

Formation au C2i®

A2 : Intégrer la dimension éthique et le respect de la déontologie

Auteur :
Dominique Maniez
Université Lyon 2

Avec le concours de :
Angélique Froger
Université d'Avignon et des Pays de Vaucluse

Module développé dans le cadre du projet C2IMES 2005,
Certification Informatique et Internet
Mutualisée pour l'Enseignement Supérieur
Version en ligne : www.c2imes.org
Edition : C2IMES, projet.c2imes.org
Scenarisateur : Angélique Froger
Version : 1.0





SOME RIGHTS RESERVED

Publié sous Licence Creative Commons "By-NonCommercial-ShareAlike"
- http://creativecommons.org/licences/by-nc-sa/2.0/ -
Remarque importante : "Vous n'avez pas le droit d'utiliser ce document à des fins commerciales sans l'autorisation préalable de l'auteur"

Décembre 2005

Table des matières

Présentation du module..... 7

Chapitre I. Introduction au module..... 9

Partie A. Les droits fondamentaux de l'Homme et Internet..... 9

1. Quels rapports entre les droits fondamentaux et Internet?..... 9

Partie B. Le droit et l'informatique..... 11

Préambule..... 11

Pour aller plus loin..... 13

Chapitre II. La maîtrise de son identité numérique..... 15

Préambule..... 15

Partie A. L'identité sur Internet..... 16

1. La notion d'identité sur Internet..... 16

2. Les solutions pour se protéger..... 16

Partie B. Les traces sur Internet..... 17

Préambule..... 17

1. Les cookies..... 17

2. Les espiogiciels..... 21

3. Autres catégories de malwares (ou codes malveillants)..... 27

4. Autres techniques d'espionnage..... 29

Partie C. Les traces sur logiciels..... 30

Préambule..... 30

1. Présentation..... 31

2. Comment supprimer quelques traces ?..... 32

3. Un mouchard dans les fichiers Word et Excel..... 32

Ressources..... 34

Chapitre III. La sécurisation des informations sensibles..... 35

Partie A. Les dangers d'Internet..... 35
1. Les virus et macro-virus informatiques..... 35
2. Les vers..... 36
3. Les canulars (hoax)..... 36
4. Les chevaux de Troie..... 37
5. "Les portes dérobées"..... 39
6. Le phishing..... 41

Partie B. Le piratage informatique..... 42
1. Les hackers..... 42
2. Illustration : les dangers du mail-bombing..... 44

Partie C. Notions de sécurité..... 44
Préambule..... 44
1. Contrôle d'accès, bon usage des mot de passe et login..... 45
2. Les outils de protection..... 46
3. Sécurisation du réseau : les pare-feux..... 47

Partie D. Sauvegarder ses données importantes..... 49
1. Pourquoi faut-il sauvegarder ?..... 49
2. Méthodologie des sauvegardes..... 50
3. Logiciels de sauvegarde..... 54

Ressources..... 55

Chapitre IV. La protection des données confidentielles..... 57

Partie A. La loi "Informatique et libertés"..... 58
1. Contexte et problématique..... 58
2. Le texte de la loi du 6 janvier 1978..... 60

Partie B. La LCEN..... 66
1. Principes..... 66
2. Le texte de la LCEN..... 66

Partie C. La cryptologie..... 72
Préambule..... 72
1. Présentation..... 73
2. Pourquoi utiliser la cryptologie ?..... 74
3. Pourquoi crypter ses courriers électroniques ?..... 76
4. Méthodes de cryptage de ses courriers électroniques..... 78
5. Le cryptage des fichiers..... 79

Partie D. La signature électronique. 79
Préambule. 79
1. Modifications législatives. 80
2. La certification numérique. 81
3. La signature numérique. 83
Partie E. Le SPAM et la loi. 86
1. L'adresse électronique.... 86
2. Les aspects juridiques du spamming. 87
3. Conseils pratiques. 90
4. Organismes de régulation et de lutte contre le spamming. 92
Ressources. 93

Chapitre V. La loi sur la création et la protection des oeuvres. 95

Les bases législatives. 95
Partie A. La propriété intellectuelle. 95
1. Principes. 95
2. Que sont les "oeuvres de l'esprit" ?. 96
Partie B. Le droit d'auteur. 97
1. Principes. 97
2. Droit d'auteur, copie privée et P2P. 98
Ressources. 100

Chapitre VI. Les chartes d'utilisation et de bon comportement. . . . 103

Internet, un autre monde ?. 103
Partie A. Les chartes. 104
1. Définition et principes. 104
2. Les établissements universitaires et les chartes. 104
Partie B. La charte RENATER. 105
1. Présentation et principes. 105
2. Liste des infractions. 105
Partie C. La netiquette. 106
1. Présentation et principes. 106
2. Respecter la loi. 107
3. Extraits de la netiquette. 108
Partie D. Illustrations et exemples de chartes. 109
1. Chartes d'établissement. 109
2. Règles de conduite dans un forum de discussion. 109

Pour aller plus loin.... 110
Conclusion. 111
Bibliographie. 113
Annexes. 115

Préambule

Présentation du module

Objectifs pédagogiques de ce module

Dans la mesure où *nul n'est censé ignorer la loi*, toute personne utilisant un ordinateur se doit de connaître les grands principes du droit de l'informatique, de la même manière que tout usager de la route (qu'il soit piéton, conducteur de deux roues ou automobiliste) a l'obligation de connaître le code de la route.

Le droit de l'informatique n'est donc pas une science à réserver aux juristes, mais *il doit être compris et assimilé par tous les utilisateurs de l'outil informatique*.
A noter également que connaître et appliquer le droit de l'informatique ne suffit pas pour autant : il faut également *apprendre les règles de bon usage qui sont en vigueur sur Internet*.

L'objectif de ce module de formation est donc de :

- vous transmettre les grands principes du droit de l'informatique ;
- vous sensibiliser aux problématiques juridiques relatives à l'usage des nouvelles technologies ;
- vous permettre de prendre connaissance des règles régissant les relations et les échanges sur Internet.

En tant qu'internaute et usager des technologies de l'information et de la communication, il est important que vous ayez connaissance de vos droits afin de les faire valoir et de ceux d'autrui afin de les respecter.

Plan

Comment atteindre cet objectif ?

Au travers de 6 chapitres, ce module vous propose d'aborder les thématiques et problématiques suivantes, vous permettant d'acquérir les connaissances juridiques relatives à l'usage des TICs :

- **Chapitre 1**

  Introduction au module qui présente les bases de votre réflexion sur les droit fondamentaux de l'Homme et l'informatique ;

- **Chapitre 2**

  La maîrise de son identité numérique sur le Web ;

- **Chapitre 3**

  La sécurisation des données sensibles ;

- **Chapitre 4**

  La protection des données confidentielles ;

- **Chapitre 5**

  La loi sur la création et la protection des oeuvres ;

- **Chapitre 6**

  Les chartes d'utilisation de bon comportement.

Infos sur le module

- **Temps d'apprentissage estimé**

  Environ 3 heures.

- **Niveau de difficulté**

  De débutant à intermédiaire.

- **Navigation et mode de lecture**

  Ce module transversal traitant de problématiques en relation directe avec l'ensemble des autres modules du dispositif (du B0 au B7), vous pouvez prendre connaissance de cette ressource dans l'ordre dans lequel vous êtes amenés à découvrir les autres composants du dispositif, soit au fur et à mesure de votre progression dans votre formation au C2i.

  Vous pouvez ainsi consulter les chapitres de ce module dans l'ordre que vous désirez.

  Pris individuellement, nous vous recommandons de suivre ce module en respect du scénario pédagogique mis en oeuvre.

Chapitre

I

Introduction au module

Partie A. Les droits fondamentaux de l'Homme et Internet

1. Quels rapports entre les droits fondamentaux et Internet?

L'informatique a toujours eu des rapports conflictuels avec le droit et il y a plusieurs raisons à ce phénomène.

1. La première difficulté est que la *technologie évolue beaucoup plus vite que le droit*, si bien que ce dernier a du mal à s'adapter aux mutations informatiques. Pour ne prendre qu'un seul exemple, l'émergence des réseaux d'échanges peer-to-peer (P2P) qui permettent à des internautes de partager des fichiers (notamment de la musique et des films) a pris de court la justice qui a mis un certain temps à réagir. Pourtant, les premières lois réglementant l'informatique sont relativement anciennes et la France a compris assez tôt qu'il fallait légiférer sur le sujet. À cet égard, la *loi Informatique et libertés du 6 janvier 1978* constitue un élément fondamental du dispositif législatif qui encadre le droit de l'informatique.
2. Le deuxième écueil est que le *droit de l'informatique est par nature complexe* si bien que les utilisateurs d'ordinateurs ne font pas toujours la différence entre ce qui est permis et ce qui est interdit. Si les internautes qui téléchargent illégalement de la musique ont la plupart du temps bien conscience de commettre un délit, en revanche ceux qui collectent des adresses électroniques sans le consentement de leur propriétaire n'ont en général absolument pas le sentiment de commettre une infraction.

On en arrive donc à un double constat d'échec : *le droit de l'informatique est méconnu et finalement peu appliqué au regard des nombreuses infractions qui sont commises quotidiennement.*
Cette relative impunité a d'ailleurs accrédité la thèse qu'Internet constituait une zone de non droit et qu'aucune législation ne pouvait s'appliquer au réseau des réseaux en raison notamment de son caractère transfrontalier. Bien évidemment, cette thèse est erronée même s'il faut bien reconnaître que l'application de certaines lois sur Internet pose problème.



Attention
Pourtant, dans la mesure où *nul n'est censé ignorer la loi*, toute personne utilisant un ordinateur se doit de connaître les grands principes du droit de l'informatique, de la même manière que tout usager de la route (qu'il soit piéton, conducteur de deux roues ou automobiliste) a l'obligation de connaître le code de la route. Le droit de l'informatique n'est donc pas une science à réserver aux juristes, mais il doit être compris et assimilé par tous les utilisateurs de l'outil informatique.



Remarque
Connaître et appliquer le droit de l'informatique ne suffit pas pour autant : il faut également *apprendre les règles de bon usage qui sont en vigueur sur Internet.*
La toile étant par essence un lieu de partage d'idées, il s'y crée de nombreuses communautés virtuelles qui possèdent des règles de savoir-vivre qu'il convient de ne pas ignorer. La lecture et le respect des chartes d'utilisation en vigueur sur Internet sont le minimum que l'on doit attendre de tout internaute.

Internet est aussi un véritable paradoxe en matière de droits car il se révèle bénéfique pour l'exercice des droits de l'homme et bafoue à la fois certains droits de la personne privée.



Exemple
Par exemple, Internet est un fantastique outil de communication et d'information qui permet à certains citoyens de pays peu démocratiques de déjouer la censure. Dans ce cas-là, c'est la liberté d'expression qui triomphe et l'article 19 de la Déclaration universelle des droits de l'homme qui stipule que *"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" (Article 19 de la Déclaration universelle des droits de l'Homme.)* est finalement respecté grâce à Internet.
En revanche, cette liberté d'expression peut également être dévoyée et servir à la transmission de propos injurieux, racistes, xénophobes ou haineux. De la même manière, le respect de vie privée ou du droit d'auteur sont très souvent mis à mal sur Internet.



Complément
Sur la thématique des droits fondamentaux des droits de l'Homme et Internet, nous vous conseillons de consulter la section juridique d'Educnet.

Partie B. Le droit et l'informatique

Préambule

Nous ne le répéterons jamais assez : *Internet n'est pas une zone de non droit* et il existe désormais de nombreuses lois françaises, européennes et internationales qui encadrent la pratique de l'outil informatique.

Il y a par conséquent *un risque juridique réel à utiliser un ordinateur en méconnaissant les lois traitant de l'informatique* dont l'expérience montre qu'elles sont très mal connues ; cette méconnaissance de la loi pose de nombreux problèmes et nous allons donc tenter de faire un survol rapide de toutes les lois qu'il faut absolument connaître, si ce n'est par coeur, du moins dans les grands principes, afin d'améliorer votre sécurité juridique quand vous utilisez un ordinateur.
Si le droit de l'informatique a pu paraître balbutiant au début des années 1980, l'arsenal juridique s'est étoffé au fil des ans, les avocats et les juristes se sont formés et on commence aujourd'hui à avoir une jurisprudence conséquente.
Dans la pratique, connaître la loi permet :

- de vous empêcher de commettre une infraction ;
- de demander réparation en justice si vous êtes victime d'une infraction.

Le code pénal est divisé en livres.

Dans le troisième livre qui est consacré aux crimes et délits contre les biens, le chapitre III du Titre II traite des *atteintes aux systèmes de traitement automatisé de données*.
Voici le texte intégral des 7 articles qui composent ce chapitre :

Article 323-1

- Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 30000 euros d'amende.
- Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 45000 euros d'amende.

Article 323-2

Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de cinq ans d'emprisonnement et de 75000 euros d'amende.

Article 323-3

Le fait d'introduire frauduleusement des données dans un système de traitement automatisé ou de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 75000 euros d'amende.

Article 323-3-1

Le fait, sans motif légitime, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3 est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée.

Article 323-4

La participation à un groupement formé ou à une entente établie en vue de la préparation, caractérisée par un ou plusieurs faits matériels, d'une ou de plusieurs des infractions prévues par les articles 323-1 à 323-3-1 est punie des peines prévues pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée.

Article 323-5

Les personnes physiques coupables des délits prévus au présent chapitre encourent également les peines complémentaires suivantes :

1. L'interdiction, pour une durée de cinq ans au plus, des droits civiques, civils et de famille, suivant les modalités de l'article 131-26 ;
2. L'interdiction, pour une durée de cinq ans au plus, d'exercer une fonction publique ou d'exercer l'activité professionnelle ou sociale dans l'exercice de laquelle ou à l'occasion de laquelle l'infraction a été commise ;
3. La confiscation de la chose qui a servi ou était destinée à commettre l'infraction ou de la chose qui en est le produit, à l'exception des objets susceptibles de restitution ;
4. La fermeture, pour une durée de cinq ans au plus, des établissements ou de l'un ou de plusieurs des établissements de l'entreprise ayant servi à commettre les faits incriminés ;
5. L'exclusion, pour une durée de cinq ans au plus, des marchés publics ;
6. L'interdiction, pour une durée de cinq ans au plus, d'émettre des chèques autres que ceux qui permettent le retrait de fonds par le tireur auprès du tiré ou ceux qui sont certifiés ;
7. L'affichage ou la diffusion de la décision prononcée dans les conditions prévues par l'article 131-35.

Article 323-6

Les personnes morales peuvent être déclarées responsables pénalement, dans les conditions prévues par l'article 121-2, des infractions définies au présent chapitre.

Les peines encourues par les personnes morales sont :

1. L'amende, suivant les modalités prévues par l'article 131-38 ;
2. Les peines mentionnées à l'article 131-39.

L'interdiction mentionnée au 2º de l'article 131-39 porte sur l'activité dans l'exercice ou à l'occasion de l'exercice de laquelle l'infraction a été commise.

Article 323-7

La tentative des délits prévus par les articles 323-1 à 323-3-1est punie des mêmes peines.



Remarque

Il faut d'abord préciser que *tous ces articles ont été modifiés par la loi du 21 juin 2004 pour la confiance dans l'économie numérique, baptisée LCEN*. Ces articles existaient pratiquement tous avant le vote de la LCEN, mais toutes les peines (durée et montant) ont pratiquement été doublées, signe manifeste de la volonté du législateur.

Le dernier article, 323-7, est lui-même assez dissuasif car *la tentative de commettre un délit est punie exactement des mêmes peines. En clair, si vous tentez de pirater une machine, mais que vous êtes un mauvais hacker, vous écoperez de la même peine que si vous y réussissez.*

En conclusion...

En conclusion, on peut dire que *la législation a été terriblement durcie* et qu'il vaut mieux éviter de jouer avec le feu.

Nous pensons notamment à tous ceux que les hackers appellent des script-kiddies qui sont des gamins qui trouvent des logiciels malveillants prêts à l'emploi sur Internet et s'amusent avec.

Si un adolescent récupère sur Internet un kit de construction de virus (il en existe plusieurs) et crée en quelques minutes une variante d'un virus, il risque très gros à diffuser sa création. Le risque est d'autant plus grand que les script-kiddies ne sont pas en général de grands informaticiens et ont donc toutes les chances de se faire prendre car ils ne sauront pas maquiller leurs traces.

Pour aller plus loin...



Site présentant une sélection de textes officiels français, européens et internationaux relatifs au domaine général de la communication et à certaines activités proposées sur l'internet : cliquez ici.

L'ensemble des dispositions contenues au sein de ces textes n'ont pas nécessairement vocation à s'appliquer à l'internet.



- Textes internationaux (traités et conventions).
- Textes européens (directives, règlements, communications).
- Textes nationaux (codes, lois, règlements, rapports et avis).

Chapitre

II

La maîtrise de son identité numérique

Préambule

L'imagination des développeurs de logiciels malveillants semble sans limite et leurs auteurs exploitent la moindre faille du système qu'ils peuvent trouver. Internet, en passant du statut d'outil destiné à la communauté universitaire à celui de média grand public, a attisé la convoitise de tous les escrocs qui cherchent à profiter de la manne que représentent les millions d'utilisateurs qui surfent sur le réseau des réseaux.

Les motivations des créateurs de ces logiciels sont bien évidemment identiques à celles des auteurs de virus, à ceci près qu'il existe généralement en plus une volonté criminelle et non pas simplement destructrice. Un créateur de virus recherche souvent une certaine forme de reconnaissance en montrant au monde (en tous cas, à ceux qui utilisent un ordinateur) qu'il est le plus intelligent et qu'il a su déjouer les mesures de sécurité.

Il y a en revanche presque toujours une motivation criminelle derrière un logiciel malveillant : l'auteur du malware veut prendre le contrôle de la machine de l'utilisateur pour lui voler des informations ou bien lui extorquer de l'argent. Là où le virus se montrait voyant du fait de sa prolifération exponentielle, le malware cherche à se faire discret et reste furtif.



Remarque

Il y a toujours un côté désespérant, quand on a goûté aux joies de l'informatique, à constater que des individus peuvent mettre leur intelligence au service de la création de logiciels malveillants.

Cela étant, on ne voit pas très bien pourquoi l'informatique serait épargnée par cette loi qui gouverne le monde et qui veut que l'être humain est capable du meilleur comme du pire.

Il faut toujours garder à l'esprit que les ordinateurs et les logiciels sont faits par des humains. On a parfois la très nette impression que, face à la puissance de certaines applications, l'utilisateur a tendance à oublier cette vérité première et à considérer que l'informatique est une science surnaturelle. On pourrait peut-être même aller jusqu'à dire que les problèmes de sécurité viennent en grande partie de cette absence de prise de conscience de la réalité. La plupart des utilisateurs d'ordinateurs ne voient pas le danger qu'il y a à exécuter un programme dont l'origine est douteuse alors qu'il ne leur viendrait absolument pas à l'esprit de garer leur voiture dans un parking public en laissant les clés sur le tableau de bord.

