures n'arrêtes pas de changer…et même la manière de les changer (les métapolymorphes)

Quelques virus célèbre

- Brain le premier virus connu (parfaitement inoffensif)
- Michelangelo
  - crée une psychose au début de l'année 1992
  - se déclenche le 6 mars, jour anniversaire de la naissance de Michel-Ange en 1475
- 1260,V2P1,V2P2,V2P6 : premiers virus polymorphiques
- Iloveyou qui s'est propagé par les mails (naïveté des utilisateurs mâles qui lisait ce mail et avait leurs ordinateurs contaminé…)

Les types de cible

- **Le système** :
  - attaque du système ou de la zone d'amorçage du disque dur
  - exemple : le boot secteur (première chose qu'un ordinateur charge en mémoire à partir du disque et exécute quand il est allumé)
  - En attaquant cette zone de disque, le virus peut obtenir le contrôle immédiat de l'ordinateur
- **Les fichiers** :
  - souvent ne connaît la structure que d'un type de fichier, voire d'un fichier
    - s'adapte à ces fichiers et donc plus facilement invisible
  - Aujourd'hui : fichiers transitant par l'Internet qui sont les plus visés
- **Les macro** :
  - explosion de ces virus grâce au développement de la bureautique

Typologie (1)

- Macrovirus
  - langage de script des outils de bureautiques ou autres
    - inséré dans des documents contenant des macros (Word, Excel, OpenOffice, Accrobat, etc.)
    - VBScript accepté par de plus en plus d'applications
  - des virus infectent les macros : exécution de code à l'ouverture pour se propager dans les fichiers et accéder au système d'exploitation
- les bombes logiques (ou à retardement ou temporelle)
  - déclenchement suite à un événement
    - date du système, lancement d'une commande, …
    - capable de s'activer à un moment précis sur un grand nombre de machines
  - généralement pour créer un déni de service
  - bombe Tchernobyl activée le 26 avril 1999, 13ème anniversaire

Typologie (2)

- Polymorphe = peut prendre plusieurs formes
  - utilise des méthodes de cryptage aléatoire de leurs codes
  - empêche de l'identifier grâce à sa signature (n'en possède pas)
- mutants (ou méta-polymorphe)
  - virus réécrit pour modifier son comportement ou sa signature
  - Détection d'autant plus difficile
- retrovirus ou "virus flibustier" (*bounty hunters*)
  - capacité de modifier les signatures des antivirus afin de les rendre inopérants

Typologie (3)

- Cheval de Troie
  - Programme caché dans un autre exécutant des commandes sournoises
    - Ex : fausse commande de listage des fichiers qui les détruit au lieu de les lister
    - généralement donne un accès à la machine sur laquelle il est exécuté
    - caché dans un programme qui aide à sa diffusion (exemple : shareware)
  - Ouvrir une brèche dans la sécurité
    - accès à des parties protégées du réseau à des personnes de l'extérieur
  - Principe : ouvrir des ports de la machine = le pirate peut alors prendre le contrôle de l'ordinateur.
    - 1er temps : infecter votre machine en vous faisant ouvrir un fichier infecté
    - 2eme temps : accéder à votre machine par le port qu'il a ouvert
  - pas nécessairement un virus
    - son but n'est pas de se reproduire pour infecter d'autres machines
  - symptômes :
    - activité anormale du modem ou de la carte réseau, plantages à répétition
    - réactions curieuses de la souris, ouvertures impromptues de programmes
  - Protection :
    - installer un firewall : programme filtrant les communications entrant et sortant
    - essentiel de ne pas autoriser la connexion aux programmes inconnus

Typologie (4)

- les vers
  - virus capables de se propager à travers un réseau
    - sans support physique ou logique (programme hôte, fichier ...)
    - Ex : Iloveyou, Sasser, Mydoom, …
  - Un exemple :
    - 1988 : Robert T. Morris (étudiant, Cornell University) fabrique un programme capable de se propager sur un réseau et le lance 8 heures après plus tard, plusieurs milliers d'ordinateurs infectés
    - Problème (déni de service) :
      - le "ver" se reproduisait trop vite pour être effacé
      - Solution : déconnecter **toutes** les machines infectées
      - Difficile sur Internet !
  - se propagent souvent grâce à la messagerie (ex : Outlook)
    - attachement avec instructions pour récupérer le carnet d'adresse
    - Envoi de copies d'eux-même à tous ces destinataires
  - pour se protéger : ne pas ouvrir "à l'aveugle"

Propagation des virus

Les virus n'envahissent pas un ordinateur sans l'intervention d'un utilisateur

- Habituellement :
  - par disquettes et autres supports
  - par le téléchargement de matériel d'Internet
  - par des pièces jointes aux mails
- impossible par un mail qui ne contient que du texte
  - uniquement par les pièces jointes ou au moyen d'un mail contenant du texte en format RTF
  - scannez les pièces jointes des expéditeurs connus et n'ouvrez même pas celles que des inconnus envoient

Une réponse

- Technique !

Selon une étude parue dans le Fig. Mag. du 6/01/2007, l'éditeur McAfee recense 217 000 (!) virus, vers et chevaux de Troie connus sur la toile : une aubaine pour le marché de la sécurité informatique:

- *+ 13,6% en 2006; chiffre d'affaire estimé à 4 milliards de $.*

Les antivirus

- programmes capables de
  - détecter la présence de virus sur un ordinateur
  - nettoyer celui-ci si possible

- Reproduction des virus :
  - copie d'une portion de code exécutable dans un programme
  - ne pas infecter plusieurs fois un même fichier
  - vérifier si le programme a préalablement été infecté : la **signature virale**

- Signature : succession de bits qui les identifie

Techniques de détection

Recherche de la signature ou scanning

- la plus ancienne et la plus utilisée
- avantage : détection avant exécution en mémoire
- principe : rechercher de signature
  - nécessité d'avoir été confronté au virus
  - base de données
- Inconvénient : pas de détection des nouveaux virus ou des virus polymorphes
- méthode la plus simple à programmer
- utile que si elle recense tous les virus existants : mises à jour de la base de donnée tous les mois sur le site WEB des antivirus

