

Module A2

Intégrer la dimension éthique et le respect de la déontologie

Bruno Bouzy

Préparation au C2I

UFR math info

Préambule

- « Nul n'est censé ignorer la loi »
- Le droit de l'informatique
 - Doit être connu des utilisateurs de l'informatique
 - N'est pas réservé aux juristes
- Objectifs du module
 - Grands principes du droit de l'informatique
 - Problématiques juridiques pour les nouvelles technologies
 - Connaître les règles d'échange sur Internet

Plan

- Ch1: Introduction
- Ch2: Maîtrise de l'identité numérique
- Ch3: Sécurisation des informations sensibles
- Ch4: Protection des données confidentielles
- Ch5: Loi sur la création et la protection des oeuvres
- Ch6: Chartes d'utilisation et de bon comportement

A2

Chapitre 1

Introduction au module

Droits fondamentaux et Internet

- Conflit entre droit et informatique
 - La technologie évolue plus vite que le droit
 - Loi informatique et libertés du 6 janvier 1978
 - Le droit de l'informatique est complexe donc méconnu
- Règles de bon usage en vigueur sur Internet

Internet fantastique outil de communication

- Article 19 de la déclaration des droits de l'homme:
- *« tout individu a droit à la liberté d'opinion et d'expression, ce qui implique le droit de ne pas être inquiété pour ses opinions, et celui de chercher, de recevoir et de répandre, sans considérations de frontières, les informations et les idées, par quelque moyen d'expression que ce soit. »*

Le droit et l'informatique

- Internet n'est pas une zone de non droit
- Risque juridique réel à utiliser un ordinateur sans connaître les lois traitant de l'informatique
- Connaître la loi permet de:
 - Ne pas commettre d'infraction
 - Demander réparation si victime d'infraction
- Le Code Pénal est divisé en Livres

Livre III Titre II Code Pénal

- Article 323-1
 - Accéder frauduleusement dans un système de traitement de données : 2 ans de prison + 30000 euros d'amende
 - Suppression ou altération des données: 3 ans de prison + 45000 euros d'amende
- Article 323-7
 - Une tentative de délit est punie de la même peine que le délit correspondant.

A2

Chapitre 2

La maîtrise de son identité numérique

Préambule

- Internet, média grand public, attise la convoitise des escrocs
- Développement de logiciels malveillants ou « malware »

Identité sur Internet

- Une utilisation d'Internet se matérialise par des traces.
- L'utilisateur n'est pas anonyme
- Identité numérique = tous les moyens logiciels ou matériels permettant d'identifier de manière fiable et unique une personne
- Identité numérique = identifiant + mot de passe
- Si Internet via Fournisseur d'Accès alors identifiant = adresse IP

Les traces sur Internet

- Identifiant
 - Login, adresse IP
 - Mot de passe
- Cookies
- Espiogiciels ou « spyware »

Les cookies (1/2)

- Fichiers créés par un site Internet sur votre ordinateur, contenant des informations sur vous et vos habitudes d'utilisation du site.
- Informations contenues dans un cookie:
 - Adresse IP
 - Système d'exploitation et navigateur utilisés
 - Informations statistiques
- Utile pour le commerçant et le publicitaire

Les cookies (2/2)

- Gestion des cookies
 - Le site doit demander l'autorisation à l'utilisateur
 - L'utilisateur accepte ou refuse
- Les cookies sont utilisés de manière
 - Bienveillante en général
 - Malveillante parfois
- Légalité des cookies
 - Obligation de demander l'autorisation à l'utilisateur

Les espioniciels

- Espioniciel = « spyware » = logiciel espion
 - A l'insu de l'utilisateur, l'espioniciel rassemble des informations sur l'utilisateur et les transmet à une organisation qui en tire parti.
 - Malveillant
 - Installé sur l'ordinateur lors d'un téléchargement d'un autre logiciel
- Ampleur:
 - En moyenne, 27 spywares détectés par ordinateur entre le 1/1/2004 et le 30/4/2004

Les espiogiciels

- Frontière entre malveillance et bienveillance
 - Un logiciel installé sur une machine collecte des informations sur l'utilisateur et les envoie à
 - l'éditeur du logiciel pour faciliter les mises à jour (bienveillance)
 - une organisation malveillante
- Diffusion des espiogiciels
 - Via l'installation de programmes gratuits d'échange de fichiers (Kazaa, iMesh, Gozilla)