Partie A. L'identité sur Internet

1. La notion d'identité sur Internet

Protégé derrière son ordinateur, l'internaute croit souvent qu'#il est totalement anonyme quand il surfe sur Internet. En fait, il n#'en est rien et toutes les activités liées à l#'usage d#'Internet génèrent toute *une série de traces* qui permettent d'*#identifier assez facilement l#'utilisateur*d#'un ordinateur. *L#'anonymat sur Internet relève donc plus du mythe que de la réalité*.

D#'autre part, il est parfois important d#'arriver à *prouver son identité sur Internet*, que ce soit pour acheter un livre en ligne, consulter son compte en banque ou bien encore télédéclarer ses impôts. Au final,chaque fois qu#'il faut prouver son identité, on aura recours, par un moyen ou un autre, à la *cryptographie*.
Petit à petit, l#'usage d#'Internet se renforçant, se développe le concept d'#identité numérique.



Explication

Par *identité numérique*, on entend *tous les moyens (logiciels ou matériels) qui permettent d#'identifier de manière fiable et unique une personne*. La plupart du temps, l'#identité numérique prend la forme du couple de données que sont l'*#identifiant* et le *mot de passe*.
Ces deux informations permettent d'#accéder, par exemple, à un service de Webmail, à un espace de travail collaboratif ou bien encore à son dossier de scolarité en ligne.

2. Les solutions pour se protéger



Les conseils relatifs à l'usage de l'adresse électronique

- Utiliser une adresse différente pour chaque activité ;
- Utiliser des adresses gratuites lorsque l'on veut être anonyme.



Les conseils quant à la navigation Web
Utiliser des navigateurs sécurisés qui permettent de limiter les informations diffusées à votre sujet...par conséquent, il est fortement conseillé d'éviter l'usage d'Internet Explorer.

Partie B. Les traces sur Internet

Préambule

Quelle que soit votre activité sur Internet (messagerie, navigation, chat,etc.), vous laissez des traces de votre passage.

D'un point de vue technique, dès que vous êtes connecté au réseau Internet, votre fournisseur d'accès vous attribue un *identifiant unique* appelé *adresse IP*. Cette information est une suite de quatre nombres séparés par des points, par exemple, *80.10.246.157*.
Chaque internaute possède donc une adresse IP unique et cette adresse est *systématiquement enregistrée* dès que vous vous livrez à une quelconque activité sur Internet.



Exemple
Par exemple, l'adresse IP de votre ordinateur figure dans chaque courrier électronique que vous envoyez.



Remarque :
Un texte législatif récent oblige les fournisseurs d'accès à *stocker pendant un an toutes les données relatives à vos connexions à Internet*.



Complément
Pour vous donner un aperçu de toutes les informations que vous diffusez sans vous en rendre compte quand vous naviguez sur le Web, nous vous conseillons de vous rendre sur le site de la CNIL où un programme liste vos traces : http://www.cnil.fr/index.php?id=19

1. Les cookies

1.1. Que sont les cookies et à quoi servent-ils ?



Qu'est-ce qu'un cookie ?
En informatique, les *cookies* ne sont pas des petits gâteaux secs, mais des fichiers qu'un serveur Internet peut vouloir stocker sur votre machine afin de mémoriser vos préférences de consultation et, ainsi, vous reconnaître la prochaine fois que vous vous connecterez à ce site.

Un cookie se présente sur votre disque dur sous la forme suivante :



▲ IMG. 1 : EXEMPLE DE COOKIE

Son contenu est constitué de diverses informations, incompréhensibles pour l'utilisateur, qui se présentent par exemple ainsi :

Exemple
FindLawTP
TOMPA-www-3-62.23.165.210-28061-1019201344-798759-112-APMOT
findlaw.com/
0
1520984064
29558341
3040740160
29484915
*

1.2. A quoi servent les cookies ?

Pour un serveur Web, rares sont les éléments qui vous distinguent des autres visiteurs. Les cookies permettent justement de "reconnaître" le visiteur en recueillant un certain nombre d'éléments d'identification :

- l'*adresse IP* ;
- le *système d'exploitation* et le *navigateur utilisés* ;
- surtout des *informations statistiques* comme les pages consultées, le nombre de visites, les actions effectuées sur le site, bref les habitudes de consultations.

Exemple 1
Les cookies permettent au serveur sur lequel on effectue des achats de "retenir" les produits que l'on a placés dans son cadi virtuel et de nous les présenter sur la facture finale.

Exemple 2
Certains forums de discussion sur le Web peuvent reconnaître un utilisateur, grâce au cookie, et lui permettre de poster immédiatement une contribution sans qu'il ait besoin de réinscrire son identifiant, son adresse de courrier électronique et son mot de passe [dans les cas où ce dernier est requis].



Attention

Le cookie est également utile pour le commerçant et le publicitaire qui l'utilisent à des fins de marketing et peuvent ainsi adapter leurs annonces commerciales ou publicitaires à nos habitudes de navigations recueillies par le cookie.
Par exemple, si nous avons visités plusieurs fois la page d'un site de vacances consacrée aux séjours en montagne, le même site nous présentera automatiquement, lors d'un prochain passage sur d'autres pages, des promotions sur des randonnées dans les Pyrénées.

Dans la mesure où les cookies peuvent recéler des données à caractère personnel, certaines personnes pensent qu'ils peuvent être dangereux pour le respect de la vie privée. Les versions récentes des navigateurs intègrent donc une gestion des cookies et permettent notamment de refuser les cookies qu'un site Web voudrait déposer sur votre machine.

Si l'on fait une application stricte de la loi, un serveur Web désirant déposer sur votre machine un cookie doit au préalable vous en avertir afin que vous puissiez donner votre accord. Si l'on prend la peine de regarder les cookies qui sont déposés sur sa propre machine [il suffit pour cela de trouver le dossier intitulé Cookies qui est en général un sous-dossier du répertoire au nom de l'utilisateur], on ne peut que constater qu'il y en a beaucoup et que pratiquement aucun des sites ayant inscrit un cookie n'a demandé l'autorisation.



La *CNIL*, prenant sans doute acte de cette situation, rappelle dans son communiqué du 7 décembre 2001 ainsi que sur son site web que *"la plupart des cookies jouent le rôle de simples témoins de connexion destinés à faciliter la navigation sur un site web ou à sécuriser l'accès (à sa messagerie électronique par exemple) sans avoir à ressaisir des informations identifiantes."* .

* *
*

Le cookie personnalise donc et facilite la navigation de l'internaute en rappelant les préférences qu'il a pu déclarer lors d'une précédente visite sur un site (langue, identifiant, mot de passe, sélection d'objets, ...).

1.3. Comment gérér les cookies dans Internet Explorer ?



La plupart des navigateurs modernes offrent la possibilité aux internautes de bloquer l'inscription des cookies sur leur ordinateur.
Nous vous conseillons donc d'adopter cette attitude et éventuellement d'accorder votre confiance à quelques sites qui la méritent et nécessitent l'utilisation d'un cookie. Quant aux sites qui nécessitent un cookie, mais qui ne le précisent pas, nous pensons qu'il est légitime de les rayer de vos favoris.

1.4. Les cookies sont-ils légaux ?

Grâce à l'utilisation des cookies, les sociétés de marketing établissent des profils de consommation qu'elles revendent à des sociétés en quête de nouveaux clients. Certains juristes s'interrogent sur la légalité d'un tel dispositif au regard de la législation sur la protection des données à caractère personnel. Nous mentionnons ci-dessous quelques points de vue sur le sujet qui, s'ils ne font pas partie de la jurisprudence, n'en demeurent pas moins intéressants.

L'installation de cookies sur la machine de l'internaute à son insu peut être assimilé au fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données, activité qui est réprimée par le code pénal.



Extrait de texte légal

La *loi du 6 janvier 1978* interdit la collecte de données opérée par tout moyen déloyal ou illicite (*article 6*). L'utilisation de cookies pour collecter des données sur la navigation d'un internaute à son insu doit donc être considérée comme ne répondant pas aux critères de loyauté et de légalité.

La CNIL, sur son site Web, recommande d'ailleurs aux webmestres d'*informer les internautes de la finalité des cookies, de leur durée de validité* s'ils ne sont pas effacés à l'issue de la session et des conséquences de la désactivation de ces procédés.

La CNIL publie en outre des modèles de mise en garde à insérer par les gestionnaires de sites web dans une page documentant la charte relative au respect de la vie privée.



Complément

Il existe un modèle pour les cookies incluant des informations concernant la navigation du visiteur et un autre modèle pour les cookies incluant des informations fournies par le visiteur. Ces modèles peuvent être consultés en cliquant ici.

Ces deux modèles conseillent de faire figurer la mention « *Nous vous informons que vous pouvez vous opposer à l'enregistrement de cookies en configurant votre navigateur.* ». Force est de constater que très peu de sites Web utilisant des cookies prennent ces précautions oratoires...

En fait, les principales difficultés soulevées par l'usage Internet en ce qui concerne la protection des données personnelles sont liées à l'*absence de confidentialité*, à la *liberté totale de circulation de l'information*, et à la *difficulté d'appliquer les juridictions nationales sur un réseau par essence mondial*.

Illustration

Pour illustrer, s'il en était encore besoin, le manque total de confidentialité du réseau Internet, songez au fait que la *commande Ping* suivie d'un numéro d'adresse IP permet de savoir si une machine est connectée à Internet sans que son propriétaire soit averti de cette requête (la plupart des pare-feu permettent cependant de bloquer ce type de requête, mais très peu d'utilisateurs activent cette fonctionnalité).

2. Les espiogiciels

2.1. Que sont les espiogiciels ?



Espiogiciel est la traduction française du terme anglais *spyware*, *spy* en anglais signifiant « *espion* », que l'on peut donc traduire par « *logiciel espion* ». Les espiogiciels sont un phénomène d'apparition récente qui est en train de prendre une ampleur considérable.



Un espiogiciel est un programme qui rassemble des informations à l'insu de son utilisateur et les transmet à une organisation qui cherche à en tirer parti. En fait, on désigne sous le terme d'espiogiciel des programmes qui recueillent des informations telles que les sites web visités, les applications installées sur l'ordinateur, la version du navigateur et du système d'exploitation. Ces données permettent de dresser un profil commercial de l'utilisateur qui est surtout considéré comme un consommateur en puissance.



Remarque
On range habituellement sous le terme *spyware* une autre catégorie de logiciels appelés *adwares* [ad, en anglais, est l'abréviation de advertisement et signifie « publicité »] qui sont des programmes qui affichent de manière intempestive des informations de nature publicitaire.

Alors qu'un *spyware* est toujours furtif et agit sans le consentement de l'utilisateur, un *adware* peut, dans le meilleur des cas, demander l'autorisation de l'utilisateur et, bien souvent, avertir l'utilisateur de ses intentions en noyant cette information dans les clauses d'utilisation d'un logiciel freeware que personne ne lit jamais.

Bien que le principe de ces deux types de logiciels ne soit pas identique, tous ces programmes consacrent l'idée qu'Internet est aujourd'hui devenu un gigantesque espace marchand.

Si le fait qu'un logiciel récupère la version de votre navigateur et de votre système d'exploitation peut paraître assez bénin, le problème est que la majorité des espiogiciels ne se contentent pas de ce genre d'informations. En outre, il convient d'être intraitable sur les principes et de considérer qu'aucune donnée ne doit sortir de votre ordinateur sans votre consentement. *Les espiogiciels menacent donc la sécurité de votre système d'information et il convient dans ces conditions de les combattre par tous les moyens*.

Remarque :

Les espiogiciels sont fréquemment associés à des logiciels proposés en téléchargement gratuit sur l'internet, comme par exemple les logiciels d'échanges de fichiers peer-to-peer, mais également dans des produits phares de grands éditeurs.
On peut également compter au nombre de ces techniques les *web bugs* qui, le plus souvent à des fins de mesure d'audience, prennent la forme d'une image invisible et indétectable constituée d'un unique pixel inséré dans des pages ou courriers électroniques au format html. Ces derniers toutefois ne font pas l'objet d'une installation permanente sur les machines des utilisateurs concernés.

Ampleur du phénomène

Un fournisseur d'accès à Internet américain (*Earthlink*) et une société spécialisée dans la sécurité informatique (*Webroot*) ont uni leurs efforts au début de l'année 2004 pour tenter de mesurer l'ampleur du phénomène des espiogiciels en offrant aux internautes la possibilité de tester leur système grâce à un programme baptisé *Spy Audit*. La particularité de ce logiciel est qu'il s'installe et scanne votre ordinateur extrêmement rapidement.

Les résultats de l'étude de ces deux sociétés sont assez édifiants et méritent que l'on s'y arrête. Vous trouverez ci-dessous un tableau résumant les résultats de l'audit réalisé au cours des quatre premiers mois de l'année 2004 :

Résultats globaux	*Période du 1er Janvier au 30 Avril 2004*
Nombre d'ordinateurs analysés	1 483 517
Nombre de spywares trouvés	40 846 089
Moyenne des spywares trouvés par ordinateur analysé	27,5
Nombres adwares trouvés	7 642 556
Nombres de chevaux de troie trouvés	257 761

▲ TAB. 1 : RÉSULTATS D'AUDIT

Complément

Vous pouvez consulter l'ensemble de l'étude en cliquant ici.
Vous pouvez tester votre ordinateur en téléchargeant cet utilitaire en cliquant ici.
Une autre étude indique qu'en octobre 2004, 80 % des ordinateurs étaient infectés par des spywares. Pour la consulter, cliquer ici.

2.2. A quoi servent les espiogiciels ?

Véritables mouchards électroniques au même titre que les cookies mais aux fonctionnalités beaucoup plus étendues, ils peuvent envoyer dès le démarrage de l'ordinateur vers les serveurs d'un organisme "maître" toutes les données qu'ils ont collectées, comme les habitudes de navigation et les adresses de tous les sites visités, mais aussi la configuration exacte de l'ordinateur et le contenu de son disque dur permettant ainsi parfois de dénicher des adresses électroniques ou, plus gênant, des mots de passe !

L'objectif affiché par les éditeurs de ces logiciels est d'assurer une meilleure maintenance des programmes dans lesquels ils sont intégrés. La transmission de données comme la version utilisée, les programmes associés ou les erreurs rencontrées, permet en effet parfois d'envoyer automatiquement à l'utilisateur les mises à jour et correctifs indispensables au bon fonctionnement du programme principal.

Une autre pratique consiste également en la revente des données ainsi collectées à des régies publicitaires, des centrales d'achats ou des sociétés de marketing. Ces données constituent une ressource appréciable pour ces entreprises, la valeur de leurs fichiers et de leurs bases de données étant déterminée par la qualification et le profilage les plus précis possible des internautes listés.

L'espiogiciel est à cet effet la réponse la plus avancée à la culture de l'anonymat et du pseudonymat qui demeure encore aujourd'hui un des traits fondamentaux de l'identité sur internet. Les fonctions d'espionnage sont même parfois la rançon de la gratuité d'un logiciel : son concepteur l'offre librement en téléchargement mais se rémunère en contrepartie par la revente des informations recueillies.



Remarque

L'espiogiciel est à cet effet la réponse la plus avancée à la culture de l'anonymat et du pseudonymat qui demeure encore aujourd'hui un des traits fondamentaux de l'identité sur internet.

Les fonctions d'espionnage sont même parfois la rançon de la gratuité d'un logiciel : son concepteur l'offre librement en téléchargement mais se rémunère en contrepartie par la revente des informations recueillies.



Exemple

Par exemple, une disposition de la licence de téléchargement du logiciel d'échange de fichiers (peer-to-peer) KaZaA, qui a fait l'objet d'un procès aux Pays-Bas, signalait bien la présence d'un logiciel espion parmi les fichiers installés. Mais la taille des caractères et la formulation employée pour prévenir l'utilisateur ne délivraient pas une information véritablement claire.

Ce manque de transparence est bien entendu de nature à entacher la validité du consentement de l'utilisateur à la collecte de ses données personnelles.



Remarque

En marge des questions liée à la protection de la vie privée, il faut enfin remarquer que les espiogiciels mobilisent des ressources de l'ordinateur lorsqu'ils sont actifs en tâche de fond [mémoire disque, mémoire vive et bande passante pour les transmissions de données].

2.3. Mode diffusion et détection des espiogiciels

La plupart des espiogiciels sont intégrés à des logiciels freeware ou shareware[le paiement de la contribution est basé sur le volontariat]. Si l'espionnage est clairement avoué, on peut considérer qu'il s'agit d'une contrepartie à la gratuité puisqu'en notre bas monde, rien n'est vraiment gratuit.

Les programmes d'échange de fichiers (P2P), comme Kazaa, iMesh ou Go!Zilla, sont

de grands pourvoyeurs de spywares. D'autres logiciels comme Babylon Translator, GetRight, Download Accelerator ou Cute FTP en contiennent également. Il est bien difficile de trouver sur Internet une liste exhaustive des logiciels hébergeant un spyware, qu'il soit externalisé ou interne. On considère cependant que plus d'un millier de programmes contiendrait un espiogiciel.
Certains spywares s'installent parce que vous avez donné votre accord, mais certains programmes particulièrement insidieux, comme Comet Cursor ou Gator, se retrouvent sur votre ordinateur sans que vous n'ayez rien demandé.



Attention
Les spywares sont souvent difficiles à supprimer manuellement et ce n'est pas parce que vous supprimez le logiciel hôte que l'espiogiciel disparaîtra. Ainsi, la suppression de Kazaa de votre disque dur n'entraîne pas la suppression du logiciel Cydoor. En revanche, la suppression d'un spyware peut entraîner des dysfonctionnements dans le logiciel auquel il est lié. En clair, si vous désinstallez Cydoor, rien n'indique que Kazaa continuera à fonctionner normalement.



Remarque
Si vous avez donné votre consentement à l'installation d'un espiogiciel de type adware, il est normal de voir apparaître de temps en temps des bannières publicitaires. En revanche, si vous n'avez pas donné votre accord et que vous constatiez des comportements surprenants après l'installation d'un logiciel gratuit, vous devez soupçonner la présence d'espiogiciels sur votre ordinateur.

Voici une liste de symptômes qui sont révélateurs de la présence de spyware :

- La page d'accueil de votre navigateur a été modifiée.
- Des fenêtres publicitaires s'affichent que vous soyez ou non sur Internet.
- Une barre d'outils a été installée dans votre navigateur et vous n'arrivez pas à la supprimer.
- Votre ordinateur ralentit de manière inexpliquée.