Techniques de détection

Utilisation d'un contrôleur d'intégrité

- construire un fichier des noms de tous les fichiers avec leurs caractéristiques
  - taille, date et heure de la dernière modification, …
- détecter toute modification ou altération
  - à chaque démarrage de l'ordinateur (Antivirus non résident)
  - dès qu'un exécutable est ouvert (Antivirus résident)
- si "checksum" avant et après exécution différent
  - virus a modifié le fichier en question
  - Information de l'utilisateur
- Antivirus peut aussi stocker la date et la taille de chaque exécutable dans une BD et tester les modifications
  - rare de modifier la taille ou la date d'un fichier exécutable
  - parade pour virus : sauvegarder la date avant modification et la rétablir après

Techniques de détection

Moniteur de comportement

- rôle : observer l'ordinateur à la recherche de toute activité de type virale
- prévenir l'utilisateur en cas de détection
- programme résident actif en arrière plan, surveillant tout comportement inhabituel :
  - description d'attaque virale
  - tentatives d'ouverture en lecture/écriture des fichiers exécutables
  - tentatives d'écriture sur les secteurs de partitions et de démarrage
  - tentatives pour devenir résident

Techniques de détection

Démarche heuristique

- recherche de code correspondant à des fonctions virales
  - rechercher un type d'instruction caractéristique
  - Exemple : Pour un virus polymorphe, suite d'instructions de lecture suivie d'une suite d'instruction d'écriture
- méthode un peu plus intelligente que les autres :
  - vise à analyser les fonctions et instructions les plus souvent présentes dans des virus
  - passive comme le scanning
  - permet contrairement au scanning, de détecter des nouveaux virus

Techniques d'éradication de virus

- après détection du virus : le supprimer
- fonction primordiale des antivirus
- pas simple de récupérer le programme original
  - impossible dans le cas de virus avec recouvrement
    - virus détruit une partie du fichier lors de sa duplication
    - solution : destruction des fichiers infectés
  - Pour les autres
    - déterminer très précisément la localisation du virus dans le fichier, sachant qu'il peut être composé de plusieurs parties
    - le supprimer
    - aller chercher la partie du programme dont le virus avait pris la place et la restaurer

LES PRINCIPAUX PRODUCTEURS D'ANTIVIRUS

- Symantec
- McAfee
- Panda Software
- Trend Micro
- Cheyenne Software
- Avast (version gratuire pour les particuliers)

De l'importance des mises à jour

- **2 août** - Depuis quelques heures, le virus **MiMail.A** se propage très rapidement par courrier électronique. Il s'agit d'un ver qui profite d'une faille dans le logiciel Outlook que Microsoft a corrigée en avril dernier mais dont beaucoup d'utilisateurs de Windows n'ont jamais fait la mise à jour.
  - MiMail.A peut récupérer les données qui se trouvent dans certaines fenêtres de Windows et les retransmettre par Internet.
  - Le fichier attaché message.zip renferme le virus qui s'exécute au moment où l'on tente de décompresser le fichier.
  - des correctifs disponibles et même un utilitaire pour se débarrasser du virus
- **5 juin** - Après **Sobig.C**, voici **Bugbear.B**, **Xolox**, **Lovgate.K**, **Mumu** et **Nako**. Seule solution, un bon antivirus mis à jour cette semaine.

Quelles sont les règles de prudence à observer ?

- Ne vous servez pas de fichiers qui n'auraient pas été scannées au préalable (testées par un logiciel antivirus) et n'exécutez jamais un programme que vous venez de télécharger par mail ou sur un site Web sans l'avoir préalablement scanné avec un antivirus
- Ou configurer votre antivirus pour qu'il le fasse de manière automatique (cela évite ce laborieux surplus de travail)
- N'ouvrez pas les fichiers joints aux mails d'origine inconnue ou douteuse ou d'une personne que vous savez naïve sur ce sujet
- Procurez vous un logiciel antivirus et un pare-feu et faites régulièrement une mise à jour
- Faire des sauvegardes régulières (pensez aussi aux plantages des disques durs…)
- *La naïveté des internautes est le premier danger!*

Détecter un virus

- Diagnostic toujours difficile
  - machines complexes et capricieuses
  - utilisateurs maladroits
- Quelques indices :
  - plantages à répétition, indisponibilité de certaines applications, saturation de la mémoire, démarrages incomplets, problèmes d'installation, etc.
  - Mais ces problèmes peuvent être dus à des incompatibilités logicielles ou matérielles classiques…
  - Alors « vigilance constante ! » (Fol-Oeil dans *Harry Potter et la coupe de feu*)

Autres formes d'attaques

spyware ou espiogiciel

- programme chargé de recueillir des informations sur l'utilisateur de l'ordinateur sur lequel il est installé
  - pour les envoyer à la société qui le diffuse
  - pour lui permettre de dresser le profil des internautes
  - Exemple : traçabilité des URL des sites visités, traquage des mots-clés saisis dans les moteurs de recherche, analyse des achats réalisés via internet, …
  - *Beaucoup de spyware sur le toile: selon une étude publiée dans le Fig. Mag. du 6/01/2007: 850 spyware récoltés en une heure de balade, avec une forte concentration sur les sites pour enfants, proies faciles*
- installé généralement en même temps que d'autres logiciels
  - la plupart du temps des freewares ou sharewares
  - permet aux auteurs des dits logiciels de rentabiliser leur programme, par de la vente d'informations statistiques
  - permet de distribuer leur logiciel gratuitement
  - modèle économique dans lequel la gratuité est obtenue contre la cession de données à caractère personnel

espiogiciels

- pas forcément illégaux
  - licence d'utilisation du logiciel qu'ils accompagnent précise que ce programme tiers va être installé
- source de nuisances diverses :
  - divulgation d'informations à caractère personnel
  - consommation de mémoire vive
  - utilisation d'espace disque
  - mobilisation des ressources du processeur
  - plantages d'autres applications
  - gêne ergonomique (ouverture d'écrans publicitaires ciblés en fonction des données collectées)

deux types de spywares

- **internes** (ou *intégrés*)
  - comportant directement des lignes de codes dédiées aux fonctions de collecte de données
- **Externes**
  - programmes de collectes autonomes installés
  - Ex : Alexa, Aureate/Radiate, BargainBuddy, ClickTillUWin, Conducent Timesink, Cydoor, Comet Cursor, Doubleclick, DSSAgent, EverAd, eZula/KaZaa Toptext, Flashpoint/Flashtrack, Flyswat, Gator / Claria, GoHip, Hotbar, ISTbar, Lop, NewDotNet, Realplayer, SaveNow, Songspy, Xupiter, Web3000 et WebHancer

Protection

- ne pas installer de logiciels dont on n'est pas sûr à 100% de la provenance et de la fiabilité (notamment les freewares, les sharewares et plus particulièrement les logiciels d'échange de fichiers en peer-to-peer)

  Les logiciels gratuits dont on n'est pas sûr se rémunèrent souvent grâce à l'ajout de spyware. Attention donc!