Maîtrise des logiciels

- « prudence est mère de sûreté »
- Ne télécharger que les logiciels dont on est sûr
- Utiliser un pare-feu ou « firewall »
- Procéder à des nettoyages réguliers

Exemples

- Ré-orienteur de navigateur vers certaines pages
- Infecteur de fichiers
- Interception de touches clavier
- Plantage d'une machine à distance
- Voleur de mots de passe
- Ecoute du trafic réseau
- Envoi de courriers non sollicités

Autres techniques d'espionnage

- Javascript = langage d'écriture de programmes insérés dans les pages web HTML et exécutés lors de la lecture de la page par le navigateur
- Applet = petite application Java effectuant des tâches spécifiques
- ActiveX = technologie Microsoft proche des applets Java
- Bienveillance à priori, mais malveillance parfois

A2

Chapitre 3

La sécurisation des informations sensibles

Virus

- Programme
 - Effectuant certaines actions
 - Cherchant à se reproduire
 - Éventuellement malveillant
 - Se propage par tout moyen d'échange d'informations numériques
 - Cédéroms, DVD, disquettes, Internet

Vers, Canulars

- Ver
 - Programme se propageant par le courrier électronique en utilisant le carnet d'adresses de l'utilisateur
- Canular = « hoax »
 - Fausse information ou rumeur se propageant par le courrier électronique
 - Pas dangereux

Chevaux de Troie, Portes dérobées

- Cheval de Troie = « Trojan Horse »
 - S'introduit sur l'ordinateur à l'insu de l'utilisateur
 - Effectue des tâches à son insu
 - Similaire à un espioniciel
- Porte dérobée = « backdoor »
 - Programme permettant d'accéder à distance à un ordinateur
 - = cheval de Troie distant
 - = client + serveur

Phishing

- Phishing = « fishing » = pêcher
 - Envoyer un courrier en se faisant passer pour une organisation (banque, administration, etc) connue de l'utilisateur afin de récupérer des informations personnelles importantes de l'utilisateur (coordonnées bancaires, mot de passe, etc)
 - Utiliser ces informations de manière malveillante

Les hackers

- Origine: « hacker » = celui qui se sert d'une hâche
- Passionné qui cherche à comprendre le fonctionnement interne de l'ordinateur
- Pas nécessairement malveillant
- « cracker » = personne qui cherche à percer un système de sécurité
- Chapeaux blancs, chapeaux gris, chapeaux noirs

Mail bombing

- Envoi dans un but malveillant d'une quantité considérable de courriers électroniques à une même adresse.

Notions de sécurité

- Pour une ressource informatique
 - seules les personnes autorisées y ont accès
- Protection via
 - Authentification (identifiant + mot de passe)
 - Sécurisation du réseau (pare-feu)

Contrôle d'accès, login, mot de passe

- Setup de l'ordinateur
- Compte de l'ordinateur
- Saisie automatique:
 - À éviter
- Règles sur le mot de passe:
 - Long, sans signification, cacactères spéciaux, changé régulièrement, etc.

Outils de protection

- Logiciel anti-virus
 - Protège en scrutant tous les fichiers entrant
 - Analyse périodiquement le contenu du disque dur
 - Désinfecte en cas de contamination
- Pare-feu = « firewall »
 - Contrôle les connexions réseau de l'ordinateur, en entrée et en sortie
 - Contrôle au niveau des paquets IP
 - 2 politiques: Opt-in & Opt-out

Sauvegarder ses données importantes

- Pourquoi ?
- Copie de sauvegarde sur un support physique indépendant du support de l'original
- Matériel informatique fragile: les données stockées sont sujettes à effacement
- Le temps joue contre nous car:
 - Les techniques de stockage ne sont pas garanties contre le vieillissement
 - Les formats de fichier changent

Sauvegarder ses données importantes

- 2 catégories
 - Sentimentales
 - Utiles et dont le remplacement est coûteux
- Argument pour faire des sauvegardes
 - Estimer le temps nécessaire pour reconstituer les données perdues

Quels fichiers sauvegarder ?

- Les fichiers dont on ne possède pas de double
- « documents »
 - Bureautiques
 - Gestion
 - Artistiques
 - Courrier électronique, carnet d'adresses

Quel support ?