Conseil
Si vous constatez de tels symptômes, vous devez vous procurer un outil qui permet de scanner votre disque dur afin de rechercher la présence de spywares. Dans la mesure où les espiogiciels ne sont pas des virus ni des chevaux de Troie, les antivirus classiques ne les détectent pas et il faut alors faire appel à une autre catégorie de programmes : les scanners de spywares.

2.4. Comment maîtriser les espiogiciels ?

En pratique, vous pouvez suivre plusieurs mesures pour vous prémunir des effets non désirés des espiogiciels.

2.4.1. "Prudence est mère de sûreté"



Conseil

Il convient tout d'abord de prendre garde à ce que vous installez sur votre ordinateur. La plus grande vigilance est notamment recommandée dans le cas de nombreux logiciels distribués gratuitement : Télécharger uniquement les logiciels dont vous êtes parfaitement sûr!



Remarque

Une des caractéristiques majeure des espiogiciels est qu'ils sont souvent installés à l'insu de l'utilisateur. Les boîtes de dialogue d'installation offrent ainsi rarement la possibilité de refuser ces fonctionnalités. Lorsqu'une installation personnalisée d'un logiciel est proposée, on désactivera les modules additionnels qui ne sont pas absolument nécessaires au fonctionnement du logiciel.
Un certain discernement quant aux actions à effectuer, propre aux utilisateurs avertis, est cependant nécessaire.

2.4.2. Lire attentivement entre les lignes



Conseil

Une seconde précaution élémentaire consiste à lire attentivement le *Contrat de Licence d'Utilisateur Final*[CLUF ou EULA pour End-User License Agreement]qui contient généralement en toutes lettres la mention de l'intégration de fonctionnalités de spyware dans le logiciel que l'utilisateur s'apprête à installer.



Remarque

La difficulté vient du fait que ces contrats sont peu lisibles et souvent ambigus, ce qui n'incite pas à leur lecture. Il est toujours possible de refuser ce contrat de licence et de ne pas procéder à l'installation du programme. Le choix d'un logiciel concurrent disposant de fonctionnalités équivalentes mais dépourvu d'espiogiciel pourra alors constituer une bonne alternative.

2.4.3. Effectuer des diagnostics réguliers et surveiller les activités de sa machine



L'usage d'un logiciel anti-virus et d'un pare feu (*firewall*) personnel peut se révéler utile. En effet, pour transmettre les données collectées, l'espiogiciel utilise obligatoirement une connexion internet. Certains pares feu permettront par exemple à l'utilisateur d'être alerté des tentatives de connexion à des serveurs distants.



Remarque

L'efficacité des pares feu est relative puisque l'essentiel des vérifications concerne les données entrantes et non les données sortantes. Celle des anti-virus l'est tout autant car les espiogiciels ne sont pas considérés ni répertoriés comme des virus et passent souvent au travers de ces filtres.

2.4.4. Procéder à des nettoyages réguliers



Le moyen le plus efficace de se prémunir contre les espiogiciels est d'avoir recours à des programmes permettant de les identifier et de les mettre hors d'usage ou de les détruire.



Remarque

Certains sites listent ainsi les espiogiciels connus, leur limite résidant dans l'absence d'exhaustivité et dans l'obsolescence rapide de ces listes.
Il existe encore plusieurs programmes anti-spyware, disponibles gratuitement sur l'internet, dont l'efficacité paraît satisfaisante. Ces logiciels identifient et permettent la désinstallation des espiogiciels indésirables. La désinstallation d'un spyware pourra parfois s'avérer difficile lorsque les fonctionnalités de ce dernier conditionnent le bon fonctionnement du programme principal.



Attention

L'usage de ces techniques de protection est toutefois réservé à des utilisateurs confirmés, une mauvaise manipulation des logiciels ou des effacements malencontreux de fichiers pouvant être préjudiciables au bon fonctionnement de la machine.
En cas de doute, n'hésitez pas à vous entourer des conseils de personnes qualifiées en informatique.

2.5. Un exemple de spyware

Quand vous installez le logiciel de partage de fichiers musicaux Kazaa sur votre ordinateur, vous installez, outre le programme de P2P (peer to peer), d'autres logiciels dont le but est d'ailleurs explicitement indiqué.

La traduction est certes calamiteuse et sent le traducteur automatique à plein nez, mais on comprend quand même qu'en échange de la gratuité de Kazaa, on va devoir supporter des publicités. Les choses ont au moins le mérite d'une apparente clarté.
Plus adware que spyware, le logiciel Kazaa est quand même perçu par la majorité des sociétés spécialisées dans la sécurité informatique comme le plus gros pourvoyeur de spywares en raison de son nombre d'utilisateurs (plus de 200 millions). L'éditeur Computer Associates le classe d'ailleurs toujours en tête de son top 5 des espiogiciels (http://www3.ca.com/securityadvisor/pest/).



Remarque

Le logiciel Cydoor, qui est associé à Kazaa[on parle alors de spyware externalisé], explique clairement sur son site son fonctionnement ; en fonction des informations données par l'utilisateur, des bannières publicitaires sont téléchargées sur le disque dur et affichées régulièrement quand le programme Kazaa est exécuté [c'est-à-dire en permanence dans la plupart des cas]. Cydoor prétend ne recueillir aucune donnée nominative, mais collecte cependant les informations suivantes : sexe, âge, centres d'intérêt, statut marital, salaire, zone d'habitation, pays et niveau d'études. Il n'y a effectivement rien de nominatif là dedans, mais on apprend un peu plus loin que l'installation de Cydoor nécessite de fournir une adresse électronique.

En France, *la CNIL considère depuis longtemps qu'une adresse électronique est une donnée à caractère nominatif* et il y a donc une contradiction entre les principes énoncés par Cydoor et la réalité.
D'autre part, Cydoor décline toute responsabilité en ce qui concerne les traitements de données nominatives qu'effectuent les sociétés pour lesquelles elle réalise de la publicité. On voit donc bien qu'il y a là un grand flou juridique et que le consommateur ne sait finalement pas grand-chose des traitements de données qui sont réalisés sur son ordinateur.

2.6. Quelques adresses utiles

- Site détaillant les moyens pratiques d'éliminer les espiogiciels
- Moteur de recherche sur les programmes intégrant des espiogiciels
- Liste de programmes contenant des espiogiciels connus[date de mise à jour non disponible]
- Site d'information sur la sécurité internet ayant réalisé un dossier complet sur les spyware
- Le logiciel Ad-Aware, de l'éditeur américain Lavasoft, connaît un grand succès

3. Autres catégories de malwares (ou codes malveillants)

Les autres catégories de programmes malveillants sont encore très nombreuses. L'éditeur d'antivirus Trend Micro propose une base de données des virus que l'on peut interroger en ligne. Cette base de données comporte un champ « *type de malware* » qui ne compte pas moins de 26 éléments dans la liste. Elle recense, par exemple, plus de 500 programmes de *backdoor*.

Terme anglais	*Equivalent français*
Backdoor	Porte dérobée
Boot Trojan	Cheval de Troie de démarrage
Clicker	Programme réorientant le navigateur vers un site spécifique
DDoS Program	Programme de déni de service distribué
Downloader	Téléchargeur
Dropper	Programme extrayant d'autres malwares sur l'ordinateur
Exploit	Exploitation d'une faille de sécurité
File infector	Infecteur de fichier
Flooder	Programme inondant une connexion pour la surcharger
Keylogger	Programme d'interception des touches saisies au clavier
Macro Trojan	Cheval de Troie macro
Notifier	Programme de notification d'informations au hacker
Nuker	Programme permettant de planter une machine à distance
Password Stealer	Voleur de mots de passe
Registry Modifier	Modificateur du registre
Script Trojan	Cheval de Troie de script
Sniffer	Programme d'écoute du trafic réseau
Spammer	Programme d'envoi de courriers non sollicités
Trojan	Cheval de Troie

▲ TAB. 2 : DIFFÉRENTES CATÉGORIES DE LOGICIELS MALVEILLANTS

Cette base de données est également intéressante car elle permet d'effectuer une recherche en prenant comme critère l'effet du malware[Effet tel que : mise en danger de la sécurité réseau, corruption de disque dur, création de fichiers, suppression de fichiers, affichage d'images ou de messages, formatage du disque dur, plantage du système, redémarrage de l'ordinateur, vol de mots de passe, etc.].



Remarque

Bien évidemment, cette classification est sujette à caution et on trouve sur Internet, dans les forums spécialisés sur la sécurité informatique, de nombreuses joutes oratoires où les experts se querellent sur la pertinence de telle ou telle catégorie. Fréquenter ce genre de base de données est cependant très formateur car cela permet de mieux appréhender l'ampleur du phénomène et sa réalité.



Complément

Vous trouverez une liste de malwares encore plus complète (71 éléments) à l'adresse suivante : http://www3.ca.com/securityadvisor/pest/search.aspx

4. Autres techniques d'espionnage

4.1. Quelles sont les autres techniques d'observation et à quoi servent-elles ?

- *Javascript* : il s'agit de lignes de code écrites en langage Java, développé par la société Sun. Intégré dans le code source de la page HTML, le javascript est exécuté directement par le navigateur et non par le serveur d'origine.
- *Applet java* : appelée aussi « appliquette », c'est une petite application autonome écrite en langage Java qui effectue quelques tâches spécifiques dans le site web sur lequel elle est intégrée.
- *ActiveX*: c'est une technologie propriété de Microsoft, qui fait partie d'un ensemble désigné sous l'appellation Component Object Model (COM). Les contrôles ActiveX s'apparentent aux applets java. Ils peuvent être téléchargés et exécutés directement par le navigateur.



Quelques lignes de VBScript pour espionner

Un informaticien américain, Richard Smith, qui travaille pour le compte de la Privacy Foundation, a tiré la sonnette d'alarme en exposant les risques que représentent les courriers électroniques au format HTML qui permettent un enrichissement typographique accroissant la lisibilité des messages. Les courriers HTLM, outre le fait qu'ils sont plus beaux, peuvent également contenir du code VBScript ou JavaScript et Richard Smith prétend qu'en rajoutant quelques lignes de programme VBScript dans un courriel au format HTML, il est facile de savoir ce que le destinataire en fait. On peut notamment apprendre à qui il le réexpédie et prendre connaissance des éventuelles remarques qu'il a faites en le transférant.

Dans la mesure où Richard Smith s'est déjà illustré par le passé en mettant à jour les cookies de DoubleCick et en révélant l'existence des webbugs (mouchards capables de pister les internautes), il n'y a pas vraiment de raison de mettre sa parole en doute, même s'il ne fait pas une démonstration du code incriminé. Certaines sociétés exploitent d'ailleurs déjà cette faille en proposant une traçabilité des messages que vous envoyez.

Faut-il pour autant examiner le code source de tous les messages que l'on reçoit ? Cela serait très fastidieux.

En revanche, il est conseillé de désactiver la fonctionnalité JavaScript d'Outlook Express.

4.2. A quoi servent ces techniques ?

Ils permettent des applications interactives lors de l'affichage et de la lecture de pages, comme la vérification des entrées dans des champs de formulaires ou la mise en forme du texte. Mais ils peuvent également servir à exécuter des tâches plus avancées en relation avec des bases de données ou avec le système informatique de l'utilisateur.

Parmi les applications rencontrées dans la navigation courante, les scripts permettent

notamment de déclencher l'ouverture de fenêtres publicitaires dites "*pop up*" ou encore l'inscription d'un site en page de démarrage.
Ils peuvent aussi servir à collecter des données personnelles. La CNIL les classe d'ailleurs dans la catégorie des *procédés de collecte automatisée de données*. A l'instar des cookies et des spywares, les données collectées peuvent aller de la configuration technique de la machine à l'historique des sites visités ou à d'autres données plus sensibles comme des adresses e-mail.



Remarque
Contrairement aux scripts java, les contrôles ActiveX sont programmables sans restrictions et sont à cet égard potentiellement plus dangereux que les java scripts. En effet, ces contrôles peuvent permettre à leur programmeur, une fois exécutés, de réaliser à distance un très grand nombre de tâches et d'actions sur la machine de l'utilisateur en disposant des mêmes privilèges sur les fichiers et les programmes que ce dernier : lier, écrire, effacer, transférer, exécuter.
Ainsi, certains contrôles ActiveX permettent de modifier la base de registre de l'utilisateur. Cette base contient les informations de configuration et de sécurité des programmes et des fichiers, toute modification ayant des conséquences non négligeables sur la sécurité. Les contrôles ActiveX ne fonctionnent toutefois que sous un environnement Windows qui constitue la majorité de systèmes d'exploitation des ordinateurs personnels.



Attention
Ce ne sont pas pour autant des virus, car ils ne se propagent pas et n'infectent pas les documents de l'utilisateur.

4.3. Comment maîtriser ces techniques d'observation ?

Partie C. Les traces sur logiciels

Préambule

Il y a près de dix ans (en 1996), la CNIL écrivait dans son 17e rapport que *"finalement, la présentation souvent faite d'Internet consistant à assimiler le réseau à une immense bibliothèque, consultable au moyen d'un navigateur, dans une relation client/serveur, qui donne à penser que l'information serait passive, transparente et maîtrisée par l'utilisateur paraît bien naïve"* . Cette vision des choses a-t-elle fondamentalement changé aujourd'hui ? Nous avons toutes les raisons de nous montrer pessimistes et ce rapide tour d'horizon montre avec acuité que la nécessité de protéger les données personnelles sur Internet doit devenir une vraie préoccupation.

1. Présentation

Il est de plus en plus fréquent de constater la mise en oeuvre de mouchards pour les applications informatiques sensibles. C'est devenu le cas de la majorité des applications utilisées dans les entreprises, les banques, les assurances, et ceci sous la pression de plus en plus forte des audits de sécurité.

Cette surveillance qui, dans sa forme la plus simple, consiste à inscrire dans un fichier le nom et les heures de connexion/déconnexion d'un utilisateur à une application informatique, permet alors de tracer plus ou moins précisément l'activité d'un salarié. Il parait en effet normal qu'une société tente de sécuriser au maximum son système informatique vu les enjeux, mais force est de constater, d'une part, que la mise en place de ces traces est rarement connue des utilisateurs et, d'autre part, que leur consultation ou leur exploitation est souvent possible pour d'autres personnes[les informaticiens internes à l'entreprise, voire les prestataires de service qui interviennent sur le système, par exemple] que celles qui y ont légitimement accès[le service de contrôle général ou la cellule sécurité de l'entreprise].



Exemple 1

Quand vous utilisez *Outlook Express*, vous laissez, par défaut, des traces de tous les courriers que vous recevez et envoyez. Si cela vous pose des problèmes de confidentialité, vous devez apprendre à supprimer tous les courriers compromettants. Pour que les courriers envoyés ne soient pas systématiquement stockés dans le dossier *Éléments envoyés*, désactivez la case à cocher *Copier les messages envoyés dans 'Éléments envoyés'* dans l'onglet *Envois de la commande Outils > Options*.



Exemple 2

Pour prendre un autre exemple, les logiciels de la suite Office stockent au sein des documents des renseignements dont la plupart des utilisateurs ignorent l'existence. Qui connaît dans Word l'existence de l'option de confidentialité dans Word?

On y accède par la commande *Enregistrer sous* en sélectionnant le menu *Outils > Options de sécurité*. L'option *Supprimer les informations personnelles* des propriétés du fichier lors de l'enregistrement permet de ne pas diffuser involontairement des informations masquées, comme le nom de l'auteur du document ou les noms associés aux commentaires ou aux marques de révision.



Conseil

D'une manière générale, vous devez prendre conscience du fait que *toutes les tâches que vous effectuez sur un ordinateur laissent des traces* : ce n'est pas parce que vous venez d'effacer un courrier compromettant qu'une copie de sauvegarde n'en a pas été faîte sur le serveur. *Méfiez-vous de toutes les fonctions logicielles qui permettent de sauvegarder automatiquement des informations.*

Par exemple, la fonction de saisie semi-automatique de Windows peut révéler des renseignements confidentiels à un intrus qui utiliserait votre ordinateur. Et nous ne parlons même pas des logiciels d'espionnage qui enregistrent à votre insu tout ce que vous saisissez sur votre clavier...

2. Comment supprimer quelques traces ?

Si vous n'aimez pas laisser de traces derrière vous quand vous utilisez un ordinateur, vous apprécierez l'utilitaire Tweak UI, créé par Microsoft, que vous pouvez télécharger en cliquant ici.



Attention
Il existe une version plus récente de *Tweak UI (2.0)* pour Windows XP, mais cette version ne comporte plus malheureusement la fonction qui nous intéresse. Vous pouvez donc télécharger cette version qui fonctionne très bien sous Windows XP.



Démarche
Pour installer ce petit utilitaire, décompactez les fichiers de l'archive dans un dossier, puis faites un clic droit sur le fichier *Tweakui.inf* et choisissez *Installer* dans le menu contextuel. Une nouvelle icône, intitulée *Tweak UI*, apparaît dans le Panneau de configuration.
En cliquant sur cette icône, vous ferez apparaître une boîte de dialogue comportant de nombreux onglets.

Tweak UI permet de configurer simplement de nombreux paramètres de Windows qui sont inaccessibles dans l'interface du système d'exploitation et qui nécessitent habituellement des modifications du registre.



Conseil
Cliquez sur l'onglet « *Paranoia* » pour accéder à de nombreuses options qui permettent d'effacer vos traces au démarrage de l'ordinateur.

3. Un mouchard dans les fichiers Word et Excel

L'histoire que nous allons vous raconter est un peu ancienne à l'échelle du temps informatique car elle date de 1999, mais elle a le mérite d'être assez exemplaire à nos yeux.

Tout a commencé le 1er mars 1999 sur le forum alt.comp.virus où Richard Smith, PDG de la société Phar Lap Software, bien connue des développeurs, a posté un message intitulé Fingerprinting of Excel and Word files [des empreintes dans les fichiers Word et Excel]. Richard Smith indique dans sa contribution qu'il a fait une découverte très intéressante :

" Apparemment, Microsoft crée une empreinte dans les fichiers Excel et Word à l'aide de l'adresse de la carte Ethernet des utilisateurs. L'adresse de la carte Ethernet (ou adresse MAC) est un numéro sur 48 bits qui est conçu pour être unique tout comme le numéro de série du Pentium III. Pour faire vous-même un test, ouvrez simplement un document Word à l'aide de Notepad et cherchez la chaîne "GUID" ; vous constaterez que l'adresse de votre carte réseau suit peu après. Personnellement, je trouve très étrange que des numéros de série matériels soient enregistrés dans des fichiers Word et Excel."
Deux jours plus tard, un article publié dans le New York Times révélait que les

fichiers créés par Word ou Excel contenaient un numéro d'identification unique. Le lendemain, la société Junkbusters publia un communiqué de presse où elle dénonçait l'attitude de Microsoft face au respect de la vie privée. Par la voix de son président, Jason Catlett, cette société dont le but est d'aider les consommateurs à protéger leur vie privée contre les agressions du marketing déclarait que *"les sociétés devaient révéler ce qu'elles faisaient avec les informations permettant d'identifier les personnes. En raison du fait que le processus d'enregistrement de Windows relie des gens à des numéros d'identification, Microsoft se doit d'informer le public sur la destination de ces numéros. Le New York Times n'est pas le lieu adéquat où vous devez découvrir que chaque document créé avec Microsoft Word a été tatoué secrètement avec un numéro d'identification."*

Nous avons personnellement longtemps cru que l'acronyme GUI signifiait Graphic User Interface[Interface utilisateur graphique], mais il a fallu se rendre à l'évidence : cela voulait dire également Globally Unique Identifier[on trouve aussi dans la littérature technique l'acronyme GUID qui signifie la même chose].