  - Exemples de logiciels connus pour embarquer un ou plusieurs spywares : Babylon Translator, GetRight, Go!Zilla, Download Accelerator, Cute FTP, PKZip, KaZaA, iMesh, …
- la désinstallation de ce type de logiciels ne supprime que rarement les spywares qui l'accompagnent
- logiciels, nommés **anti-spywares** permettant de détecter et de supprimer les fichiers, processus et entrées de la base de registres créés par des spywares
- installation d'un pare-feu pour empêcher l'accès à Internet (donc de transmettre les informations collectées)

keylogger

- dispositif chargé d'enregistrer les frappes de touches du clavier et de les enregistrer, à l'insu de l'utilisateur
  - dispositif d'espionnage
- Capables parfois d'enregistrer les URL visitées, les courriers électroniques consultés ou envoyés, les fichiers ouverts, voire de créer une vidéo retraçant toute l'activité de l'ordinateur
- peut servir à des personnes malintentionnées pour récupérer les mots de passe des utilisateurs du poste de travail
- soit logiciel soit matériel
- Protection : ne pas installer n'importe quel logiciel

Le problème du Droit pour Internet

Une nouvelle problématique

- Modification des échanges d'information
  - Transmission immédiate
  - Achat et vente en ligne
  - Dématérialisation des procédures
  - Transfert "temps réel" de gros volumes de données
- Nécessité pour le droit
  - de prendre en compte les progrès techniques
  - de s'adapter pour sauvegarder les principes antérieurs qui le fondent et le légitiment

Les enjeux

- Naissance de l'Internet
  - Création de ses institutions
  - Création de règles, techniques puis de comportements
- Développement de l'Internet
  - de nouveaux utilisateurs
  - de nouveaux usages (commerciaux par exemple)
- Montée des enjeux économiques

Dualité de l'Internet

- Outil de connaissance et d'échange contribuant à la liberté d'expression et de communication
- Porteur de dérives et de menaces
  - utilisable pour commettre des actes illicites
  - diffuser des messages racistes
  - organiser le terrorisme international
  - violer la vie privée
  - …

Réponses possibles

- Mode d'organisation le plus adapté
  - Loi
  - Jurisprudence
  - Arbitrage
  - Codes de bonne conduite
  - Usages
  - aucun

Réticences à l'égard du droit

- Idée d'un espace de totale liberté : L'idée d'un monde virtuel : perte de contact avec la réalité
- Antinomie entre un droit par essence «national » et un univers transnational
- Incapacité du droit à traiter les problèmes : Volatilité de l'information, anonymat, internationalité, …
- Admiration des hackers et des pirates

2 axes de réponse

- Auto –régulation
- Réponse juridique

L'auto-régulation des règles de vie

UNIVERSITÉ PARIS VAL de MARNE

CONNAISSANCE ACTION

U.F.R. de DROIT

Université PARIS 12 - VAL DE MARNE

Auto régulation

- Soft law
- Netiquette
- Chartes
- Sceaux

Soft Law

- Code de bonne conduite, autorégulation
- Exemple des USA :
  - Safe harbour principles publié par le département du commerce américain (dernière version mars 2000)
  - En réponse à la directive européenne de 1995(95/46/CE)
  - Assurer la protection des données à caractère personnel transférées d'un état membre européen vers les EU
  - Les entreprises américaines ayant une activité transnationale peuvent déclarer l'adopter dans la gestion de leurs fichiers
  - Principes insuffisants au regard des lois européennes mais l'idée est là

Netiquette

- Avant : utilisateurs avaient "grandi" avec Internet
- Maintenant : Grand public
- But : définir un ensemble minimal de règles utilisables et adaptables par les institutions et personnes pour leur propre usage
- **RFC 1855**
- ***Netiquette Guidelines*** *d'octobre 1995*
  - note destinée à informer la communauté de l'Internet
  - ne spécifie en aucune manière un standard de l'Internet
- lignes de conduite pour les utilisateurs et gestionnaires
- oeuvre du groupe de travail *Responsible Use of the Network* (RUN) de l'IETF

Exemple : règles pour le courrier électronique

- règles de courtoisie habituelles s'appliquent
  - important vu que sans expression corporelle et intonation
- règles sur la propriété du mail varient d'un pays à l'autre
- Ne mailez pas ce que vous ne mettriez pas sur une carte postale
- N'envoyez pas de grandes quantités d'information non demandée
- N'envoyez pas de lettre-chaîne
- Attention aux Cc lorsque vous répondez
- LES MAJUSCULES DONNENT L'IMPRESSION DE CRIER
- Vérifiez que le destinataire peut décoder le message
- frais payés aussi par le destinataire
  - Envoyer un mail à quelqu'un peut lui coûter en bande passante, stockage ou temps machine
  - une raison fondamentale d'ordre économique qui rend la publicité par mail malvenue

La charte de Paris 12

- Accessible sur le site web ou au moment de l'inscription ou demander à l'accueil en Droit
- Valable pour tous (même les enseignants…)
- Utilisation pédagogique des moyens
- Respect des autres
- Respect du matériel
- Respecter les règles comme par exemple
  - ne pas communiquer ce mot de passe
  - prévenir le responsable informatique de toute anomalie constatée
  - ne jamais quitter un poste de travail sans se déconnecter
  - …
- Lisez la chartre !