- Coût du support
- Volume des données
 - Clé USB
 - Disque dur externe
- Facilité de restauration
- Longévité des sauvegardes ?
- Fréquence
- Logiciel de sauvegarde (zip, rar, gzip, tar)

A2

Chapitre 4

La protection des données confidentielles

Protection des données confidentielles

- Partie A: La loi informatique et libertés
- Partie B: La Loi pour la Confiance en l'Economie Numérique (LCEN)
- Partie C: La cryptologie
- Partie D: La signature électronique
- Partie E: Le SPAM

La loi « informatique et libertés »

- Talleyrand:
 - La vie privée doit être murée, il n'est pas permis de chercher et de faire connaître ce qui se passe dans la maison d'un particulier
- Événements inquiétants:
 - Numéro INSEE utilisé par l'administration fiscale
 - Fichier de la police
 - Numéro de série du PentiumIII
 - Enregistrement dans Windows XP
 - Tatouage des documents Office

La loi « informatique et libertés »

- Années 1970, projets de grande envergure visant à ficher les individus sur supports magnétiques
- Projet SAFARI: interconnexion des fichiers des services publics avec création du numéro INSEE
- Création de la Commission Nationale de L'Informatique et des Libertés (CNIL)
- Loi du 6 janvier 1978.

Le texte, article 1

- **Extrait:**
 - « 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 l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques »

Quelques articles (1/3)

- Article 2
 - Définit précisément ce qu'est une donnée personnelle ainsi que les traitements qui s'y appliquent
- Article 6
 - Définit la manière dont les données à caractère personnel peuvent être traitées
- Article 7
 - Un traitement de données à caractère personnel doit avoir reçu le consentement de la personne concernée

Quelques articles (2/3)

- Article 8
 - Il est interdit de collecter des informations sur les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses, la santé ou la vie sexuelle des personnes
- Articles 11 à 31
 - Définit le rôle et le fonctionnement de la CNIL
- Articles 32 à 37
 - Devoirs des responsables effectuant le traitement de données

Quelques articles (3/3)

- Articles 38 à 43
 - Droits des personnes objet d'un traitement de données à caractère personnel
 - Être informé
 - S'opposer au traitement
 - Accès aux données collectées
 - Rectification des données
- Articles 45 à 52
 - Sanctions prises par la CNIL et sanctions pénales

La LCEN

- Loi du 21 juin 2004 pour la Confiance en l'Economie Numérique
- Faits déclencheurs:
 - Responsabilité des hébergeurs
 - Lutte contre le SPAM
 - Libéralisation de la cryptographie
 - Commerce électronique

Le texte, articles 1 et 2

- Article 1:
 - « La communication au public par voie électronique est libre ... »
- Article 2:
 - « On entend par communications électroniques les émissions, transmissions ou réceptions de signes, de signaux, d'écrits, d'images ou de sons, par voie électromagnétique. ... »

Cas traités par l'article 6

- Commerce électronique
 - Activité économique par laquelle une personne propose ou assure à distance et par voie électronique la fourniture de biens ou de services.
- Publicité par voie électronique
- Fournisseurs d'Accès à Internet (FAI)

LCEN et FAI

- Tant qu'un FAI n'est pas au courant de l'existence d'un contenu illicite sur son site, il n'est pas responsable de ce contenu
- Dès qu'il en a la connaissance, il devient responsable et il doit retirer ce contenu ou rendre son accès impossible.
- Un FAI doit conserver les données pendant au moins un an.
- Un FAI est responsable en matière de droits d'auteur

LCEN et publicité

- Article 20
 - Une publicité doit être identifiée comme telle, et rendre clairement identifiable la personne physique ou morale pour laquelle elle est réalisée.