Les bonnes âmes s'étaient émues lors de la sortie de Windows 98 de la procédure d'installation qui proposait à l'utilisateur de s'inscrire en ligne car, outre les informations nécessaires à tout enregistrement de licence[nom de l'utilisateur, adresse, etc.], l'assistant proposait d'examiner l'environnement matériel dans lequel l'utilisateur évoluait et pouvait ainsi récolter des informations qui étaient transmises à Microsoft. Or, dans l'édition du 7 mars du New-York Times, on a appris que Richard Smith avait découvert qu'un numéro d'identification unique était transmis à Microsoft lors de l'enregistrement en ligne de Windows 98 même si l'utilisateur ne souhaitait pas communiquer le profil matériel de son ordinateur. Le PDG de Phar Lap montrait comment l'Assistant d'enregistrement de Windows 98 (*RegWiz*) pouvait divulguer les numéros de l'ordinateur et du client. Le premier des deux numéros est appelé *Hardware ID* ou *HWID* [Il s'agit d'un numéro unique assigné par Microsoft qui identifie votre ordinateur. Il contient également l'adresse de votre carte réseau si vous en possédez une. L'adresse est contenue dans les douze derniers chiffres du HWID.] Le deuxième numéro est appelé *Microsoft ID* ou *MSID*. Un magazine allemand, *CT Magazine*, a pu prouver que ce numéro est placé dans un cookie afin de pister les déplacements de l'utilisateur sur le site web de Microsoft. Il s'agit d'un numéro de série unique qui identifie la personne qui a enregistré Windows 98 sur son ordinateur.

Comme le démontre Richard Smith, en raison d'un bug dans le contrôle *ActiveX RegWiz*, ces deux numéros peuvent être lus par d'autres sites web et stockés dans leurs propres bases de données alors que, normalement, ils ne devaient être disponibles que pour Microsoft.

À la suite de cette histoire, Microsoft proposa en téléchargement un outil pour supprimer cet identificateur unique[Office 97 Unique Identifier Removal Tool] et jura ses grands dieux que la version suivante d'Office ne contiendrait plus cette fonctionnalité. Malheureusement, Microsoft ne tint pas promesse : les documents d'Office 2000 étaient encore tatoués. Il a fallu attendre la version d'Office XP (2002) pour que cet identificateur disparaisse, en tous les cas sous la forme que nous connaissons.



Remarque

Si vous avez encore des documents Office 2000 sur votre disque dur, vous pouvez faire le test à l'aide d'un petit utilitaire que l'on peut télécharger sur le Web à l'adresse suivante : http://www.vecdev.com/guideon.html



Complément

Guideon permet non seulement de supprimer l'identificateur unique, mais également de le sauvegarder au préalable dans un fichier journal. Cela permet de constater que, dans l'adresse MAC de sa carte réseau [lisible grâce à la commande IPCONFIG/ALL], se trouve bien le mouchard.
À quelque chose, malheur est bon : c'est grâce au GUID que l'on a pu arrêter l'auteur du virus macro Melissa.

Application

Amusez-vous à lancer *REGEDIT*, l'utilitaire de modification du registre, et recherchez *l'adresse MAC* de votre carte réseau en saisissant tous les chiffres sans espace. Vous serez étonné du nombre d'occurrences que vous rencontrerez...

Ressources



http://www.tactika.com/cookie/



Article "Les cookies démystifiés" de Clément Gagnon.



Coockiecentral.com : Site en anglais qui présente toute l'actualité sur les cookies et autres "témoins" informatiques, une importante FAQ explicative et un forum de discussion.



En anglais.

Chapitre

III

La sécurisation des informations sensibles

Partie A. Les dangers d'Internet

1. Les virus et macro-virus informatiques



Qu'est-ce qu'un virus informatique ?

Un virus informatique est un *programme*[des instructions écrites dans un langage de programmation] qui *effectue certaines actions* et, en général, *cherche à se reproduire*. Il peut aussi avoir comme effet, recherché ou non, de *nuire en perturbant plus ou moins gravement le fonctionnement de l'oridnateur infecté*.
Les actions effectuées dépendent du virus et sont différentes d'un virus à l'autre : cela peut aller du simple affichage d'images ou de messages à l'écran à l'effacement complet du disque dur (dans ce cas, on parle de « *bombe logique* » ou de « *charge utile* »), en passant par la suppression de certains fichiers.
Les virus informatiques peuvent *se répandre à travers tout moyen d'échange de données numériques* comme l'Internet, mais aussi les disquettes, les cédéroms,...
Son appellation provient d'une analogie avec le virus biologique puisqu'il présente des similitudes dans sa manière de se propager et de se reproduire.



Remarque :
Sachez que le nombre de virus en circulation sur PC s'élève à plusieurs dizaines de milliers. Le danger est donc bien réel et cela n'arrive pas qu'aux autres. Il faut donc *apprendre à bien identifier les risques pour ne pas se faire contaminer ni, par voie de conséquence, contaminer les autres* ; en effet, quand vous êtes victime d'un virus, outre le désagrément de la situation, la plupart du temps vous le transmettez à vos correspondants chaque fois que vous envoyez un e-mail. Raison de plus pour vous protéger !



Attention
Les virus font souvent l'objet de fausses alertes que la rumeur propage, encombrant les messageries. Certaines d'enre elles, jouant sur l'ignorance informatique des utilisateurs, leur font parfois détruire des éléments de système d'exploitation totalement sains.

Les macro-virus

Les macro-virus s'attaquent aux macros de logiciels de la suite Microsoft Office (Word, Excel,...) grâce au VBA de Microsoft.



Exemple
Par exemple, en s'intégrant dans le modèle *normal.dot* de Word, un virus peut être activé à chaque fois que l'utilisateur lance ce programme.

2. Les vers

Les vers se répandent dans le courrier électronique en profitant des failles des différents logiciels de messagerie (notamment Microsoft Outlook). Dès qu'ils ont infecté un ordinateur, ils s'envoient eux-mêmes dans tout le carnet d'adresses, ce qui fait que l'on reçoit ce virus de personnes connues. Certains d'entre eux ont connu une expansion fulgurante (« *I Love You* »).

Les experts n'arrivent pas à se mettre d'accord sur l'appartenance ou non des vers à la classe des virus informatiques.

3. Les canulars (hoax)



Hoax
Terme anglais qu'on peut traduire par canular, le hoax peut être défini comme une fausse information ou une rumeur. C'est une forme particulière de spam puisqu'il se base sur le courrier électronique. Il utilise la crédulité des utilisateurs pour se propager. En faisant circuler des informations qui apparaissent à l'utilisateur comme essentielles il compte sur celui-ci pour relayer (forwarder) l'information à tous ses contacts.

En général, le hoax n'est pas réellement dangereux puisqu'il ne met pas en défaut la sécurité des données de l'utilisateur et n'essaie pas de lui extorquer de l'argent. Cependant, le hoax possède quelques côtés pervers :

- Il sert la désinformation en faisant circuler de fausses informations ou des rumeurs non fondées et décrédibilise le moyen de diffusion que représente Internet.
- Il engorge les réseaux et les boîtes aux lettres en se servant des utilisateurs crédules pour être propagé.

Le site web www.hoaxbuster.com est une ressource en ligne recensant tous les hoax qui circulent sur Internet. Pour lutter contre la désinformation, pensez à toujours vérifier une information avant de l'envoyer à vos amis.



Conseil

- Une alerte de virus par email : mettez votre anti-virus à jour et laissez-le faire son boulot !
- Une chaîne de solidarité : vérifiez sur www.hoaxbuster.com !
- Votre souhait se réalisera ... arrêtez de lire l'horoscope, vous allez finir par y croire !

4. Les chevaux de Troie



Explication

Le terme *cheval de Troie* (en anglais, *trojan horse* ou simplement *trojan*) tire bien entendu son origine d'un célèbre épisode de la mythologie grecque où un cheval en bois contenant des guerriers avait été introduit, grâce à une ruse, dans la ville de Troie assiégée.



Un cheval de Troie est donc un programme qui effectue une tâche spécifique à l'insu de l'utilisateur.
À la différence d'un virus, *un cheval de Troie ne se reproduit pas*, mais de nombreux virus diffusent également un cheval de Troie sur l'ordinateur qu'ils infectent.

Un cheval de Troie peut être exécuté de manière furtive à chaque démarrage de l'ordinateur si un virus a programmé son exécution automatique en ajoutant des clés dans le registre.

Un cheval de Troie peut aussi se cacher dans un logiciel qui lui servira d'hôte.



Exemple

Quand un utilisateur croit exécuter un programme de jeu de dames qu'il a téléchargé sur Internet, il va également lancer un petit logiciel furtif qui va enregistrer toutes les touches qu'il saisit au clavier et, par conséquent, dévoiler tous ses mots de passe, son numéro de carte bancaire s'il réalise des achats sur Internet, etc. C'est ensuite un jeu d'enfant pour le cheval de Troie de stocker toutes ces informations dans un fichier qui sera ensuite transmis par protocole FTP, dès l'activation de la connexion Internet, sur un serveur situé dans un pays où la législation n'est pas trop regardante...



Attention

Internet représente une véritable mine car on y trouve de très nombreuses informations gratuites et de qualité. Cela est également vrai pour les logiciels et vous pouvez trouver sur la Toile de très nombreux programmes freeware (gratuits) d'excellente facture.

Il convient cependant d'être particulièrement méfiant et de faire attention où l'on met les pieds. Il ne s'agit absolument pas de jeter ici l'anathème et de semer le doute sur tout ce qui est gratuit car certains programmes freeware sont bien meilleurs que d'autres qui sont commercialisés. Pour autant, il faut reconnaître que de nombreux chevaux de Troie sont diffusés par le biais de programmes freeware en téléchargement sur Internet.

Dans ces conditions, *évitez de télécharger tout et n'importe quoi* car vous risquez d'affaiblir considérablement la sécurité de votre ordinateur. Si vous appréciez les logiciels freeware, adoptez les règles suivantes :

- *Préférez les programmes qui sont livrés sur les CD-ROM des revues* (en principe, ils ont déjà été testés et sont garantis sans virus).
- *Optez pour les programmes freeware écrits par des individus ou des sociétés dont la réputation est irréprochable* (faites-vous votre opinion en lisant les commentaires des autres utilisateurs).
- *Méfiez-vous des programmes qui viennent de sortir et qui sont inconnus.*
- *Proscrivez les logiciels dont le but est clairement illégal et que l'on trouve sur certains sites underground*. Récupérer un programme qui permet de craquer les mots de passe ou de générer de vrais faux numéros de cartes bancaires peut vous donner l'impression (fausse) d'être un gourou de l'informatique et vous procurer des frissons insondables en vous persuadant que vous êtes en train de passer du côté de la force obscure, mais vous risquez surtout d'introduire un cheval de Troie sur votre ordinateur.
- *Privilégiez les logiciels dont les développeurs publient le code source* (vous ne serez peut-être pas capables de l'analyser, mais des professionnels de la sécurité pourront le faire à votre place et émettre un avis).
- *En cas de doute, abstenez-vous et optez pour un autre logiciel, même s'il s'agit d'un programme payant.* N'oubliez pas qu'avec un logiciel commercial, vous pouvez avoir un recours en cas de problème.



Complément

D'après tous les éditeurs d'antivirus, le nombre de chevaux de Troie est en très nette augmentation depuis quelques années ; dans la liste des virus recensés par la base de données de Symantec, le terme « trojan » apparaît plus d'un millier de fois.

Si les premiers chevaux de Troie étaient assez primitifs et ne faisaient pas dans la dentelle[En formatant, par exemple, votre disque dur comme le programme Mungabunga], on a affaire aujourd'hui à des programmes de plus en plus sophistiqués.

En janvier 2005, les policiers espagnols ont ainsi arrêté un programmeur de 37 ans qui avait écrit un cheval de Troie permettant de récupérer des informations sur les comptes bancaires des utilisateurs. De plus, disponible sur les réseaux d'échanges de fichiers (P2P), ce logiciel espionnait les utilisateurs munis d'une Webcam...



Les programmeurs de chevaux de Troie rivalisent aussi d'imagination pour diffuser leurs oeuvres. Certains n'hésitent pas à se faire passer pour Microsoft et envoient ainsi des courriels qui ressemblent à s'y méprendre aux messages que Microsoft diffuse. La seule différence est que Microsoft ne diffuse jamais de programme par courrier électronique. Ses correctifs logiciels se téléchargent soit par Windows Update, soit directement sur le site web de Microsoft.

5. "Les portes dérobées"



Une *porte dérobée* (en anglais *backdoor*) est un programme qui permet d'accéder à distance à un ordinateur. Il s'agit en fait d'un type particulier de cheval de Troie que l'on appelle parfois aussi cheval de Troie distant. Certains programmes légitimes offrent cette fonctionnalité : il s'agit notamment de tous les logiciels de prise de contrôle à distance qui sont utilisés dans le cadre de la maintenance.

Dans le cas d'une porte dérobée, *l'accès distant se réalise évidemment sans le consentement de son propriétaire et à son insu*. Les portes dérobées se composent habituellement de deux parties : le *client* et le *serveur*.

Le composant serveur est installé sur la machine de la victime grâce à un virus ou à un cheval de Troie. En général, la première action que réalise la porte dérobée est de modifier certaines valeurs du registre afin de s'assurer d'être chargée en mémoire à chaque démarrage de la machine. Une fois cela mis en place, le composant serveur ouvre un port réseau de telle sorte que l'utilisateur malveillant puisse se connecter à la machine en tout tranquillité et sans éveiller les soupçons de la victime. Quand l'attaquant a pris le contrôle de la machine, il peut réaliser toute une série d'actions qui dépendent du degré de sophistication de la porte dérobée.

Exemples d'actions réalisées par les portes dérobées

Parmi ces actions, on peut citer :

- Le transfert de fichiers (dans un sens ou dans l'autre) ;
- La suppression et la modification de fichiers ;
- Le vol d'informations ;
- L'enregistrement de la saisie au clavier ;
- L'arrêt de certaines application[L'antivirus, par exemple.] ;
- Le démarrage d'un serveur FTP qui permettra ainsi à d'autres attaquants de se connecter à la machine.

Illustration

Afin de mieux comprendre le fonctionnement de ce genre de programme, nous allons illustrer notre propos à l'aide d'un exemple et étudier le comportement de la *porte dérobée Berbew* qui est justement recherchée par l'outil de suppression de logiciels malveillants de Microsoft.

Tout commence par la réception d'un courrier électronique en provenance d'une banque. L'adresse électronique a été falsifiée, mais le courriel semble provenir d'un service nommé Citibank Accouting. Le sujet du message, « *Re : Your credit applicatio*n », semble indiquer que la banque répond à l'un de vos courriers. Dans le corps du mail, il est indiqué que le prêt en ligne que vous avez demandé a été refusé et que les informations concernant le profil bancaire que vous avez fourni à la banque sont incluses en pièce jointe. Le courriel vous incite à les vérifier en ouvrant la pièce jointe. La pièce jointe dont le poids est de 5 664 octets a pour nom *web.da.us.citi.heloc.pi*f.

Cette pièce jointe est un cheval de Troie de type *downloader* (*téléchargeur*), qui a pour mission de télécharger sur Internet la *porte dérobée nommée Berbew*, de l'enregistrer dans le répertoire système de Windows sous le nom de *Rtdx32.exe*, puis de l'exécuter.

La porte dérobée :

- copie le programme dans le répertoire système de Windows sous un nom aléatoire ;
- crée une clé dans le registre de manière que la porte dérobée s'exécute au démarrage de Windows ;
- crée un fichier de configuration afin de stocker différentes informations nécessaires au bon déroulement du programme[Par exemple, numéros des ports réseau utilisés par la porte dérobée, URL où envoyer les informations volées, etc.] ;
- tente d'accéder aux différents mots de passe stockés sur l'ordinateur[Connexion Internet, partages réseau, etc.] ;
- récupère les informations saisies au clavier ainsi que le contenu du Presse-papiers. Elle tente aussi de récupérer des informations bancaires. Pour récupérer les informations, le programme modifie certaines options de Windows, comme la saisie semi-automatique.

♦ ouvre des ports réseau et cherche des connexions entrantes.

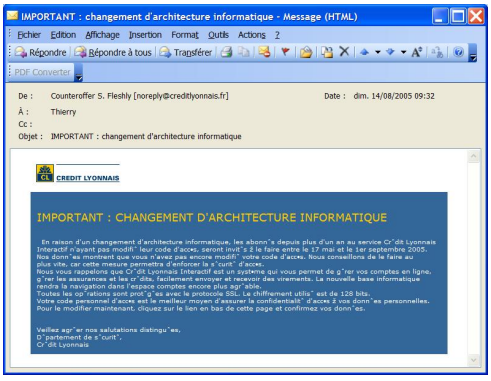
6. Le phishing

6.1. Qu'est-ce que le phishing et en quoi consiste t-il ?

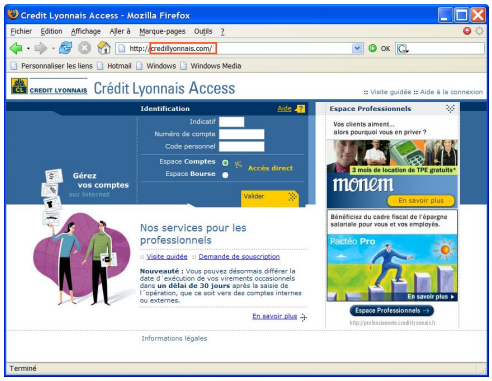
Le phishing (qui vient du mot anglais fishing qui signifie la pêche) est une technique d'ingénierie sociale qui consiste à envoyer un courriel en se faisant passer pour une organisation avec laquelle vous êtes en relation (une banque, une administration, un éditeur de logiciel, un fournisseur d'accès à Internet, etc.).