Régulation par les acteurs d'internet

- Certains sites proposent des chartes de régulation
  - Apparues dès 1996
  - Explications sur la nature des données récoltées, leur utilisation, vos possibilités d'accès pour rectification
- Souvent illisibles dans les sites commerciaux
  - Plus pour servir de défense en cas de recours
  - Avec des avocats à la clés …

Une "bonne" charte

- Comporte les éléments suivants :
  - Description détaillée des informations recueillies
  - Raison de cette collecte
  - Traitements, identités des intervenants avec les conditions d'accès
  - Possibilité d'accéder aux données sur soi
- Dans un langage clair
  - Pour que le visiteur comprenne vite
  - Pour éviter toute ambiguïté en cas de procès

A vérifier

- Quelles sont les infos recueillies ?
  - Nom, prénom, adresse IP, code carte bancaire, la liste de vos achats, les pages visitées, …
- Comment et dans quelles pages sont collectées vos données ?
  - formulaire de saisie, …
- Comment seront exploitées les données ?
  - Personnalisation du site, marketing, revente des données, ….
- Quels sont les moyens d'arrêter la collecte ?
  - Coockies, autre site à visiter, …
- Comment savoir les données en possession du site, les faire modifier ou supprimer ?
  - Par demande, …
- Comment le site protège la confidentialité des données ?
  - Cryptage des données, …
- Communication à des tiers

Les chartes des professionnels

- AFA : association des fournisseurs d'accès et de services Internet
  - Réunit les prestataires techniques de communication électronique (réseau, hébergement, accès, service en ligne)
- Mission d'information du public
  - Décrire les usages
  - Attester de la relation de confiance avec les utilisateurs
- Favorable à la Netiquette
- Mise en œuvre d'outils de détection de spam, virus, …
- Confidentialité des courriers électroniques
- Pour le réseau : principe de la poste

Les sceaux de certification

- La présence du sceau indique clairement que le site ne présente pas de risque
  - Pour la relation commerciale **OU**
  - Pour la relation informative
- les sceaux doivent répondre aux critères suivants :
  - pouvoir vérifier leur authenticité :
    - distinguer les vrais sceaux des faux
  - clairement indiquer la protection fournie
  - permettre aux consommateurs de signaler facilement tout cas de non-respect des mesures de sécurité par l'exploitant du site
  - donner l'assurance que l'organisme qui les décerne est digne de confiance

Un exemple anglo-saxon : TRUSTe

- sans doute le plus réputé, www.truste.org
- parrainé par IBM, Microsoft, Novell, AOL, Compaq, …
- Accordé et affiché par des milliers de sites Web
  - adoptent ses principes de confidentialité, son processus de résolution des conflits
  - acceptent de se soumettre à une surveillance continue
  - programme de certification exclusivement sur la confidentialité
- Entre autres principes de confidentialité :
  - adoption et application de directives tenant compte de l'appréhension des consommateurs à fournir de l'information personnelle en ligne
  - communication des pratiques de collecte et d'utilisation des renseignements
  - consentement de l'internaute, accès aux données

Pour la France

- Relation commerciale :
  - Direction générale de la consommation, concurrence et de la répression des fraudes (DGCCRF)
  - Sceaux de certification n'offrent presque pas de garantie à l'internaute
  - interdit les termes Label, site certifié, référentiel
- Vie privée : la CNIL (Commission National Informatique et Liberté)

3 niveaux de garantie

- Définis par la DGCCRF
- Niveau 3 : Indépendants
  - Déclaration autonome
  - Avec un logo ou une marque distinctive
    - respecter une déontologie commerciale et/ou protection de la vie privée
    - Aucune valeur juridique
    - Création de réseau de confiance
    - Au visiteur de faire la démarche de contrôle
- Niveau 2 : Groupes professionnels
  - Correspond aux corporations, fédérations, …
  - Le groupe engage sa réputation en se laissant associer à un site
  - Charte commune
  - Mesures pour garantir la conformité des sites à la charte
- Niveau 1 : Certification officielle

Et pourtant …

- Faillite en 2000 du site américain de jouets ToySmart
- Le liquidateur du tribunal vend tout pour payer les créanciers ; Problème, la base de données des clients
  - Tollé de clients, TRUSTe et la FTC (~de la DBCCRF)
  - Dilemme : entre tribunal et FTC
  - Sauvé par Disney qui a racheté et immédiatement détruit

La réponse juridique

La réponse juridique

- Consensus sur la nécessité de soumettre l'Internet au droit
- Admettre que la liberté n'est pas absolue sur Internet
  - En tout cas pas plus qu'ailleurs
  - "ma liberté s'arrête où commence celle des autres"

Les défis

- Nécessité d'une réponse juridique adaptée
- Concilier
  - Protection des droits de la personne
  - Préservation de la liberté d'expression et de communication
- Internet n'est pas une zone de non-droit !
- Quel droit ?
  - Droit préexistant ou droit spécifique

droit spécifique ou droit commun ?

- Diversité : tous (ou presque) les domaines du droit concernés
- Droit commun s'applique tel quel dans beaucoup de domaines de l'Internet
  - La vente des livres sur Internet soumise à la loi du 10/8/81 (TGI Versailles du 5 juillet 2001)
  - "le site Internet d'une société ayant pour objet la commercialisation de tous matériels, logiciels, et toutes publications écrites, correspond à un magasin virtuel que le consommateur va visiter au moyen de son ordinateur par une démarche analogue à celle qui consiste à se rendre à l'intérieur d'un magasin"

Principe juridique fondamental

- Application des droits nationaux
  - Droit applicable au réseau : droit commun des différents états
- En France, le Conseil d'état a estimé que :
  - "l'ensemble de la législation existante s'applique aux acteurs de Internet … Il n'existe pas et n'est nul besoin d'un droit spécifique d'Internet et des réseaux" (rapport de la commission intergouvernementale mise en place le 16 mars 1996)
  - Si la culture est virtuelle et mondialisée, la citoyenneté d'un internaute est étatique

D'où

- Application distributive aux diverses applications de l'Internet des règles relevant de différentes branches du droit
- Le droit commun
  - Nécessité d'adaptations ponctuelles au regard de certaines spécificités techniques
  - Œuvre du juge : constitution d'une jurisprudence
  - Œuvre du législateur : exemple la loi "Informatique et libertés"

Internet et le droit

- Nécessité de prendre en compte le contexte par nature international
- Diverses approches :
  - En Europe : plutôt extension des règles traditionnelles
  - Aux USA : plutôt adoption de règles spécifiques
- Pas de consensus sur la nature des solutions : encore moins de droit international !