LCEN et Signature électronique

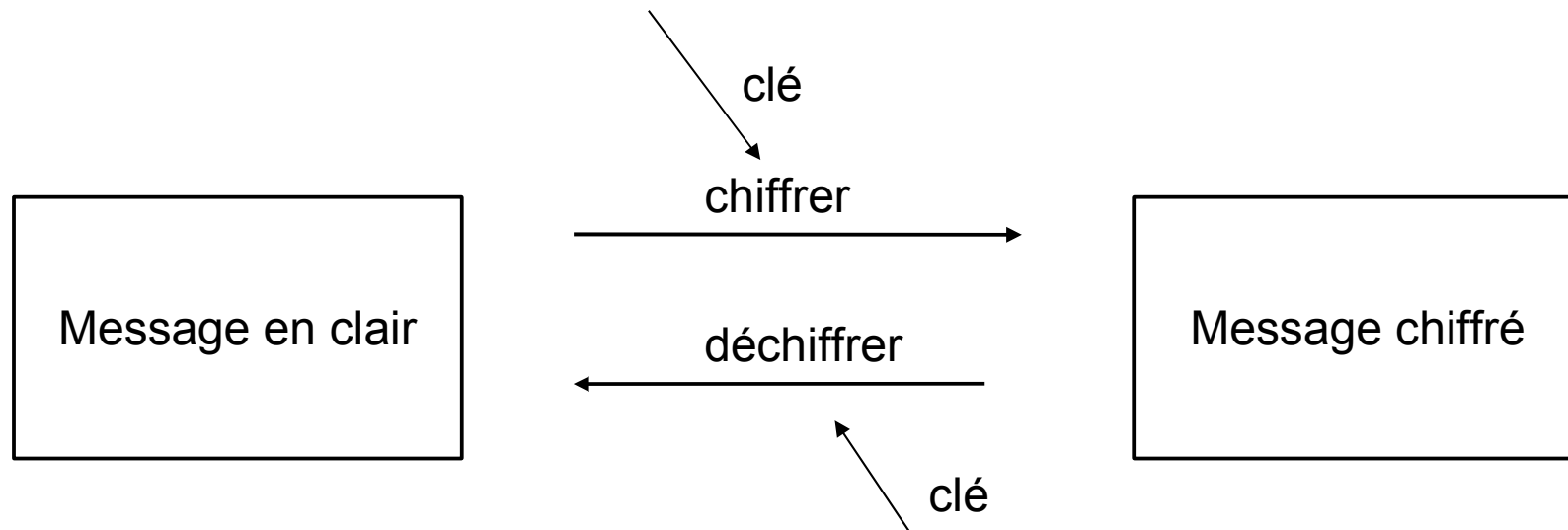
- Procédé permettant donner les mêmes garanties à un texte électronique que les garanties données par une signature papier sur un texte papier.
- La signature électronique légalisée par la LCEN rendre possible le commerce électronique dans un cadre légal.

LCEN et cryptologie

- Article 29:
 - Définition
- Article 30
 - La cryptologie dans le but d'authentifier ou de contrôler l'intégrité est libre
 - Corollaire: la cryptologie en général n'est pas libre
- Article 39
 - L'utilisation de la cryptologie dans le but de la défense nationale est autorisée

Cryptologie (définition)

- Utilisée pendant la guerre par les services secrets, centrale pour la sécurité informatique
- Science étudiant les moyens de chiffrer les informations ou de les déchiffrer



Cryptologie (vocabulaire)

Chiffrement: avec une clé, transformer le message en clair en un message chiffré

Déchiffrement: avec une clé, transformer le message chiffré en un message en clair

Décryptage: sans clé, transformer le message chiffré en un message en clair

Cryptographie à **clés symétriques:** la clé de chiffrement = la clé de déchiffrement

Cryptologie (clés publiques)

- Point faible: la transmission des clés de chiffrement et déchiffrement
- RSA: La cryptologie à clés publiques
 - Chaque utilisateur possède une clé de chiffrement publique et une clé de déchiffrement privée
 - Réduction du problème de transmission de clés
 - La clé privée et la clé publique sont complémentaires mais le calcul de la clé privée à partir de la clé publique est impossible, voire très difficile

Cryptologie (exemple)

- Bob veut envoyer un message secret à Alice.
- Il prend connaissance de la clé publique de Alice
- Il chiffre son message avec cette clé
- Il envoie le message chiffré à Alice
- Alice le reçoit
- Alice déchiffre le message avec sa clé privée
- Elle est la seule à pouvoir le faire

Cryptologie (les acteurs)

- Les **marchands** qui veulent faire du commerce électronique: signer les contrats et protéger les moyens de paiements (n° de carte bleue, mots de passe, etc).
- Les **citoyens** qui veulent garder leur vie privée privée.
- L'**état** qui veut surveiller les citoyens, empêcher le terrorisme, et développer sa défense.

Internet et la cryptologie

- Courrier électronique: pour les citoyens, certains messages doivent être chiffrés; pour les entreprises, tous les contrats doivent être chiffrés.
- IP est le protocole utilisé sur Internet permettant de faire suivre un message (router un message) depuis son émetteur vers son destinataire: il ne prévoit pas de chiffrement.

Comment avoir des clés ?