Dans ce courriel, il vous est demandé de fournir des renseignements personnels qu'une personne malveillante pourra exploiter ultérieurement pour, par exemple, pirater votre compte bancaire. Le courriel peut aussi vous rediriger vers un site Web qui affichera un formulaire de saisie imitant parfaitement le formulaire réel de l'entreprise dont le pirate cherche à usurper l'identité.

Tout est mis en oeuvre pour mettre l'internaute en confiance : l'adresse du site Web pirate ressemble à une lettre près à l'adresse du site Web de l'entreprise et l'identité visuelle (logo, polices de caractères, mise en page, etc.) est reprise à l'identique. Vous avez ainsi l'impression de communiquer avec une entreprise que vous connaissez et avec laquelle vous entretenez des relations commerciales. En réalité, vous fournissez des renseignements à un pirate.



▲ IMG. 2



▲ IMG. 3

6.2. Pour en savoir plus sur le phishing et l'ingénierie sociale...

Pour aller plus loin

Plus d'informations sur le phishing peuvent être trouvées dans le polycope B3 « Sauvegarder sécuriser, archiver ses données en local et en réseau filaire ou sans fil » de CIIMES Partie III, Chapitre A

Pour en savoir plus sur le phishing et l'ingénierie sociale, visitez les liens suivants:

http://www.foruminternet.org/cyberconso/
http://fr.wikipedia.org/wiki/Ingénierie_sociale
http://fr.wikipedia.org/wiki/Phishing

Partie B. Le piratage informatique

1. Les hackers

Derrière le terme *hacker*, le grand public a souvent la vision d'adolescents en train de pirater les ordinateurs du FBI. La réalité est cependant un peu différente. Nous allons commencer par étudier l'origine de ce mot et voir qu'il existe différents types de hackers.



À l'origine, le mot *hacker* désigne celui qui se sert d'une hache, mais dans le contexte informatique, il semble que ce mot ait été employé pour la première fois au MIT, la célèbre université américaine.
Un hacker est avant tout *quelqu'un qui cherche à comprendre ce qui se passe sous le capot et qui étudie au plus près le fonctionnement interne d'un ordinateur, tant du point de vue matériel que logiciel*.
En fait, un hacker désigne un passionné qui s'investit à fond dans son domaine de prédilection qui n'est pas forcément l'informatique.

Bien évidemment, à force de chercher dans les entrailles du système le hacker informaticien va découvrir des choses et fatalement quelques failles de sécurité. Mais ce n'est pas parce que le hacker met à jour une faille du système qu'il va l'exploiter ; pour désigner cette attitude, les hackers ont créé le terme *cracker*.



Un *cracker* est une personne qui cherche par tous les moyens à percer les systèmes de sécurité d'un logiciel ou d'un réseau.



Remarque
Il existe différentes catégories de hackers : les *chapeaux blancs*, les *chapeaux noirs* et les *chapeaux gris*.
Un chapeau blanc est un hacker qui ne commet jamais aucune infraction à la loi alors qu'un chapeau noir est un hacker qui utilise ses connaissances des systèmes informatiques pour commettre des indélicatesses.
Entre les deux, il y a les chapeaux gris qui n'enfreignent pas la loi, mais sont prêts à publier des informations qui permettront d'exploiter une faille de sécurité.

Certains hackers prétendent développer une éthique que l'on appelle « *hacktivisme* » ; il s'agit là de justifier les délits informatiques en invoquant des raisons politiques. Certains groupes de hackers vont ainsi changer la page d'accueil d'un site web, mettre à genoux les serveurs d'un site de commerce en ligne ou bien encore attaquer le système d'information d'un état ou d'une organisation dont ils ne partagent pas les vues.

Il est bien évident qu'en tant que particulier, vous ne risquez pas grand-chose de ce genre d'individus. Il est tout de même possible que votre machine soit la cible d'un cheval de Troie qui l'oblige à servir de relais, par exemple, pour une attaque de déni de service[Déni de service : Attaque d'un système informatique qui a pour but de réduire ses performances et, au final, de le bloquer totalement. Ainsi, un serveur web qui subira une attaque de déni de service ne sera plus en mesure de répondre aux requêtes des utilisateurs. Les attaques de déni de service distribué sont élaborées à partir de plusieurs ordinateurs (parfois plusieurs centaines) qui unissent leurs efforts pour attaquer leur cible. En général, les machines qui participent à une attaque de déni de service distribué ont été contaminées par un cheval de Troie.].

En revanche, de nombreux hackers n'ont aucune motivation politique : l'appât du gain est la seule raison qui les pousse à hacker une machine, c'est-à-dire à en prendre le contrôle. Votre machine sera attaquée soit parce qu'elle renferme des informations qui sont susceptibles d'être monnayées, soit tout simplement parce qu'elle est mal verrouillée et qu'elle pourra servir de base arrière à un pirate qui brouillera ainsi les pistes en n'utilisant pas sa propre machine pour commettre son forfait.

* *
*

Une fois introduit sur le réseau privé, l'objectif du hacker peut être multiple :

- Obtention d'informations confidentielles ;
- Utilisation des machines pour compromettre d'autres actes illicites ;
- Destruction ou altération d'informations (comme des comptes en banque).

2. Illustration : les dangers du mail-bombing



Les dangers du mail-bombing

Le mail-bombing, que nos amis du Québec traduisent par bombarderie, est l'envoi, dans un but malveillant, d'une quantité considérable de courriers électroniques à une même adresse.

Cette pratique, si facile à mettre en oeuvre quand on souhaite se venger de quelqu'un, est pourtant répréhensible par la loi, comme l'a appris à ses dépens un jeune homme un peu insouciant.

Ce dernier, voulant mettre en difficulté son ancien employeur, s'est mis à le bombarder de courriers électroniques afin de mettre en déroute son serveur de messagerie.

Mais le Tribunal de grande instance de Lyon, dans un jugement en date du 20 février 2001, a rappelé qu' *"attendu que Patrice C. est prévenu d'avoir à Lyon, entre le 22 avril 2000 et le 3 mai 2000, altéré le fonctionnement des systèmes de traitement automatisé de données de la société Claranet par suite d'un accès frauduleux réalisé au moyen du logiciel Aenima permettant l'envoi de grande quantité de courriers électroniques vides ainsi que l'envoi de gros fichiers au moyen d'un compte anonyme souscrit chez le fournisseur internet Prontomail, visant à encombrer la bande passante de la victime et ralentir son système, condamne Patrice C. à 8 mois d'emprisonnement avec sursis et à une amende délictuelle de 20.000 F pour l'infraction d'altération du fonctionnement d'un système de traitement automatisé, suite à accès frauduleux."*

Et je ne vous parle même pas de la somme de 300 000 F à débourser à titre de dommages et intérêts pour le préjudice subi par la société Claranet ! Alors, avant de vous venger, réfléchissez un peu...

Partie C. Notions de sécurité

Préambule

Le piratage des systèmes d'information est un danger dont toute personne doit être consciente.

La confidentialité est un aspects de la sécurité informatique consistant à assurer que seules les personnes autorisées aient accès aux ressources et informations.

Pour mettre en oeuvre cette confidentialité, on utilise des techniques et outils de sécurisation des réseaux :

- *Protection via l'authentification* : identifiants et mots de passe ;
- *Protection via la sécurisation du réseau* : l'exemple du pare-feu.

1. Contrôle d'accès, bon usage des mot de passe et login

Jusqu'à maintenant, nous avons toujours supposé que le hacker était distant et qu'il cherchait à atteindre votre machine en utilisant un réseau. Il ne faut pas pour autant négliger l'hypothèse où votre assaillant s'est subrepticement introduit dans votre bureau ou a tout simplement volé votre ordinateur, et se trouve maintenant bien tranquillement assis devant votre machine.

Le premier rempart contre les intrus consiste tout simplement à utiliser des *mots de passe*. Un peu de la même manière qu'un cambrioleur sera dissuadé de fracturer une porte qui possède de nombreux verrous, un hacker rechignera à pénétrer une machine dont les verrous logiciels auront été multipliés.



Conseil

Dans ces conditions, vous devez multiplier l'utilisation des mots de passe à tous les niveaux :

- Le premier niveau est bien sûr celui du *setup de l'ordinateur*. Vous devez choisir un mot de passe de manière que personne d'autre que vous ne puisse modifier la configuration matérielle de votre ordinateur. La plupart des BIOS modernes offrent également la possibilité de saisir un mot de passe au démarrage de la machine (avant le mot de passe de Windows).
- Ensuite, vous devez choisir un mot de passe pour le *compte de Windows*, même si vous êtes le seul utilisateur de votre ordinateur.

La multiplication des mots de passe peut vite devenir un véritable casse-tête car il faut bien reconnaître que les applications qui requièrent un mot de passe sont nombreuses, notamment sur le Web.



Attention

Microsoft, pour remédier à ce problème, propose dans Internet Explorer une fonction intitulée *saisie semi-automatique* ; cette dernière permet de mémoriser les saisies précédentes réalisées pour les adresses, les formulaires et les mots de passe web.
Cette fonctionnalité peut de prime abord paraître très pratique car elle permet de retenir les mots de passe à notre place. Si cela part d'un bon sentiment, *il faut à tout prix éviter de sauvegarder un mot de passe de cette manière* car quiconque serait physiquement devant notre machine pourrait dans ces conditions exécuter l'application nécessitant un contrôle d'accès sans connaître le mot de passe.

On peut penser que, dans un avenir relativement proche, la baisse du coût des appareils de contrôle biométrique[Scanner d'empreintes digitales, par exemple]simplifiera grandement les procédures et permettra ainsi d'éviter d'avoir à gérer de nombreux mots de passe dont la multiplication est une source d'erreurs et d'insécurité.



Du bon usage des mots de passe

Le dernier rempart de la sécurité informatique, qu'il s'agisse de l'accès à votre ordinateur, à votre compte de courrier électronique ou à votre clé privée, c'est bien évidemment le mot de passe.

Vous pouvez bénéficier des dispositifs matériels et logiciels les plus sophistiqués, au bout du compte, il y aura toujours un mot de passe dont vous serez responsable. Dans cette optique, *le choix du mot de passe et sa conservation deviennent primordiaux*.
Voici quelques conseils pour bien gérer vos mots de passe :

- Un mot de passe doit être long (au minimum 8 caractères).
- Un mot de passe ne doit pas avoir de signification.
- Un mot de passe ne doit pas faire référence à votre vie privée : ne choisissez pas le nom de votre chien, votre date de naissance, etc.
- Un mot de passe doit contenir tous les caractères possibles (minuscules, majuscules, chiffres, symboles, etc.).
- Un mot de passe doit être changé régulièrement.
- Un mot de passe ne doit jamais être écrit nulle part, hormis dans un coffre-fort dont la combinaison ne sera jamais écrite.
- Ne faites pas mémoriser vos mots de passe par vos logiciels.
- Ne révélez jamais votre mot de passe à qui que ce soit.
- Utilisez un écran de veille muni d'un mot de passe.

2. Les outils de protection

Pour éviter toute contamination virale, vous devez utiliser un logiciel antivirus. Comme son nom l'indique, l'antivirus combat les virus.

L'anti-virus a plusieurs actions :

- Il *protège* en scrutant tous les fichiers qui pénètrent sur votre ordinateur ;
- Il *analyse* périodiquement le contenu de votre disque dur ;
- Il *désinfecte* en cas de contamination.



Conseil

Vous devez posséder un *logiciel antivirus qui s'interface avec votre logiciel de messagerie et examine tout le courrier entrant et sortant*.
La plupart des antivirus fonctionnent en intégrant une base de données qui contient les caractéristiques des virus connus à ce jour. Dans la mesure où des virus sont découverts tous les jours, ou presque, votre logiciel antivirus doit prévoir un *mécanisme de mise à jour par Internet de sa base de données quand de nouveaux virus apparaissent. Une mise à jour quotidienne ne paraît pas, en ce sens, superflue, compte tenu de la vitesse de propagation de certains virus*.

Conseil

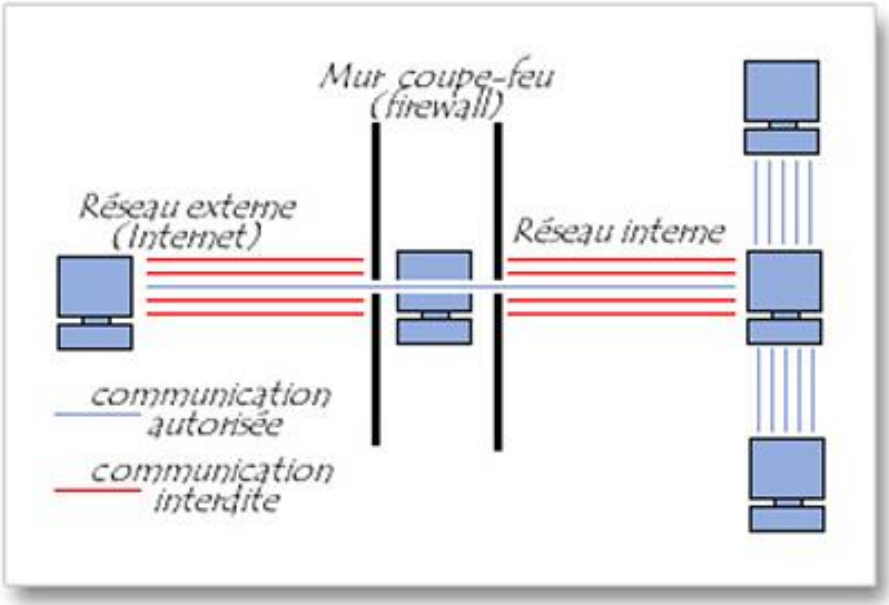
Il existe de multiples façons de se protéger des diverses nuisances présentées, mais la première et la plus efficace est de *changer ses comportement*.
Notamment, n'ouvrez pas les courriels de personnes qui vous sont inconnues ou dont les sujets vous semblent suspects: Hi ! My picture ! ...

3. Sécurisation du réseau : les pare-feux

Un *pare-feu* (en anglais, *firewall*) est un *dispositif matériel ou logiciel qui contrôle les connexions réseau de votre ordinateur, aussi bien en entrée qu'en sortie*.
Dans le cadre d'une utilisation domestique, le pare-feu est la plupart du temps un logiciel qui est installé sur l'ordinateur ; il peut cependant également faire partie d'un équipement réseau tel qu'un routeur ou une passerelle résidentielle comme la Freebox ou la Livebox.

Les informations sur Internet, ainsi que sur un réseau local, transitent sous la forme de *paquets IP*. Le rôle du pare-feu est de filtrer ces paquets ; il peut, dans certains cas, autoriser la communication et, dans d'autres, la bloquer.

Outre cette fonction de rempart contre les éventuels assaillants, certains pare-feu peuvent, entre autres, masquer les informations permettant de donner des renseignements aux hackers qui écoutent les ports ouverts de votre connexion TCP/IP. Ainsi, votre ordinateur passe en *mode furtif* et *ne répond pas aux sollicitations des connexions extérieures qui n'ont même pas la confirmation de l'inexistence de votre ordinateur*. Votre machine est invisible sur Internet et ne répond qu'aux programmes qui sont dûment autorisés et qu'aux ordinateurs que vous avez approuvés.



▲ Img. 4 : Schéma



Remarque

Certains pare-feu permettent également de tenir un *journal* (en anglais, *log*) de toutes les tentatives d'intrusion sur votre ordinateur. Ces statistiques peuvent par la suite être étudiées par des spécialistes ou la police.

Fondamentaux

A l'aide du firewall l'utilisateur peut définir sa politique de sécurité :

- Soit il autorise uniquement les communications ayant été explicitement autorisées donc *tout ce qui n'est pas explicitement autorisé est interdit.*
- Soit il empêche les échanges qui ont été explicitement interdits donc *tout le reste est autorisé*.

La première méthode est sans nul doute la plus sûre, mais elle impose toutefois une définition précise et contraignante des besoins en communication. En effet, chaque fois que le firewall détecte un échange jamais rencontré jusqu'ici, il demande à l'utilisateur d'autoriser ou d'interdire cet échange.



Attention

Ce n'est pas parce que vous avez installé un pare-feu qu'il faut vous sentir invulnérable. *Un pare-feu n'arrête pas les virus ni les chevaux de Troie*. Sachez qu'en matière de sécurité informatique, il vaut mieux rester prudent et humble. La protection à 100 % n'existe pas et même si votre système est à jour, équipé d'un antivirus et d'un pare-feu, il existe toujours un risque potentiel.

Si vous pensez être à l'abri des hackers parce que vous ne possédez aucune information de valeur sur votre ordinateur et ne détenez aucun secret qui pourrait se monnayer, ne croyez pas pour autant que vous ne courez aucun risque. Gardez à l'esprit que, comme les sportifs, les hackers doivent s'entraîner pour rester performants et essayer de trouver de nouvelles failles de sécurité. Et croyez-moi, quand ils s'entraînent, les hackers frappent n'importe où, sans distinction aucune.



Complément

Partie D. Sauvegarder ses données importantes

1. Pourquoi faut-il sauvegarder ?

Il existe quelques axiomes de base en informatique et notamment le fait que l'on doit toujours effectuer une copie de sauvegarde de ses informations importantes.
Cette copie de sauvegarde doit bien évidemment s'effectuer sur un support physique indépendant de l'emplacement où le fichier original se situe ; en effet, il serait totalement inutile d'effectuer une copie de sauvegarde sur le même disque qui renferme le fichier original car, en cas de défaillance du disque, l'original et sa copie seraient perdus.
Pratiquement, cela signifie que si l'on stocke ses fichiers sur son disque dur, ce qui est le cas le plus fréquent, il faut créer la copie de sauvegarde sur une disquette, un CD-R, une clé USB, un DVD-R, un disque amovible, un bureau virtuel, etc.
Le matériel informatique est somme toute fragile et par voie de conséquence les données qui y sont stockées sont par nature sujettes à effacement. Il existe de très nombreuses raisons pour qu'une information stockée sur un support informatique devienne illisible ; dresser un inventaire complet de tous les types d'accidents qui peuvent survenir serait fastidieux, mais nous pensons qu'il n'est pas inutile de rappeler que les coupures de courant, les virus, l'inattention, la malveillance, l'incendie, les dégâts des eaux et le vol existent et n'arrivent pas qu'aux autres. Il existe également un autre facteur auquel on ne pense pas souvent, mais qui se révèle cruel en informatique : le *temps*.



Remarque
Le temps joue contre nous doublement car :

- d'une part rien n'indique vraiment que les technologies de stockage actuelles vieillissent bien ;
- d'autre part, étant donné la rapide obsolescence des logiciels, il n'est pas rare de constater que moins d'une dizaine d'années après, un format de fichier est devenu illisible.