Tout un arsenal en droit français

- Code pénal : permet de réprimer les atteintes à la pudeur, la diffusion de message à caractère violent, pornographique ou incitant à la violence
- Droit d'auteur : la loi interdit les reproductions illicites de documents originaux (écrits, sons, images, …) quel que soit le support
- …

Difficultés

- Nécessité d'une évolution relative aux règles nouvelles de la société de l'information en Europe et dans le monde
- Nécessité d'une adaptation aux spécificités
  - Caractère transnational
  - Volatilité et fugacité des contenus
  - D'où difficulté en matière pénale de la constatation de l'infraction et de l'identification de l'auteur
  - Maintenant : écrit électronique admis comme l'écrit papier en matière de preuve (depuis 2000)

Libertés et droits fondamentaux

Libertés et droits fondamentaux

- Notion récente (fondamental utilisé pour la première fois par le conseil constitutionnel dans sa décision du 16 janvier 1982 relative aux nationalisations)
- Une grande diversité, considération
  - De l'être (dignité de la personne humaine, respect du corps humain, vie privée, protection de l'enfance, …)
  - Du citoyen (droit à une nationalité, de vote, liberté politique, religieuse, d'aller et venir, à la sûreté, de pensée, de croyance, d'expression, de créer, …)
  - Du justiciable (droit à un tribunal impartial, à la défense en pénal, présomption d'innocence, droit des victimes, exécution des décisions de justice, ..)
  - De l'acteur économique et social (propriété, liberté du commerce et de l'industrie, du travail, droits sociaux, à la santé, au logement, …)

Concernés par l'Internet

- Protection des données personnelles
- Secret des correspondances électroniques
- Respect de la vie privée
- Liberté d'expression
- Protection des mineurs
- …

La fracture numérique

- 1 foyer sur 2 connecté en France, 2006
- Question de l'égalité entre les citoyens
- Problème si l'Internet devient le seul mode d'accès à des procédures ou des informations
  - Dématérialisation
  - La garantie de l'accès à l'Internet un droit essentiel de l'homme ?
  - Un petit village andalou a déclaré la gratuité de l'Internet droit imprescriptible de l'homme (Libération, oct 2001)

Les données personnelles

- Directive du 24 oct. 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation des données
- toute information concernant une personne physique identifiée ou identifiable
  - Directement ou indirectement par référence à un numéro ou à un ou plusieurs éléments spécifiques propres à son identité physique, psychique, économique, culturelle ou sociale

Remarques

- Concerne les données de toute nature
- Concerne seulement les personnes physiques
- Numéro IP est-il concerné ?
  - Identifie une machine
  - Mais indirectement son propriétaire
- Protections juridiques de la vie privée
  - ex : code civil art. 9, art.8 de la CESDH (convention européenne de sauvegarde des droits de l'homme)
  - Insuffisantes face aux dangers de traitements des données

Les menaces

- Diffusion d'informations
  - Rapidité
  - Planétaire
- Collecte d'informations
  - Favorisée par le commerce électronique
  - Recueillies de plein gré
    - Ex des infos dévoilées dans les forums (la CNIL recommande l'information des utilisateurs rappelant l'interdiction d'utiliser les infos révélées à d'autres fins que celles ayant justifié leur diffusion)
    - Formulaire en ligne : 41% des internautes renoncent à livrer des infos personnelles et 40% mentent (sondages américains, 2002)
  - Recueillies à l'insu de l'internaute

Quelques moyens de "pister"

- Les variables d’environnement
- Les cookies
- Les traçages à base de fichiers d'audit
- La mémoire cache et proxy

Les variables d'environnement

- outil fourni au programmeur par le système d'exploitation
  - Objectif : permettre aux applications de partager des informations
  - Moyen : placer les informations dans des variables
- très utilisé
- Ex : navigateur pour prendre en compte des éléments propres à votre configuration
  - type de navigateur utilisé, version : permet au serveur de ne pas lancer des applications incompatibles
  - les références de la dernière page lue
  - Les sites qui achètent des bandeaux publicitaires comptent le nombre de connexions effectuées immédiatement après un clic sur une des pages contenant un de ces bandeaux

Les cookies

- Fichier de très petit taille contenant des informations, déposé sur votre ordinateur, émis et transmis au serveur
- Objectif : stocker des informations et déterminer votre parcours durant une session et vous profiler
- avantage :
  - dispensent d'un stockage sur le serveur
  - Propriété de l'utilisateur
- inconvénient :
  - si l'internaute utilise une machine différente, cookies introuvables
  - Peut être effacé ou modifié directement par l'internaute
  - Peut être refusé par l'internaute
- souvent exploités au cours d'une même session
- Les informations figurant dans le cookie peuvent être claires ou codées : un code qui renvoie à des informations stockées sur le site

Exemples

- un site d'actualité : demande de remplir un formulaire de vos préférences
- un site de commerce électronique : chaque fois que l'utilisateur sélectionne un produit
- un moteur de recherche de sites : positionne des cookies selon les rubriques visitées pour afficher dynamiquement des bandeaux publicitaires ciblés
- un site web :
  - propose de choisir la couleur du fond d'écran, la présence de multi fenêtrage ou encore les polices de caractère utilisées
  - pour présenter une page d'accueil correspondant aux goûts

Les fichiers d'audit

- Collecter les requêtes reçues sur un serveur
- But :
  - permettre à l'administrateur de connaître avec précision la répartition des charges du système
    - quand le serveur est-il le plus mis à contribution ?
    - quels fichiers sont les plus téléchargés ?
  - optimiser le fonctionnement du site
- Caractéristiques :
  - l'internaute ne peut pas deviner qu'on enregistre ses transactions
  - Le traçage comme le traitement du fichier (tris, croisements) peut être réalisé entièrement à son insu