- Certificat = (clé publique, clé privée)
- Créé et envoyé par des organismes de certification
- Le problème de transmission des clé est réduit mais pas totalement résolu

La signature électronique

- Mécanisme électronique attaché à un fichier électronique donnant à l'auteur du fichier les mêmes droits et devoirs que ceux donnés à l'auteur d'un document papier signé par lui.
- Droits et devoirs de la signature papier:
 - Paternité du document: preuve que l'on est bien l'auteur du document
 - Intégrité du document signé
 - Indissociabilité de la signature et du document signé

Signature électronique (exemple 1/2)

- Alice veut envoyer le message $M1 = \text{« Bob je t'aime. Alice »}$ signé à Bob. Elle veut que ce message soit chiffré et elle veut prouver que c'est bien elle qui a envoyé le message.
- Elle chiffre le message avec sa clé privée ce qui donne $M2$.
- Elle crée le message $M3 = M1 + M2$
- Elle chiffre ce message avec la clé publique de Bob, ce qui donne $M4$

Signature électronique (exemple 2/2)

- Bob reçoit M4. Bob déchiffre M4 avec sa clé privée et obtient M3.
- Il constate que $M3=M1+M2$ avec $M1=$ « Bob, je t'aime. Alice » et M2 chiffré. Il pense que Alice est l'auteur du message mais il n'en a pas la preuve.
- Il déchiffre M2 avec la clé publique de Alice et obtient M1 donc il a la preuve que Alice a envoyé le message.

Le SPAM et la loi (1/3)

- L'adresse électronique est une donnée à caractère personnel...
- ... possédant une valeur marchande.
- Pour un marchand, connaître une adresse électronique est bien, savoir qu'elle correspond à une personne réelle lisant et envoyant du courrier est mieux!

Le SPAM et la loi (2/3)

- SPAM = Spice Pork And Meat (Film des Monty Python)
- SPAM = message publicitaire non sollicité
- Envahit les boîtes aux lettres
- Le droit en France: il est interdit d'envoyer du courrier électronique publicitaire de manière automatisée

Le SPAM et la loi (3/3)

- Deux approches de gestion du SPAM
- Opt-in ou Opt-out
- Opt-in (= accepter): pour recevoir des messages publicitaires, l'utilisateur doit accepter; par défaut il ne reçoit rien.
- Opt-out (= refuser): pour ne pas recevoir des messages publicitaires, l'utilisateur doit refuser; par défaut il reçoit du SPAM.
- Opt-in est légal; Opt-out est illégal.

A2

Chapitre 5

La loi sur la création et la protection des oeuvres

Protection des oeuvres

- La législation sur l'information est liée à la protection d'une oeuvre de création de l'esprit et se rattache à la notion de **propriété intellectuelle**.
- Pays anglo-saxons: législation du **copyright**
- Europe: législation du **droit d'auteur**

Propriété intellectuelle

- Le code de la propriété intellectuelle est celui qui encadre le droit d'auteur.
- Il se décompose en deux parties:
 - La propriété littéraire et artistique (droit d'auteur)
 - La propriété industrielle (brevet, etc)

Oeuvres de l'esprit

- Livre, écrits littéraires, artistiques ou scientifiques,
- Conférences, allocutions, sermons, plaidoiries,
- Ouvres dramatiques, chorégraphiques,
- Compositions musicales,
- Oeuvres cinématographiques et audiovisuelles,
- Dessins, peintures, sculptures, gravures,
- Photographies, illustrations, cartes, plans croquis,
- Logiciels et documents associés.

Droit d'auteur

- Le droit d'auteur est composé de deux parties
 - Droit moral
 - Droit patrimonial
- Droit moral:
 - Permet de revendiquer la paternité de son oeuvre
- Droit patrimonial
 - Permet de retirer des bénéfices de son oeuvre,
 - Exploitation et diffusion de l'oeuvre.

A2

Chapitre 6

Les chartes d'utilisation et de bon comportement

Chartes

- Les chartes d'utilisation et de comportement ont pour but de fixer les règles liées à l'usage des TICs.
- Elles s'adressent directement aux usagers.
- Elles constituent le règlement d'une organisation, le guide du bon usage
- Elles rappellent l'existence de la loi
- Les Universités ont une charte particulières ou par défaut: la charte RENATER

Charte RENATER

- Charte par défaut du REseau NAtional de télécommunications pour la Technologie, l'Enseignement et de la Recherche.
- Utilisation pour l'enseignement et la recherche
- Utilisation rationnelle, loyale
- Mise à disposition de données licites
- Pas d'accès à des tiers non autorisés.

La Netiquette

- Netiquette = Etiquette des réseaux
- Charte de bon comportement établie par l'ETF (Internet Engineering task Force) en 1996.
- Extraits
 - Cf doc C2IMES...