Nous vivons donc dans un *contexte numérique qui est incertain* et il convient de bien réfléchir à une *politique de sauvegarde des données que l'on juge importantes*.

Le premier écueil vient du fait que la majorité des particuliers ne voit pas du tout l'intérêt de réaliser des sauvegardes. Pour l'utilisateur d'un ordinateur domestique, la sauvegarde des données est fastidieuse, coûte cher en temps et en argent et reste réservée au monde des entreprises. Sur ce dernier point, il se trompe car bon nombre de PME et PMI n'ont pas de politique de sauvegarde digne de ce nom...
Quand on discute avec des possesseurs de micro-ordinateurs de l'intérêt des sauvegardes, le discours est récurrent : *" Nous n'avons aucune information qui mérite d'être sauvegardée ; en cas de problème, nous repartirons de zéro"* . Ceux qui ont eu des problèmes tiennent un autre discours et les mésaventures qu'ils ont subies valent en général tous les argumentaires.



Remarque

Il y a principalement deux raisons qui peuvent nous pousser à faire des sauvegardes :

Nous vivons aujourd'hui dans un *monde hautement numérisé* et *nous manipulons de plus en plus d'informations numériques*.

Certaines informations sont importantes pour nous, mais nous ne nous en rendons pas compte.



Rappel

C'est une évidence de rappeler qu'aujourd'hui le numérique a envahi notre maison, l'ordinateur étant le grand chef d'orchestre de cette nouvelle organisation de l'information. Nous écoutons de la musique numérique, prenons des photos numériques et échangeons des courriers électroniques. Nous faisons nos achats en ligne, gérons nos comptes bancaires en ligne et recevons nos chaînes de télévision par ADSL.

Pour bien vous pénétrer de cette réalité, il existe un test simple qui consiste à imaginer ce dont nous nous priverions aujourd'hui si notre ordinateur tombait en panne. Posez-vous la question et vous mesurerez ainsi votre dépendance à l'égard de cette petite machine.

Une fois ce constat réalisé, il faut faire l'inventaire de toutes les informations qui feraient gravement défaut si l'on n'en disposait plus.

Cette réalité recouvre en général deux catégories bien différentes : les *informations auxquelles nous sommes attachés sentimentalement* et les *informations qui ont une valeur parce qu'elles nous sont utiles et dont le remplacement coûterait cher ou prendrait du temps*.

Il existe aussi des informations dont nous nous servons tous les jours et dont la perte se révèlerait gênante. Bien évidemment, ces informations n'ont pas de caractère vital, mais leur indisponibilité vous ferait perdre beaucoup de temps. Le seul argument qui puisse faire réfléchir à la nécessité de réaliser des sauvegardes est d'*estimer le temps qu'il faudrait pour recréer complètement toutes ces données*: *Si ce temps excède de beaucoup le temps nécessaire à la réalisation des sauvegardes, c'est peut-être le moment de modifier vos habitudes de travai*l.

2. Méthodologie des sauvegardes

Si vous avez décidé de faire des sauvegardes, autant faire les choses comme il faut. Vous devez donc répondre aux questions suivantes :

- Quels sont les fichiers à sauvegarder ?
- Sur quel support faut-il faire les sauvegardes ?
- À quelle fréquence doit-on réaliser les sauvegardes ?

2.1. Comment choisir les fichiers à sauvegarder ?

Cette question est finalement assez facile à trancher. *Il faut sauvegarder les données importantes dont vous ne possédez pas de double*. Cela implique que vous n'avez pas à sauvegarder vos logiciels puisqu'en théorie vous les avez acquis et possédez donc les CD-ROM d'installation. En définitive, vous devez principalement réaliser des copies de sauvegarde des documents que vous créez.
Il faut prendre ici le terme « *document* » dans un sens très large et nous incluons dans cet ensemble :

- les *documents bureautiques* (fichiers Word, Excel, Access, etc.) ;
- les *documents de gestion* (fichier de comptabilité, fichier de gestion d'une association, etc.) ;
- les *documents artistiques* (dessins, photos numériques, partitions, etc.). Ces documents sont assez faciles à sauvegarder car à chaque création correspondent en général un ou plusieurs fichiers qui sont facilement identifiables.

  En revanche, cela n'est pas toujours aussi simple! Par exemple, si vous voulez sauvegarder vos courriers électroniques ou bien vos favoris, vous verrez que cela n'est pas toujours aussi simple. Il existe donc toute une série d'informations qui sont importantes à sauvegarder, mais qui demandent des opérations plus spécifiques que la simple copie d'un fichier de données, même si au final les informations sont toujours stockées dans des fichiers.

2.1.1. Sauvegarde du corrier électronique

Si le courrier électronique est souvent utilisé pour des échanges informels, il est devenu un instrument de travail indispensable pour tous les gens qui ont à échanger des informations importantes. En ce sens, il a intégré la panoplie des outils professionnels dont les entreprises ne peuvent plus faire l'économie aujourd'hui. Des sociétés s'envoient des contrats par e-mail, des formules, des plans, etc. La valeur des informations échangées, ainsi que l'accroissement du volume des courriers électroniques reçus et envoyés, posent toute une série de problèmes nouveaux, aussi bien pour les entreprises que pour les particuliers car ces derniers envoient également de plus en plus de courriels.



Attention
Face à ces enjeux naissants, il faut définir des stratégies et acquérir de nouvelles habitudes.
La première des priorités est l'archivage car si les informations échangées par courrier électronique ont de la valeur, elles doivent être protégées.
De la même manière, si un document électronique a la même valeur qu'un document papier, il faut alors lui appliquer les mêmes règles de conservation dans le temps, à ceci près qu'un document électronique doit toujours bénéficier d'une copie de sauvegarde, étant donné sa fragilité.
Vous devez donc prendre autant de soin à conserver un courrier électronique que vous le feriez avec un document imprimé sur une feuille.

2.1.2. Sauvegarde du carnet d'adresse

Au fil du temps, votre carnet d'adresses va se remplir et il deviendra vitre un outil indispensable, surtout si vous décidez d'y saisir également les adresses et les numéros de téléphone de vos contacts. Si ce fichier vous est vraiment très utile, sa perte vous créerait d'énormes problèmes.



Conseil

Dans ces conditions, vous devez envisager d'en *faire des sauvegardes régulières* : *une fois par mois au moins*, plus souvent si l'ajout et la modification des informations sont plus fréquents.

2.2. Comment choisir son support de sauvegarde ?

Le problème du choix du support de sauvegarde ; pour vous guider dans votre choix, il faut prendre en compte les éléments suivants :
Coût ;
Facilité de sauvegarde ;
Facilité de restauration ;
Estimation de la longévité des sauvegardes.

2.2.1. Coût

En général, on estime le coût d'une sauvegarde en calculant le prix de revient au Mo ou au Go. Si, par exemple, un CD-R de 700 Mo coûte 0,50 Euro, le coût au Go sera donc de 0,71 Euro (0,5 / 0,7). Il est toujours intéressant de faire ce genre de calcul car cela permet de comparer facilement les supports physiques. On s'aperçoit ainsi que certains supports qui paraissent plus onéreux de prime abord sont en fait meilleur marché.



La sauvegarde en ligne

Généralisation de l'ADSL oblige, les possibilités de sauvegarde en ligne se multiplient. Si l'on n'a pas un gros volume de données à sauvegarder et que l'on dispose d'une connexion ADSL, cette solution est facile à mettre en oeuvre et très peu onéreuse.

Les clients des fournisseurs d'accès à Internet oublient souvent que leur FAI met également à leur disposition un espace pour créer des pages personnelles Web. Ce n'est pas parce que vous ne créez pas de pages perso qu'il faut laisser cet espace inutilisé. Il suffit d'apprendre à se servir d'un logiciel de FTP pour bénéficier ainsi d'un espace de stockage en ligne dont le volume est en général proche de 100 Mo.

On commence aussi à voir apparaître sur le marché plusieurs offres commerciales de stockage en ligne dont le coût abordable les destine aux particuliers.

Beaucoup de personnes pratiquaient déjà la sauvegarde en ligne sans le savoir en s'envoyant sur leur compte de courrier électronique les fichiers importants qu'ils désiraient conserver sous la main. Avec l'inflation du volume mis à la disposition des utilisateurs de Webmail, les possibilités de ce système sont encore renforcées, surtout si l'on utilise en plus un logiciel de compression.

2.2.2. Facilité de sauvegarde

Si vous avez pris la décision d'effectuer des sauvegardes de vos données, vous avez tout intérêt à privilégier un *système facile à mettre en oeuvre*. En effet, si votre système de sauvegarde nécessite l'arrêt total de vos activités, prend trois heures de votre temps et vous oblige à rester présent devant l'ordinateur, vous allez très vite renoncer à vos bonnes résolutions. Vous devez donc choisir une solution de sauvegarde qui soit la plus simple à mettre en place. Le choix que vous allez faire dépend en grande partie du *volume d'informations que vous avez à sauvegarder* :

- Si ce dernier est faible, de l'ordre de quelques centaines de Mo, vous pouvez tout à fait vous contenter d'une ou de plusieurs clés USB.
- En revanche, si vous avez de gros volumes à archiver (plusieurs Go de données), il vaut mieux penser à une solution de type disque dur externe.



Conseil

Lors du choix de votre système de sauvegarde, privilégiez toujours la *simplicité* et la *rapidité* à la sophistication. N'oubliez jamais qu'on n'utilise pas un système quand il est trop complexe.

2.2.3. Facilité de restauration

Ce n'est pas le tout de faire des sauvegardes, mais il faut aussi penser à la restauration qui est le mécanisme qui consiste à récupérer les informations à partir de la sauvegarde. Si vous vous contentez de récupérer quelques fichiers sur une clé USB, cela sera simple, mais si vous avez réalisé votre sauvegarde sur une bande ou une cartouche, la restauration d'un seul fichier du jeu de sauvegarde peut prendre plusieurs minutes. Cet élément est donc à prendre en compte et il faut là également privilégier la simplicité.



Conseil

Lors du choix de votre système de sauvegarde, évaluez le temps qu'il vous faudra pour retrouver vos informations en cas de sinistre.

2.2.4. Estimation de la longévité des sauvegardes

Il s'agit là du problème le plus épineux car aujourd'hui aucun fabricant ne sait prédire de manière fiable la longévité de son matériel, même si certains prétendent le contraire. Au moment où le support CD-R est apparu, certains industriels ont entrepris des recherches en laboratoire pour tenter de déterminer la durée de vie de leur média. Bien évidemment, toutes ces études reposent sur des simulations de vieillissement et rien n'indique qu'elles soient exactes.



Conseil

Il convient donc d'être très prudent en la matière et de ne pas accorder une foi excessive dans les déclarations des fabricants de support de sauvegarde. Par exemple, seul le temps nous permettra de connaître la durée de vie d'un CD-Rom.



Attention
Tout système de secours doit être régulièrement testé et c'est la raison pour laquelle on fait des exercices d'alerte au feu. Vos sauvegardes ne font pas exception à cette règle de base en matière de sécurité et vous devez donc régulièrement vérifier la qualité de vos sauvegardes.

2.3. La fréquence

Idéalement, dès que vous avez modifié une information, il faudrait en créer une copie de sauvegarde. Les systèmes professionnels fonctionnent d'ailleurs de la sorte grâce à des dispositifs de *disque miroir*, chaque information écrite sur un disque dur étant dupliquée instantanément sur un deuxième disque dur. Dans le cadre d'une utilisation domestique, il est bien évidemment impensable de procéder de la sorte.



Conseil
Nous vous conseillons de réaliser sur clé USB une sauvegarde des fichiers sur lesquels vous travaillez régulièrement dès que vous les avez modifiés ; nous préconisons d'autre part une sauvegarde hebdomadaire de votre système.



Attention
Si vous avez des documents vraiment importants, il est préférable de réaliser deux copies de sauvegarde et de les stocker dans deux endroits différents. En effet, si un incendie détruit votre habitation, il y a de grands risques pour que votre ordinateur et vos sauvegardes partent en fumée. Un utilisateur prudent conserve un deuxième jeu de sauvegarde dans un autre lieu.

3. Logiciels de sauvegarde

Bien évidemment, votre premier logiciel de sauvegarde sera l'*Explorateur Windows* dans la mesure où il permet de faire une copie de fichiers de votre disque dur sur une autre unité.

Vous noterez également *l'intérêt des logiciels de compression* qui permettent :
- d'une part de gagner de la place en réduisant la taille des fichiers ;
- d'autre part, de sauvegarder toute une série de fichiers et de dossiers sous un seul nom de fichier archivé.



Remarque
La notion de dossier compressé étant à présent intégrée dans les versions actuelles de Windows, les logiciels spécifiques de compression tels que *WinZip*, *WinRAR* ou bien encore *PowerArchiver* ont moins la cote, mais il peut toujours s'avérer utile d'avoir ce genre de logiciels dans sa boîte à outils car il n'est pas rare de tomber sur un format d'archive un peu ésotérique qui n'est pas pris en compte par Windows.



Conseil

Si vous ne possédez pas d'utilitaire de compression de fichiers, pointez votre navigateur sur le site http://www.telecharger.com et vous découvrirez une centaine de programmes dans la rubrique *Utilitaire > Compression et décompression*, dont certains sont gratuits.

Utilitaire de sauvegarde Windows

Absent des premières versions de Windows, le système d'exploitation offre depuis Windows 98 un utilitaire de sauvegarde. Ce dernier est bien caché et pour l'exécuter, vous devez cliquer sur la séquence *Démarrer > Tous les programmes > Accessoires > Outils système > Utilitaire de sauvegarde*.



Conseil

Lors de l'exécution de cet utilitaire, l'écran de démarrage vous propose d'utiliser un assistant ; si c'est la première fois que vous utilisez ce programme, nous vous conseillons d'employer l'assistant qui vous guidera pas à pas.



Attention

Même si l'Utilitaire de sauvegarde possède de nombreux assistants qui vous guideront lors des opérations de restauration, vous devez premièrement vous familiariser avec le fonctionnement de la restauration, ce qui signifie que vous devez vous entraîner à restaurer des données sauvegardées. En cas de plantage de votre système, vous serez ainsi habitué à cette opération et risquerez moins de commettre des erreurs dans cette situation d'urgence. Deuxièmement, vous devez tester le bon fonctionnement de votre sauvegarde (bons fichiers sauvegardés, qualité du support, etc.).

Ressources



Introduction à la sécurité informatique



Site "Comment ça marche?".



Virus et codes cachés



Attaques et arnaques



Site "Comment ça marche?".

Authentification

Site "Comment ça marche?".

Protection

Site "Comment ça marche?".

Contenus et comportements illicites

Site "Droit du Net".

Chapitre

IV

La protection des données confidentielles

Cliquez sur le lien ci-dessous afin de découvrir les menaces qui pèsent sur les infrastructures de signature numérique.

♦ Quelles sont les menaces ?

Partie A. La loi "Informatique et libertés"

1. Contexte et problématique

"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." (Talleyrand)

Depuis son avènement, l'informatique a libéré l'être humain d'un nombre considérable de tâches pénibles et peu intéressantes. En devenant communicante, la micro-informatique a également permis d'autres libérations comme le télétravail. Mais cette mise en réseau des PC, qu'elle se fasse au sein de l'entreprise ou bien par l'intermédiaire d'Internet, a également des côtés négatifs que l'actualité vient nous rappeler régulièrement. Depuis quelques années, un certain nombre de faits portés à la connaissance du public montrent que le syndrome orwellien de 1984 devient un peu plus réel chaque jour.

Dressons une liste rapide de quelques-uns de ces événements : autorisation d'utiliser le numéro INSEE pour l'administration fiscale, fichier de la police (STIC) déjà en service avant d'avoir été autorisé par la CNIL, numéro de série du Pentium III, procédure d'enregistrement de Windows XP, tatouage des documents Office. .

C'est une évidence de rappeler que chacun d'entre nous est fiché plusieurs centaines de fois et nous semblons avoir accepté cette situation avec la plus grande fatalité. Les belles âmes ont toujours d'excellentes justifications : il faut lutter contre la fraude fiscale, contre le piratage ou bien encore le terrorisme. Si l'on peut être parfaitement d'accord avec le principe de la lutte contre le piratage ou bien l'échange illégal de fichiers musicaux, encore faut-il que ces combats soient menés de manière licite. Dans les faits que nous avons mentionnés, *le plus répréhensible est bien évidemment le côté sournois et caché de ces procédures car si la loi Informatique et Libertés nous permet d'exercer un droit de regard sur les données nominatives qui ont été collectées, encore faut-il que nous soyons avertis que lesdites données ont été recueillies.*
Nous pensons donc qu'il ne s'agit pas là d'un fantasme de vieux barbon ayant du mal à intégrer la réalité des nouvelles technologies : il y a bien un réel danger pour la démocratie, d'autant plus important que les autoroutes de l'information font désormais partie du quotidien des Français. Comme nous allons le voir, il y a tout lieu de s'inquiéter du *manque de respect de la vie privée sur Internet.*
Notre propos n'est pas donc celui d'un moraliste, mais vise essentiellement à *rappeler la loi* (qu'en France nul n'est censé ignorer) et à *faire réfléchir au pouvoir de l'informatique*, ce qui implique la nécessaire élaboration d'un contre-pouvoir.

1.1. Contexte historique

Avant de rentrer dans le vif du sujet, il est nécessaire de rappeler brièvement le contexte historique dans lequel la législation traitant de l'informatique et des libertés a été élaborée.

- Dans le *courant des années 1970*, avec la montée en puissance de la mini-informatique et des mainframes, on a vu se développer toute une *série de projets de grande envergure visant à ficher les individus sur des supports magnétiques*. Les grandes administrations ont eu à concevoir des fichiers informatiques regroupant peu ou prou la totalité de la population française (fichier des services fiscaux, de la sécurité sociale, etc.).
- Puis le *projet SAFARI* est né : il prévoyait l'*interconnexion des fichiers émanant de services publics sur la base d'un identifiant unique, le numéro INSEE*. Certains esprits se sont alors émus des dangers d'un tel projet et un groupe de travail, sous la présidence du conseiller d'État Tricot, a été créé. Les travaux de cette commission sont à l'origine de la *loi du 6 janvier 1978 sur les rapports entre l'informatique et les libertés*, et de la *Commission nationale de l'informatique et des libertés (CNIL)* qui est chargée de veiller au respect de la loi.



Conseil

Tous ceux qui s'intéressent à la problématique des rapports entre l'informatique et les libertés peuvent consulter le site web de la CNIL qui est une véritable référence en la matière. Sont notamment accessibles en ligne les rapports annuels publiés par la CNIL, qui sont une mine d'informations. Toujours passionnants, ils épinglent les pratiques délictueuses et dressent un inventaire des problèmes actuels relatifs aux traitements de données à caractère personnel.