Un exemple

- Nécessité que toute exploitation du fichier d'audit se situe dans le cadre légal : information des personnes, finalité claire et déclarée, droit d'opposition, droit d'accès, etc.
- Dans le cas d'une procédure judiciaire : l'exploitation du fichier d'audit est un moyen extrêmement efficace pour retrouver un internaute se livrant à des activités illicites

La mémoire cache et proxy

- Rôle : optimiser les transactions
- **sur votre ordinateur :**
  - le navigateur enregistre dans un répertoire cache les pages consultées
  - si la fonctionnalité de mémoire cache est activée, il suffit pour reconstituer entièrement votre parcours et même visualiser les pages que vous avez consultées
    - de passer après vous sur le poste
    - d'ouvrir le répertoire qui contient les fichiers cache
    - de les classer en un clic par ordre chronologique
- **Sur un serveur proxy :** si vos requêtes passent par le proxy, vous n'avez pas de prise sur la conservation éventuelle de fichiers d'audit

Le cadre légal

- Diversité des sources
  - Nationale : loi Informatique et libertés le 6 janvier 1978
  - Directives communautaires :
    - "Vie privée et communications électroniques" du 12 juillet 2002
    - Internationales :
      - Conventions sur la protection des personnes à l'égard du traitement des données à caractère personnel du 28 janvier 1981(Conseil de l'Europe)
- Loi Sarkozy sur la sécurité intérieur :
  - Les entreprises sont obligés de gardé des traces pendant 1 ans des connexions internet : url, ftp, méls, etc.
  - Gros coût pour les entreprises
  - Plusieurs déjà condamnés pour ne pas avoir pu données les fichiers de log (les traces internet des utilisateurs/employés de l'entreprise) à des jours donnés

La CNIL

Commission Nationale de l'Informatique et des Libertés

- Autorité indépendante
  - Tout responsable – ministre, PDG, ..- doit lui faciliter la tâche, ne peut s'opposer à son action
  - Ne reçoit d'instruction d'aucune autorité
- Autorité administrative
  - recours possible devant la juridiction administrative
  - budget imputé sur celui de l'état
- Créée par la loi N° 78-17 "informatique et libertés" du 6 janvier 1978

Missions

- Information des personnes sur leurs droits et obligations
- Aide aux particuliers dans l'exercice de leurs droits : réception des plaintes, réclamations et intervention auprès des organismes concernés
- Conseil et concertation :
  - Recommandations sur des sujets divers (vidéosurveillance, sondages)
  - Proposition de mesures législatives ou réglementaires au gouvernement
- Environ 4000 plaintes ou demandes de conseils par an
- Expertise et veille technologique
- Garantir le droit d'accès : au nom des citoyens auprès des RG, ….
- Faire respecter la loi
  - Recenser tous les fichiers informatiques (300 par jour) : mise en œuvre nécessite un avis favorable de la CNIL
  - Mission de contrôle et de vérification des fichiers
  - En cas de manquement avertissements (49) ou plaintes au parquet (25)

Garante du respect de la loi Informatique et Liberté

- « L'informatique doit être au service de chaque citoyen »
- Son développement doit s'opérer dans le cadre de la coopération internationale
- Elle ne doit porter atteinte ni à la dignité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques" (art. 1)

La loi reconnaît 7 droits

- le droit à l'information préalable :
  - Les fichiers ne doivent pas être créés à votre insu.
  - Les personnes qui créent des traitements ne doivent pas vous laisser dans l'ignorance de l'utilisation qu'ils vont faire de ces données.
- Le droit de curiosité : pour pouvoir accéder aux données qui vous concernent, vous avez le droit de demander à tout organisme s'il détient des informations sur vous.

Vos droits (2)

- Le droit d'accès direct : vous pouvez obtenir communication des informations qui vous concernent en les demandant directement à l'organisme qui détient le fichier dans lequel vous figurez
- Le droit d'accès indirect : pour certaines données nominatives, la loi prévoit un intermédiaire entre vous et l'organisme qui détient le traitement
  - données médicales : médecin de votre choix
  - données figurant dans des traitements intéressant la sûreté de l'État, la défense et la sécurité publique : un commissaire de la CNIL

Vos droits (3)

- le droit de rectification :
  - si vous avez constaté des erreurs lorsque l'organisme qui détient le fichier vous a communiqué les données vous concernant, vous pouvez les faire corriger.
  - La loi oblige l'organisme à rectifier d'office et de lui-même les informations dès lors qu'il a connaissance de leur inexactitude.
- le droit à l'oubli :
  - l'informatique permet de conserver indéfiniment les données personnelles.
  - La loi a donc prévu un droit à l'oubli, afin que les personnes ne soient pas marquées à vie par tel ou tel événement

Vos droits (4)

- Le droit d'opposition :
  - si vous avez des raisons légitimes pour ne pas figurer dans tel ou tel fichier, vous pouvez vous opposer à votre fichage.
  - On peut l’exercer au moment de la collecte ou plus tard, en demandant par exemple la radiation des données contenues dans les fichiers commerciaux.
  - Ce droit ne s'applique qu'aux fichiers qui n'ont pas été rendus obligatoires par une loi.

Le respect de vos droits

- Le non-respect par les responsables de fichiers de vos droits lorsque vous souhaitez les exercer est le plus souvent sanctionné pénalement :
  - porter plainte
  - faire condamner les fautifs

Création de sites web et protection des données personnelles

- Loi « Informatique et Libertés »
- Avant la mise en ligne d'un site web
  - Obligation de déclaration CNIL
    - De tout traitement automatisé de données nominatives
    - Par la personne qui a le pouvoir de décider de la création du traitement
  - Obligation d'information
    - Accord recueilli des personnes avant toute diffusion sur Internet (accord tacite en l'absence de réponse au-delà d'un certain délai)

Loi pour la confiance dans l'économie numérique

UNIVERSITÉ PARIS VAL de MARNE
CONNAISSANCE ACTION

U.F.R. de DROIT
Université PARIS 12 - VAL DE MARNE

Loi pour la confiance dans l'économie numérique (LEN)