1.2. Problématique

Avant de décrire la loi et le rôle de la CNIL, il nous faut poser la problématique de l'informatique et des libertés. Si nous sommes tous convaincus de l'utilité et du progrès de l'informatisation, il faut bien *être conscient des dangers que peut comporter le fait que des informations nominatives soient stockées dans des ordinateurs et puissent être facilement exploitées, recoupées et analysées*.
En effet, l'*article 9 du code civil* qui reconnaît le *droit au respect de la vie privée* est souvent mis à mal par la constitution de fichiers nominatifs. Auparavant, il faut bien reconnaître que de tels fichiers manuels existaient, mais leur exploitation était trop lourde pour être vraiment menaçante. Aujourd'hui, avec la puissance de l'informatique, les fichiers nominatifs deviennent des enjeux de toute nature.

Pour être plus précis, nous citerons trois exemples concrets de cas où la mauvaise utilisation de fichiers peut être préjudiciable aux libertés individuelles.

Exemple

- Le premier grand risque est l'*interconnexion des fichiers* : seule la personne qui a recueilli l'information est en droit de l'exploiter. Le principe du secret professionnel ne doit pas être bafoué. Si les fichiers sont interconnectés, rien n'empêche par exemple votre banquier de savoir que vous êtes atteint d'une maladie virale ou bien votre médecin d'apprendre que vous êtes interdit de chéquier.
- Se pose aussi le problème du *détournement des fichiers de leur usage primitif*. Les journaux se font assez régulièrement l'écho de piratages de fichiers publics ou privés à des fins commerciales ou politiques : ainsi, un syndicat d'une entreprise publique produisant de l'énergie s'est vu épingler par la CNIL pour avoir détourné le fichier du personnel.
- Enfin, il peut arriver que les *informations stockées soient inexactes*. De telles erreurs peuvent entraîner des injustices sans que l'intéressé en soit même averti. Se pose alors la question du droit d'accès aux informations et de la modification des informations faussement saisies.

* *
*

Les missions de la CNIL - Commission Nationale Informatique et Libertés - consistent à :

- recenser et contrôler les fichiers ;
- réglementer ;
- garantir le droit d'accès ;
- instruire les plaintes ;
- informer.

2. Le texte de la loi du 6 janvier 1978

2.1. Article 1

La loi du 6 janvier 1978 tâche de répondre à ces questions et ses principes sont résumés dans le premier article :

Extrait de texte légal

" 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." (Article 1 de la loi du 6 janvier 1978.)

Pour garantir le respect des règles qu'elle édicte, la loi crée une institution de contrôle : la *Commission Nationale de l'Informatique et des Libertés*. Pour assurer la transparence des fichiers informatisés, la loi instaure un système de formalités

préalables à la mise en oeuvre des traitements automatisés.



Remarque

La loi du 6 janvier 1978 fut une des premières lois au monde à encadrer l'usage des fichiers informatiques. En 1995, l'Union européenne accoucha d'une directive (n° 95/46 CE du 24 octobre) sur la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation des données. La France avait trois ans pour transcrire cette directive européenne et dans la mesure où nos gouvernements successifs ont quelque peu tardé dans la transposition, la directive européenne est entrée automatiquement en vigueur le 25 octobre 1998. En effet, peu de gens le savent, mais il faut ici rappeler que tout individu qui subit des dommages suite au manquement d'un État membre de transposer une directive, est autorisé à obtenir des réparations devant les tribunaux nationaux, aux termes d'une jurisprudence de la Cour de Justice (affaire Francovich).

La France s'est enfin décidée à transposer la directive européenne, presque dix ans après sa publication, avec la loi du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel. Pour autant, on a gardé la référence originale à la loi du 6 janvier 1978.
La loi de 1978 comportait 48 articles et la loi de 2004 en compte 72. Pour résumer, on peut dire que la nouvelle a renforcé les pouvoirs de la CNIL, élargi son champ d'application, augmenté les droits des personnes tout en simplifiant les procédures administratives. Vous trouverez une analyse détaillée des différences entre les deux lois sur le site de la CNIL à l'adresse suivante : http://www.cnil.fr/index.php?id=1744

Vous trouverez une version du texte consolidé (c'est-à-dire prenant en compte toutes les modifications législatives) de la loi du 6 janvier 1978 à l'adresse suivante : http://www.cnil.fr/index.php?id=301

La loi réglemente la collecte l'enregistrement et la conservation des informations nominatives; elle reconnaît des droits aux individus et met des obligations à la charge des détenteurs de fichiers informatiques ou manuels.



Attention

Beaucoup de gens pensent que la loi ne concerne que les fichiers automatisés, c'est-à-dire informatiques. En fait, la loi s'applique à tous les fichiers nominatifs, même ceux qui figurent sur de bonnes vieilles fiches bristol.

2.2. Article 2

Le grand mérite de la loi (dans son article 2) est de *définir précisément ce qu'est une donnée personnelle ainsi que les traitements qui s'y appliquent.*



Extrait de texte légal

" Constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne. Constitue un traitement de données à caractère personnel toute opération ou tout ensemble d'opérations portant sur de telles données, quel que soit le procédé utilisé, et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction." (Article 2 de la loi du 6 Janvier 1978.)



Remarque

Que les possesseurs d'agenda électronique se rassurent : le champ d'application de la loi écarte les traitements mis en oeuvre pour l'exercice d'activités exclusivement personnelles, ce qui signifie que les contacts de votre carnet d'adresses ne sont pas pris en compte par cette loi.



Rappel

Bien que l'on parle en général de données nominatives, il convient de bien comprendre que toute information qui permet d'identifier une personne est une donnée nominative. Cela signifie qu'une adresse électronique, l'adresse IP que vous attribue votre fournisseur d'accès à Internet ou bien encore votre numéro de téléphone sont des données à caractère personnel dont l'utilisation est encadrée par la loi.

2.3. Article 6

L'article 6 de la loi *définit la manière dont les données à caractère personnel peuvent être traitées* ; il définit notamment les points suivants :

- Les données sont collectées et traitées de manière loyale et licite ;
- Elles sont collectées pour des finalités déterminées, explicites et légitimes et ne sont pas traitées ultérieurement de manière incompatible avec ces finalités ;
- Elles sont adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et de leurs traitements ultérieurs ;
- Elles sont exactes, complètes et, si nécessaire, mises à jour ; les mesures appropriées doivent être prises pour que les données inexactes ou incomplètes au regard des finalités pour lesquelles elles sont collectées ou traitées soient effacées ou rectifiées ;
- Elles sont conservées sous une forme permettant l'identification des personnes concernées pendant une durée qui n'excède pas la durée nécessaire aux finalités pour lesquelles elles sont collectées et traitées.

2.4. Article 7

L'article 7 de la loi précise qu'*un traitement de données à caractère personnel doit avoir reçu le consentement de la personne concernée*.



Remarque
Il existe bien évidemment des cas où l'on ne vous demande pas votre avis, mais ces exceptions sont bien définies et encadrées par la loi (obligation légale, exécution d'une mission de service public, intérêt légitime poursuivi par le responsable du traitement, etc.)

2.5. Article 8

L'article 8 précise qu'il est interdit de collecter ou de traiter des données à caractère personnel qui font apparaître, directement ou indirectement :

- les origines raciales ou ethniques
- les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes
- les informations qui sont relatives à la santé ou à la vie sexuelle des personnes.



Remarque
Bien évidemment, la loi prévoit des exceptions et l'on comprend bien qu'un chercheur en médecine puisse réaliser une enquête comportant des questions relatives à la santé.

2.6. Article 9

L'article 9 de la loi est intéressant à plus d'un titre et nous le reproduisons ci-dessous intégralement :



Extrait de texte légal
Les traitements de données à caractère personnel relatives aux infractions, condamnations et mesures de sûreté ne peuvent être mis en oeuvre que par :

1. Les juridictions, les autorités publiques et les personnes morales gérant un service public, agissant dans le cadre de leurs attributions légales ;
2. Les auxiliaires de justice, pour les stricts besoins de l'exercice des missions qui leur sont confiées par la loi ;
3. [Dispositions déclarées non conformes à la Constitution par décision du Conseil constitutionnel n° 2004-499 DC du 29 juillet 2004 ;]
4. Les personnes morales mentionnées aux articles L. 321-1 et L. 331-1 du code de la propriété intellectuelle, agissant au titre des droits dont elles assurent la gestion ou pour le compte des victimes d'atteintes aux droits prévus aux livres Ier, II et III du même code aux fins d'assurer la défense de ces droits.



Remarque
Cet article encadre donc les fichiers de la police et de la justice. Il est intéressant de noter que l'article 3 a été censuré par le Conseil constitutionnel. Cela prouve, s'il en était encore besoin, que le problème de l'informatique et des libertés est un sujet sensible et qu'un certain nombre de députés ont cru bon d'interpeller le Conseil constitutionnel qui leur a donné en partie raison.



Complément
La décision motivée du Conseil constitutionnel peut être consultée en cliquant sur ce lien



Attention
La lecture de l'alinéa 4 pour les personnes qui ne sont pas habituées aux textes juridiques peut sembler complètement absconse.
En fait, ces quelques phrases sont ce que l'on appelle un *texte de circonstance* car c'est sur sa base que les industriels du disque vont pouvoir *poursuivre les internautes adeptes des échanges de fichiers grâce aux réseaux peer to peer (P2P)*.
En clair, les maisons de disques vont pouvoir *collecter les adresses IP* de ceux qui s'adonnent aux joies du P2P et demander à un juge d'ordonner à un FAI de *fournir l'identité du titulaire de l'abonnement Internet*.

2.7. Articles 11 à 31

Les articles 11 à 21 de la loi définissent *la composition et le rôle de la CNIL*.



Remarque
Il faut noter que *la CNIL n'est pas un tribunal*, mais *une autorité administrative indépendante*. Son rôle est de *regrouper* et de *contrôler l'ensemble des déclarations des traitements automatisés d'informations nominatives*.

Les articles 22 à 31 décrivent les formalités de ces déclarations.

2.8. Articles 32 à 37

Les articles 32 à 37 de la loi décrivent les *obligations incombant aux responsables des traitements*.



Conseil
Nous vous encourageons vivement à lire la totalité de ces articles, ce qui permettra de vous rendre compte que la majeure partie des questionnaires que vous remplissez en ligne ne respecte pas ces obligations.

2.9. Articles 38 à 43

Les articles 38 à 43 de la loi précisent les *droits des personnes qui sont l'objet d'un traitement de données à caractère personnel*.

Nous vous conseillons d'apprendre par coeur l'article 38 de cette loi et d'en user autant

que vous le voulez :



Extrait de texte légal

" Toute personne physique a le droit de s'opposer, pour des motifs légitimes, à ce que des données à caractère personnel la concernant fassent l'objet d'un traitement. " (Article 38 de la loi du 6 janvier 1978.)

"Elle a le droit de s'opposer, sans frais, à ce que les données la concernant soient utilisées à des fins de prospection, notamment commerciale, par le responsable actuel du traitement ou celui d'un traitement ultérieur." (Article 38 de la loi du 6 janvier 1978.)



Remarque

C'est grâce au deuxième alinéa de cet article que l'on peut désormais faire figurer son numéro de téléphone en liste rouge sans avoir besoin de payer quoi que ce soit.

* *
*

Pour résumer, une personne peut exercer les droits suivants face à un traitement de données à caractère personnel :

- *Droit d'être informé* sur la nature du traitement ;
- *Droit de s'opposer* au traitement ;
- *Droit d'accès* aux données collectées ;
- *Droit de rectification* des données.

2.10. Articles 45 à 52

Les articles 45 à 49 de la loi définissent les *sanctions que peut prendre la CNIL lorsqu'un responsable d'un traitement de données ne respecte pas ses obligations*.

Les articles 50 à 52 précisent les *sanctions pénales prévues par la loi en cas d'infraction*.

Ces infractions ont d'ailleurs été reprises dans le code pénal (*articles 226-16 à 226-24*).



Exemple

À titre indicatif, le fait, y compris par négligence, de procéder ou de faire procéder à des traitements de données à caractère personnel sans qu'aient été respectées les formalités préalables à leur mise en oeuvre prévues par la loi est puni de *cinq ans d'emprisonnement* et de *300 000 Euros d'amende*.

* *
*

Voir annexe A en fin de fascicule

Partie B. La LCEN

1. Principes

La *loi du 21 juin 2004 pour la confiance dans l'économie numérique* (ou *LCEN*) est un texte qui a mis du temps à aboutir. En effet, la LCEN est quelque part l'héritière du projet baptisé *Loi sur la société de l'information* (*LSI*) que le gouvernement de Lionel Jospin avait mis en chantier, mais qui n'a jamais vu le jour. Pourtant, dès le mois d'août 1997, le gouvernement avait fait de l'entrée de la France dans la société de l'information une de ses priorités.

Malgré cette volonté affichée, les députés ont mis 5 ans (juin 2001) pour accoucher d'un projet de 32 pages qui n'a jamais pu passer devant l'Assemblée nationale. Arrivé au pouvoir, Jean-Pierre Raffarin a choisi d'abandonner ce projet pour en remettre un autre en route, la LCEN. Il aura également fallu 2 ans pour que ce texte de loi voit le jour et soit publié au Journal Officiel. Certes, d'autres textes importants ont quand même été adoptés pendant cette période, comme celui sur la signature électronique, mais on a quand même dû attendre une année entre le vote de cette loi et la publication de son décret d'application.

La LCEN était attendue car il commençait à y avoir urgence sur plusieurs fronts. En effet, plusieurs problèmes relatifs à la *responsabilité des hébergeurs*, à la *lutte contre le spam* ou bien encore à la *libéralisation totale de la cryptographie* n'étaient pas réglés et les professionnels de l'Internet réclamaient à grands cris le vote d'une loi.

Remarque
La LCEN, qui compte 58 articles, est une loi vraiment importante pour Internet. Dans le cadre de cette formation, il nous est impossible de citer tous les articles qui la composent, mais nous vous conseillons de consulter le document en téléchargement ci-dessous et même d'aller sur le site de Legifrance pour la lire intégralement.

2. Le texte de la LCEN

2.1. Article 1

Dans son premier article, la LCEN affirme un principe de liberté :

Extrait de texte légal
" La communication au public par voie électronique est libre. " (Article 1 de la LCEN.)

"L'exercice de cette liberté ne peut être limité que dans la mesure requise, d'une part, par le respect de la dignité de la personne humaine, de la liberté et de la propriété d'autrui, du caractère pluraliste de l'expression des courants de pensée et d'opinion et, d'autre part, par la sauvegarde de l'ordre public, par les besoins de la défense nationale, par les exigences de service public, par les

contraintes techniques inhérentes aux moyens de communication, ainsi que par la nécessité, pour les services audiovisuels, de développer la production audiovisuelle." (Article 1 de la LCEN.)

2.2. Article 2

L'article 2 de la LCEN précise des définitions qui n'avaient jamais été données auparavant :



Extrait de texte légal

" On entend par communications électroniques les émissions, transmissions ou réceptions de signes, de signaux, d'écrits, d'images ou de sons, par voie électromagnétique." (Article 2 de la LCEN.)

"On entend par communication au public par voie électronique toute mise à disposition du public ou de catégories de public, par un procédé de communication électronique, de signes, de signaux, d'écrits, d'images, de sons ou de messages de toute nature qui n'ont pas le caractère d'une correspondance privée." (Article 2 de la LCEN.)



Remarque

C'est désormais le Conseil supérieur de l'audiovisuel (CSA) qui a la mission de garantir l'exercice de la liberté de communication audiovisuelle en matière de radio et de télévision par tout procédé de communication électronique

2.3. Chapitre II - Article 6

Le Titre II de la LCEN traite du *commerce électronique* qu'il définit comme *l'activité économique par laquelle une personne propose ou assure à distance et par voie électronique la fourniture de biens ou de services*. Le commerce électronique couvre aussi les *services* tels que ceux consistant à *fournir des informations en ligne*, des *communications commerciales* et des *outils de recherche*, d'*accès et de récupération de données*, d'*accès à un réseau de communication ou d'hébergement d'informations*, y compris lorsqu'ils ne sont pas rémunérés par ceux qui les reçoivent.
Le Chapitre II de la LCEN règlemente *la publicité par voie électronique* mais il s'agit là plus d'une tentative de régler les problèmes posés par l'inflation croissance du spam.
Le Chapitre II de la LCEN traite également des *fournisseurs d'accès à Internet* (*FAI*) appelés dans la loi prestataires techniques.

L'article 6 règle le délicat problème de la *responsabilité des hébergeurs*.



Rappel

Il faut ici rappeler qu'en cas de contenu illicite publié sur un site Web, l'hébergeur pouvait être déclaré complice. Les hébergeurs prétendaient à juste titre qu'ils ne pouvaient pas surveiller tous leurs clients étant donné leur grand nombre et que la mission de contrôle du contenu de ce qui passait dans leurs tuyaux ne pouvait pas leur incomber.



Extrait de texte légal

Le législateur leur a donné satisfaction et précise que *"les personnes physiques ou morales qui assurent, même à titre gratuit, pour mise à disposition du public par des services de communication au public en ligne, le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par des destinataires de ces services ne peuvent pas voir leur responsabilité civile engagée du fait des activités ou des informations stockées à la demande d'un destinataire de ces services si elles n'avaient pas effectivement connaissance de leur caractère illicite ou de faits et circonstances faisant apparaître ce caractère ou si, dès le moment où elles en ont eu cette connaissance, elles ont agi promptement pour retirer ces données ou en rendre l'accès impossible" (Article 6 de la LCEN.)* .



Remarque

Un autre alinéa précise que la *responsabilité pénale de l'hébergeur n'est pas non plus engagée*.

Ce texte règle donc le problème de la responsabilité a priori de l'hébergeur. La loi précise clairement que *les FAI ne sont pas soumis à une obligation générale de surveiller les informations qu'ils transmettent ou stockent, ni à une obligation générale de rechercher des faits ou des circonstances révélant des activités illicites*.



Attention

En revanche, *si un FAI est avisé d'un contenu illicite mis en ligne sur la page personnelle d'un de ses clients, il doit immédiatement faire cesser le trouble*.

Le législateur a quand même pris une mesure pour limiter les recours des personnes qui voudraient faire cesser la publication d'une information sur un site Web. Ainsi toute personne qui présenterait à un hébergeur un contenu ou une activité comme étant illicite dans le but d'en obtenir le retrait ou d'en faire cesser la diffusion, alors qu'elle sait cette information inexacte, serait punie d'une peine d'*un an d'emprisonnement* et de *15 000 euros d'amende*.

Les FAI doivent *conserver pendant un an les données de nature à permettre l'identification de quiconque a contribué à la création du contenu* ou de l'un des contenus des services dont elles sont prestataires.