- Loi N° 2004-575 du 21 juin 2004
- Objectif : favoriser le développement du e-commerce
- Moyen : clarifier les règles pour les consommateurs et les prestataires techniques et commerciaux
- « La communication au public par voie électronique est libre » (art 1)
- Minimum de surveillance imposée aux hébergeurs de sites (apologie de crime contre l'humanité, racisme, pédophilie)
- Responsabilité globale du e-marchand sur l'ensemble de la vente (reconnaissance du contrat électronique et principe du double clic)
- Interdiction de la publicité non sollicitée par mail
- Mieux sécuriser les échanges (cryptologie libre) et favoriser la lutte contre la cybercriminalité

LEN (2)

- Sur un plan contractuel :
  - les conditions générales d'utilisation des services d'accès à internet, telles qu'elles sont rédigées dans l'ensemble des contrats d'abonnement chez les FAI, référencent la Netiquette ou interdisent explicitement la pratique du 'spamming'
  - les FAI n'hésitent alors pas à priver d'accès leurs clients identifiés comme émetteurs de spam
- Diverses décisions de justice
  - TGI Rochefort-sur-mer, 28 février 2001 ; TGI Paris, 15 janvier 2002 ont reconnu la licéité d'une telle solution
  - Notamment en se basant sur l'article 1135 du Code civil : "Les conventions obligent non seulement à ce qui y est exprimé, mais encore à toutes les suites que l'équité, l'usage ou la loi donnent à l'obligation d'après sa nature"

La liberté d'expression

UNIVERSITÉ PARIS VAL de MARNE
CONNAISSANCE ACTION

U.F.R. de DROIT
Université PARIS 12 - VAL DE MARNE

La liberté d'expression sur Internet

- Naissance d'un journalisme sauvage (ex du 11 septembre 2001) et les webzines
- Pluralité de l'information (affaire Clinton)
- Développement de l'auto publication (sorte d'édition à compte d'auteur)
- Les weblogs ou dazibaos informatiques
- Tribunes d'expression à faible coût
  - Interdit dans certains pays
  - Sous haute surveillance dans certains pays (ouverture au commerce électronique mais adaptation du code pénal chinois pour sanctionner la diffusion d'informations jugées subversives et interdiction de certains sites comme les sites de journaux étrangers par exemple)

Les effets pervers

- Trop d'informations nuit à l'information
  - Estimation à 9 Milliards de sites en 2001
  - En 2001 : recherche de « business » sur google produisait 81 Millions de réponses (avec 3 milliards de pages indexées)
- Risque de désinformation
  - Publicité
  - Fiabilité ; Ex : remise en compte de l'attentat contre le Pentagone le 11 septembre…
  - Les rumeurs :
    - Ex : la COB a créé une équipe chargée de repérer les fausse rumeurs boursières sur Internet
    - Les hoax

Les hoax

- Annonces reçues par mail
  - par exemple l'annonce de l'apparition d'un nouveau virus destructeur ou bien la possibilité de gagner un téléphone portable gratuitement, de tueurs fous sur la route, RG estimait J.-M. L.-P. vainceur en 2002 à 51%, ...) accompagnées d'une note précisant de faire suivre la nouvelle
  - But : l'engorgement des réseaux ainsi que la désinformation
- Site : http://www.hoaxbuster.com/

Un exemple « rigolo »

- Craig (Ou Greg, Sonia ou encore Denis) Sherehold, 17 ans, atteint d'un cancer en phase terminale
- Son vœu le plus cher : *"Etre, avant de mourir, dans le livre Guinness des records en tant que particulier possédant le plus grand nombre de cartes de visites"*
- Mail envoyé aux chefs d'entreprises, cadres de collectivités, élus, …
- A chacun de l'envoyer si possible à d'autres cadres
- Question : Greg existe-t-il vraiment ou n'est-il plutôt, comme on le sait aujourd'hui, qu'un agent fictif d'un genre spécial ?
- Soupçons : des sociétés de renseignement privés qui utilisent la maladie pour récolter un maximum d'information sur les dirigeants et leurs sociétés

A qui profite le crime ?

- Rumeur : diffuser n'importe quoi …
- Nouvelle forme d'intelligence économique
- Attention aux mails
  - De source inconnue
  - Avec des sujets trop pompeux
  - Des textes trop larmoyants
  - Des demandes d'aide, de soutien, …
  - Des gains mirifiques :
    - La techniques Nigérienne (existait avant par lettre depuis les années 1970) : on vous promet des millions de dollars à débloqués si vous donnez 100 dollars (compte d'un fils de PDG, Ministre, Président d'un club de foot … du Niger). Ce fils qui vous a écrit vous supplie de le faire car à cause d'un complot/coup d'état militaire, le compte est bloqué en Suisse (naturellement…)
    - Bien évidemment, le gogo qui prend contacte et donne ne voit rien venir…
    - Pire : les escrots peuvent ensuite se faire passer pour la douane et demander une amende à payer pour ne pas finir en prison…

Droit, site web et entreprise

Le droit de l'entreprise

- Les sites web
  - Nom de domaine
  - Les obligations à respecter
- Le droit à la propriété intellectuelle

Nom de domaine

- accès à un site par son URL
- Ex : http://www.votre-fournisseur.com/votrenom (difficile à mémoriser)
- Préférable d'avoir une adresse du type :

  http://www.votrenom.com

  http://www.votrenom.org

  http://www.votrenom.fr …

  - plus simple à mémoriser
  - favorise le bouche à oreille (diffuser rapidement une adresse)
  - donne généralement une touche de professionnalisme

Création de sites web

- Nommage
  - International : ICANN (org, com, net, biz, …): aucune précaution : premier arrivé premier servi
  - National : AFNIC .fr
  - Nom de domaine communautaire (règlement du 22 avril 2002) : en attente des règles ?
- Objectif de l'AFNIC
  - Prévenir le cybersquatting
  - Dans le respect du droit des marques et de la propriété intellectuelle

Acquérir un *.fr*

- Principe de territorialité
- l'Afnic, chargée d'attribuer les noms en *.fr* uniquement (liste non exhaustive) :
  - aux titulaires d'une marque déposée
  - aux entreprises
  - aux associations immatriculées à l'INSEE
  - aux professions libérales
  - aux artisans
  - aux collectivités publiques
- + dès début 2005 (liste non exhaustive) :
  - les particuliers
  - toutes les associations, même non immatriculées à l'INSEE

Nom de domaine

- Une ressource rare : conflits !
- Jurisprudence : En général fait primer la marque préexistante sur le nom de domaine; Date d'enregistrement, notoriété, absence de déchéance de la marque, ….

grabbing

- prévoir l'achat de noms de domaines de certaines entreprises et de les acheter avant celles-ci (les .com, .net et .org n'étant soumises à aucun contrôle...)

- des personnes peu scrupuleuses ont revendu à prix d'or (plusieurs millions de dollars parfois) des noms de domaine intéressants pour certaines compagnies (leur propre marque généralement)

Attention !

- On ne peut pas déposer n'importe quel nom
- Ex : michel-edouard-leclerc.fr (site porno)
  - Le 28 juin 2004, Nanterre
  - Dépôt possible mais illicite
    - Abandon du droit nom par ME Leclerc
    - Mépris du droit à la personnalité : non respect de la charte de l'Afnic (ne pas porter atteinte aux droits des tiers)
  - Condamnation : retrait du nom et 3000€ amende

L'internet et la propriété intellectuelle

- Article 1 de la convention de l'union de Paris du 20 mars 1883
  - « la protection de la propriété industrielle a pour objet les brevets d'utilité, les dessins ou modèles industriels, les marques de fabrique ou de commerce, les marques de service, le nom commercial et les indications de provenance ou d'origine, ainsi que a répression de la concurrence déloyale »
- Le droit de la propriété intellectuelle englobe le droit d'auteur classique et les bases de données (à voir l'année prochaine)

Les risques liés à l'utilisation de logiciels illicites

- Risques techniques : Virus, dysfonctionnements, …
- Risques juridiques
  - Logiciel = œuvre de l'esprit
  - Protégé par le régime juridique du droit d'auteur
  - Des contrôles possibles

10 règles pour détecter un risque de contrefaçon

- Prix inférieur à celui du marché
- Logiciel vendu sans manuel d'utilisation ni documentation
- Présence de mentions manuscrites sur le CD
- Le site d'achat en ligne propose des copies de sauvegarde
- Le logiciel porte des mentions non usuelles
- Des logiciels d'éditeurs différents sur un même CD
- Logiciel sans emballage d'origine, pochette mal imprimée, CD doré et non argenté
- Absence des dispositifs de sécurité prévus par l'éditeur
- Vendu aux enchères
- Vendeurs sans garantie de fiabilité
- …

Le droit d'auteur

UNIVERSITÉ PARIS VAL de MARNE
CONNAISSANCE ACTION

U.F.R. de DROIT
Université PARIS 12 - VAL DE MARNE

Le droit d'auteur (1)

- S'applique à Internet au travers
  - du code de la propriété intellectuelle (Loi N° 92-597 du 1er juil. 1992)
  - De textes et traités internationaux signés par un grand nombre de pays (Traité de L'OMPI sur le droit d'auteur du 20 déc. 1996 par exemple)
- Sont des œuvres protégées
  - Texte
  - Image
  - Son
  - Logiciel
  - Vidéo
- Le CPI précise
  - Toute œuvre protégée par le droit d'auteur ne doit pas reproduite modifiée même partiellement sans autorisation de l'auteur ou de ses ayants droits (art. L. 122-4 du CPI)
  - L'auteur d'une œuvre de l'esprit jouit sur cette œuvre du seul fait de sa création d'un droit de propriété incorporelle exclusif et opposable à tous (art. L 111-1 du CPI)

Le droit d'auteur (2)

- Peut être défini comme un droit d'exploitation monopolistique et privatif
- Porte sur des éléments pouvant être considérés comme originaux, portant l'empreinte personnelle de leur auteur et fixée sur un support
- Implique pour son possesseur
  - Des droits patrimoniaux : cessibles, exclusifs, temporaires et indépendants du support matériel
  - Des droits moraux : perpétuels, incessibles et inaliénables

Droits patrimoniaux

- Prescriptibles 70 ans après le décès de l'auteur
- Essentiellement de 3 types :
  - Droit d'exploitation
  - Droit de représentation (communication de l'œuvre au public par un procédé quelconque)
  - Droit de reproduction (fixation matérielle par tout procédé permettant la communication au public)
    - Ex : la numérisation (donc soumise à autorisation préalable de l'auteur sinon contrefaçon)
    - Exception pour le logiciel : la copie de sauvegarde

Droits moraux

Parmi les prérogatives conférées par le droit moral :

- Droit au nom et à la paternité
- Droit de divulgation
- Droit au respect et à intégrité de l'œuvre

Une autre exception

- Les webmestres peuvent librement effectuer « des analyses et courtes citations » de œuvres protégées (art. L 122-5-3 du CPI)
- les pages web qui les incorporent doivent alors présenter un caractère critique, polémique, pédagogique, scientifique ou d'information
- Attention : il faut citer le nom de l'auteur

Les sanctions

- Actes de contrefaçon : Délit pénal
- Sanctions jusqu'à
  - 2 ans d'emprisonnement
  - Et 150 000 € d'amende
  - Octroi de dommages et intérêts

Un exemple

L’exploitant du site shootgame.com a été condamné à 4500€ de dommages et intérêts pour avoir reproduit sans autorisation des auteurs des éléments graphiques leur appartenant

Un exemple : la musique

- Compresser ses propres disques et pour son usage personnel est légal
- Mettre à disposition de la musique sur Internet est illégal sans autorisation des ayants droit (Auteurs, éditeurs, producteurs, interprètes)
- Détenir des fichiers sans avoir acquis le support original est un délit
- Mettre sur son site des liens hypertextes vers ce type de fichier peut donner lieu à des poursuites pour complicité de contrefaçon

Un autre exemple : les photographies

- Reproduction interdite sans l'accord de l'auteur ou de l'agence de presse titulaire des droits
- De plus, normalement obligatoire de mentionner le nom de l'auteur sous la photo

Les sites internet

- Peut constituer une œuvre de l'esprit dès lors qu'il présente des caractères d'originalité
- Attention :
  - Aux chartes graphique des site préexistants
  - Aux logos
  - Aux extractions de bases de données
  - A ne pas porter atteinte aux droits d'un tiers en affichant un site dans une fenêtre de son site (framing)