* *
*

La LCEN tente de *responsabiliser les FAI en matière de droit d'auteur*. Ainsi lorsqu'un FAI évoque dans une publicité la possibilité de télécharger des fichiers dont il n'est pas le fournisseur, il doit faire figurer dans cette publicité une mention facilement identifiable et lisible rappelant que le piratage nuit à la création artistique.

Le FAI a également l'*obligation de suspendre, par tout moyen, le contenu d'un site Web portant atteinte à l'un des droits de l'auteu*r, y compris en ordonnant de cesser de stocker ce contenu ou, à défaut, de cesser d'en permettre l'accès.

2.4. Article 20



Extrait de texte légal

L'article 20 stipule que *"toute publicité, sous quelque forme que ce soit, accessible par un service de communication au public en ligne, doit pouvoir être clairement identifiée comme telle. Elle doit rendre clairement identifiable la personne physique ou morale pour le compte de laquelle elle est réalisée" (Article 20 de la LCEN.)* .

La loi enfonce le clou en précisant que *"dans tous les cas, il est interdit d'émettre, à des fins de prospection directe, des messages au moyen d'automates d'appel, télécopieurs et courriers électroniques, sans indiquer de coordonnées valables auxquelles le destinataire puisse utilement transmettre une demande tendant à obtenir que ces communications cessent sans frais autres que ceux liés à la transmission de celle-ci. Il est également interdit de dissimuler l'identité de la personne pour le compte de laquelle la communication est émise et de mentionner un objet sans rapport avec la prestation ou le service proposé"* .



Attention

Signalons un système pernicieux mis en place par certaines sociétés peu scrupuleuses :

Vous recevez un courriel publicitaire au bas duquel figure un lien permettant de vous désabonner et de ne plus recevoir ainsi de publicité. Vous cliquez sur ce lien qui affiche une page Web vous demandant de saisir votre adresse électronique. Si vous possédez plusieurs adresses électroniques grâce à des systèmes de redirection et que le champ "*Destinataire*" a été masqué par le spam, vous êtes alors incapable de savoir quelle adresse électronique il faut inscrire dans le formulaire de désabonnement.

D'autre part, on peut légitimement se demander si une telle pratique n'est pas une *méthode pour vérifier si votre adresse est bien valide*. En général, quand on écrit à quelqu'un, on connaît son adresse électronique et si on souhaite lui donner la possibilité de ne plus lui envoyer de courrier, on n'a pas besoin de la lui demander.

2.5. Chapitre III

Le Chapitre III de la LCEN consacre *l'usage de l'écrit sous forme électronique grâce à la signature électronique*.

Ainsi, lorsqu'un écrit est exigé pour la *validité d'un acte juridique*, il peut être *établi et conservé sous forme électronique*.

De la même manière, lorsqu'est exigée une mention écrite de la main même de celui qui s'oblige, ce dernier peut l'apposer sous forme électronique si les conditions de cette apposition sont de nature à garantir qu'elle ne peut être effectuée que par lui-même.

La LCEN définit également la manière dont *les contrats sous forme électronique peuvent être conclus*.

2.6. Article 29

Le Titre III de la LCEN, intitulé "*De la sécurité dans l'économie numérique*" traite des *moyens et prestations de cryptologie*.



Extrait de texte légal

L'article 29 propose les définitions suivantes :

" On entend par moyen de cryptologie tout matériel ou logiciel conçu ou modifié pour transformer des données, qu'il s'agisse d'informations ou de signaux, à l'aide de conventions secrètes ou pour réaliser l'opération inverse avec ou sans convention secrète. Ces moyens de cryptologie ont principalement pour objet de garantir la sécurité du stockage ou de la transmission de données, en permettant d'assurer leur confidentialité, leur authentification ou le contrôle de leur intégrité. " (Article 29 de la LCEN.)
" On entend par prestation de cryptologie toute opération visant à la mise en oeuvre, pour le compte d'autrui, de moyens de cryptologie." (Article 29 de la LCEN.)

2.7. Article 30



Extrait de texte légal

L'article 30 est une véritable révolution car *"il énonce que l'utilisation des moyens de cryptologie est libre"* . Les professionnels de la sécurité attendaient cette disposition réglementaire depuis des années et ils ont donc toutes les raisons de s'en satisfaire. Cela étant, l'alinéa suivant précise que *"la fourniture, le transfert depuis ou vers un Etat membre de la Communauté européenne, l'importation et l'exportation des moyens de cryptologie assurant exclusivement des fonctions d'authentification ou de contrôle d'intégrité sont libres" (Article 30 de la LCEN.)* .



Remarque

On ne comprend pas bien à la lecture de ce texte pourquoi le législateur a tenu à préciser son propos dans la mesure où il indiqué plus que la *cryptologie était libre*. En y regardant de plus près, on s'aperçoit que *sont libres l'utilisation de la cryptologie pour authentifier et contrôler l'intégrité*. Quelle est donc l'autre fonction de la cryptologie qui manque dans cette énonciation ? Si vous avez suivi, vous savez que la cryptologie sert bien évidemment aussi à masquer, cacher, chiffrer des informations.

Bizarrement, cette fonctionnalité de la cryptologie n'est pas indiquée dans cet alinéa. On comprend mieux pourquoi quand on lit le suivant :
"La fourniture, le transfert depuis un Etat membre de la Communauté européenne ou l'importation d'un moyen de cryptologie n'assurant pas exclusivement des fonctions d'authentification ou de contrôle d'intégrité sont soumis à une déclaration préalable auprès du Premier ministre, sauf dans les cas prévus au b du présent III."

On reste dubitatif quand on considère un pareil énoncé : pourquoi ne pas appeler

un chat un chat ? La cryptologie qui chiffre est donc désignée par la périphrase *"moyen de cryptologie n'assurant pas exclusivement des fonctions d'authentification ou de contrôle d'intégrité"* .



Complément

Au cas où le lecteur n'aurait pas compris, le législateur indique que les outils qui ne sont pas soumis à déclaration sont *"les catégories de moyens dont les caractéristiques techniques ou les conditions d'utilisation sont telles que, au regard des intérêts de la défense nationale et de la sécurité intérieure ou extérieure de l'Etat, leur fourniture, leur transfert depuis un Etat membre de la Communauté européenne ou leur importation peuvent être dispensés de toute formalité préalable" (LCEN)* .

Bref, ce texte signifie que l'on peut chiffrer ses fichiers tant que cela ne nuit pas aux intérêts de l'armée et de la police. Dans ces conditions, la cryptologie est-elle vraiment libre ?

Pour tous ceux qui n'auraient encore pas compris, le législateur précise que le fait de fournir des prestations de cryptologie visant à assurer des fonctions de confidentialité sans avoir satisfait à l'obligation de déclaration prévue à l'article 31 est puni de deux ans d'emprisonnement et de 30 000 euros d'amende.



Attention

*La LCEN modifie également le code pénal*en indiquant que *lorsqu'un moyen de cryptologie a été utilisé pour préparer ou commettre un crime ou un délit, ou pour en faciliter la préparation ou la commission, cela constitue une circonstance aggravante qui accroît le nombre d'années de prison de la peine prévue*.

2.8. Article 39



L'article 39 de la LCEN paraît tellement étonnant que nous ne résistons pas au plaisir de vous le soumettre :

" Les dispositions du présent chapitre ne font pas obstacle à l'application du décret du 18 avril 1939 fixant le régime des matériels de guerre, armes et munitions, à ceux des moyens de cryptologie qui sont spécialement conçus ou modifiés pour porter, utiliser ou mettre en oeuvre les armes, soutenir ou mettre en oeuvre les forces armées, ainsi qu'à ceux spécialement conçus ou modifiés pour le compte du ministère de la défense en vue de protéger les secrets de la défense nationale. " (Article 39 de la LCEN.)

* *
*

La LCEN se termine sur des dispositions sur les *systèmes satellitaires* et la *couverture du territoire par les services numériques*.

Au final, *la LCEN est un texte juridique complexe et incomplet dans la mesure où il manque de nombreux décrets d'application importants*, ce qui semble être une véritable spécialité française. En effet, on ne compte plus le nombre de textes votés, mais inappliqués en raison de la non publication des décrets d'application. Encore récent, ce texte a également besoin que la jurisprudence en précise certaines orientations. Il n'en reste pas moins qu'il s'agit du *texte principal qui régit le droit de l'Internet. En tant que tel, il paraît difficile de l'ignorer si l'on est internaute*.

Voir annexe B en fin de fascicule

Partie C. La cryptologie

Préambule

Parler de cryptologie est un exercice très délicat.

Dans l'esprit du grand public, la cryptographie évoque souvent l'image des casseurs de code mythiques comme Alan Turing qui réussit à déchiffrer le code de l'Enigma, ce qui permit aux alliés de débarquer un an plus tôt en Normandie pendant la Deuxième Guerre mondiale.
Pour les spécialistes, la cryptologie n'est qu'une affaire de factorisation et de nombres premiers ; ne dit-on pas d'ailleurs que le premier employeur de mathématiciens au monde est la *NSA* (*National Security Agency*), le service de renseignements américain qui pilote le programme d'écoute Echelon ?

L'usage de la *cryptographie* a longtemps été réservé en France aux gens qui sont chargés de préparer la guerre, à savoir les militaires. Les politiques ayant finalement compris que ces restrictions législatives étaient un frein énorme au développement du commerce électronique, la loi a été modifiée et les moyens cryptographiques ne sont plus désormais considérés comme des armes de guerre.

Quand on conseille à un utilisateur d'employer un outil de cryptographie, son premier réflexe est de prétendre qu'il n'a rien à cacher. Quand bien même cela serait vrai (ce qui reste encore à prouver...), nous allons voir que les enjeux de la cryptographie sont tout autres et que *la cryptologie est aujourd'hui au centre de toute démarche sécuritaire en informatique*.

1. Présentation



La cryptographie

- La cryptographie est la science qui étudie les *moyens de chiffrer* (c'est à dire de rendre secrets) et de *déchiffrer des messages*.
- Un message est chiffré (ou codé) à l'aide d'une *clé* (ou chiffre). La clé peut être aussi simple qu'un décalage ou une permutation de lettres.
- Le passage du texte codé au texte en clair, en utilisant la clé de chiffrement, est appelé *déchiffrement*.
- Le *décryptement* est l'opération qui consiste à obtenir le texte en clair à partir du texte codé, sans connaissance de la clé de chiffrement.

La cryptographie est très ancienne puisque Jules César l'utilisait déjà ; pendant deux mille ans, les techniques cryptographiques se sont affinées, allant jusqu'à donner naissance à des machines sophistiquées comme l'Enigma.

La cryptographie à clé symétrique

Si le chiffre est devenu au fil du temps de plus en plus complexe, le principe reste identique : c'est *la même clé qui sert à la fois à chiffrer et à déchiffrer les messages*.
Ce système, appelé *cryptographie à clé symétrique*, comporte cependant une grosse lacune : si l'on veut que son correspondant puisse déchiffrer les messages codés qu'on lui envoie, il faut bien lui faire parvenir la clé.
Cette opération est le maillon faible de la cryptographie symétrique car, à ce moment-là, la clé peut être interceptée. Dans les années 1970, plusieurs chercheurs ont exploré d'autres pistes afin de trouver un autre système qui permette de faire l'économie de l'échange des clés. Ainsi naquit le concept de cryptographie à clé publique (ou asymétrique) qui allait s'imposer comme le pivot central de toute la cryptographie moderne.

La cryptographie publique

Dans un système cryptographique symétrique, on utilise la même clé pour chiffrer et déchiffrer
Avec la *cryptographie à clé publique*, on emploie *deux clés*: *la clé publique pour chiffrer* et *la clé privée pour déchiffrer*. Les deux clés sont liées par une fonction mathématique très complexe qui a la particularité de ne pas être réversible. Cela signifie en clair que *la clé publique est calculée à partir de la clé privée*, mais que l'on ne peut pas déduire la clé privée si l'on connaît la clé publique.
Avec ce système, le problème de l'échange des clés est résolu car les correspondants n'ont besoin de s'échanger que leur clé publique qui ne sert qu'à chiffrer un message. Cela fonctionne un peu comme un cadenas : on peut le fermer, mais si l'on ne connaît pas la combinaison, on ne peut pas l'ouvrir.

Illustration des principes de fonctionnement de la cryptographie publique

Quand Bernard veut envoyer à Alice un message crypté, il procède de la manière suivante :

- Bernard demande à Alice sa clé publique.
- Alice la lui envoie par courrier électronique.
- Bernard chiffre son message à l'aide de la clé publique d'Alice.
- Bernard envoie son message chiffré à Alice.
- Alice utilise la clé privée pour déchiffrer le message de Bernard.

Avec ce système, ni l'un ni l'autre n'a dû envoyer une clé privée.

2. Pourquoi utiliser la cryptologie ?

En France, l'usage de la cryptographie a été très longtemps encadré et sa libéralisation partielle est somme toute relativement récente puisqu'elle ne date que de 1998. Avant cette date, la France était la seule démocratie occidentale à bénéficier d'une législation aussi restrictive, preuve s'il en est de la puissance du lobby militaire.

Aujourd'hui, les choses ont heureusement changé, mais le combat législatif a laissé des traces et les différentes lois votées montrent bien que les parties en présence, à savoir les *marchands*, les *citoyens* et la *puissance publique* n'ont pas vraiment les mêmes préoccupations. On se retrouve donc dans un conflit d'intérêt assez classique dont les enjeux démocratiques sont pourtant fondamentaux.
Les marchands veulent commercer en toute sécurité et donc fiabiliser toutes les transactions comme c'est déjà le cas avec les cartes bancaires. *Internet n'étant pas spécialement sécurisé, les protocoles cryptographiques restent à normaliser si l'on souhaite développer le commerce électronique*.
La puissance publique, quant à elle, voit d'un très mauvais oeil le développement d'Internet conjointement aux progrès considérables de la cryptologie ; en effet, si intercepter une communication téléphonique est toujours possible et assez simple[Même avec le système GSM qui est pourtant crypté ; mais les autorités ont les clés...], la lecture d'un courrier électronique encodé grâce au *logiciel PGP* peut donner beaucoup plus de fil à retordre à n'importe quel service du chiffre pourtant richement doté en machines multiprocesseurs.
L'État, qui veut donc se réserver le droit de pouvoir lire à livre ouvert les correspondances de ses sujets, doit normalement, dans cette optique, interdire ou contrôler sévèrement la mise en oeuvre de moyens cryptologiques. L'argument invoqué est d'ailleurs toujours le même : *il faut pouvoir lutter efficacement contre le crime organisé et les mouvements terroristes*. Face à cette menace, différentes associations dans le monde n'en demandent pas moins la levée immédiate de toutes les entraves à la liberté de crypter et revendiquent ainsi un droit absolu à la confidentialité des correspondances, de quelque nature qu'elle soit.



Remarque

On voit donc bien que parler de *cryptologie* n'est pas une chose aisée car cette *activité scientifique* a de *multiples implications dans des domaines aussi variées que le commerce, la communication et les libertés publiques*.
Si l'on essaye de confronter les différents points de vue en présence, il faut d'abord parler des commerçants qui veulent pouvoir offrir à leurs clients des *moyens de paiement sécurisés*. Si l'on se focalise aujourd'hui sur le *commerce électronique et notamment par Internet*, il faut rappeler que les *banques* ont été les premières grosses consommatrices de cryptologie et que la carte à puce que chacun possède fait bien évidemment usage de procédés cryptographiques. Il est donc clair que le développement du commerce sur Internet ne pouvait pas faire l'économie d'un assouplissement de la législation en la matière.

La cryptologie est la science du secret et ceux qui prétendent ne rien avoir à cacher ne voient pas l'intérêt de passer du temps à comprendre l'utilisation d'une telle technologie.

Outre le fait qu'il n'est pas certain que vous n'ayez rien à cacher puisque, pour reprendre la célèbre formule de *Florian*, *"pour vivre heureux, vivons cachés "* , il faut bien comprendre que *la cryptologie est le seul moyen efficace* que l'on possède aujourd'hui pour *sécuriser certaines opérations en ligne*.
En effet, la cryptologie, aussi bizarre que cela puisse paraître, ne sert pas qu'à crypter, mais on l'utilise également pour la *signature électronique* qui est promise à un bel avenir. Si l'on veut développer toute une série de services en ligne, comme la *dématérialisation* de certaines démarches administratives, il est obligatoire d'utiliser des moyens cryptographiques.



Exemple

Par exemple, si vous faites partie de ces Français qui ont fait leur déclaration d'impôt par Internet, vous avez utilisé une des multiples applications de la cryptographie.

* *
*

La cryptologie est donc très utile dans notre monde virtuel et il faut donc apprendre à l'apprivoiser. L'autre raison est qu'il s'agit d'un domaine sensible pour les libertés publiques, ce qui signifie qu'il vaut mieux en avoir une vision claire si l'on veut exercer son pouvoir de citoyen. Enfin, la cryptologie est un sujet qui touche à de nombreuses disciplines intellectuelles et son étude se révèle passionnante.

3. Pourquoi crypter ses courriers électroniques ?

Si le courrier électronique est un instrument formidable, il faut cependant admettre qu'il est à peu près aussi confidentiel qu'une carte postale que l'on expédie sans prendre la précaution de la glisser dans une enveloppe.
Cela est loin de constituer toujours un problème, car de nombreux courriers électroniques ne revêtent pas un caractère confidentiel ; en effet, quand nous envoyons à un proche un message de prompt rétablissement parce ce que ce dernier est valétudinaire, nous nous moquons bien de savoir que notre mot puisse être intercepté et tomber entre les mains d'une puissance étrangère.
Il existe cependant des courriers qui doivent rester secrets ; les entreprises notamment s'échangent couramment des informations confidentielles, qu'il s'agisse de contrats, d'analyses ou de secrets de fabrique. On est d'ailleurs en mesure d'affirmer que bien peu d'entre elles ont pris la mesure du problème ; dans l'esprit de nombreuses personnes, il semble que la rapidité d'expédition du courrier électronique soit un facteur de sécurité : comme un courriel est acheminé en quelques secondes, beaucoup de gens pensent qu'il est impossible à intercepter. Ce en quoi ils ont tort. Outre le *problème de l'interception*, il faut prendre garde au fait que *l'envoi ou la réception d'un courrier électronique laissent de multiples traces*, notamment sur l'ordinateur qui sert à le réceptionner. *Il faut savoir parfaitement identifier toutes ces faiblesses qui menacent la confidentialité du courrier électronique de manière à pouvoir les surmonter si besoin est.*

3.1. On nous écoute !

Au départ, ce ne furent que quelques papiers dans la presse spécialisée. Puis le nom d'*Echelon* revint de plus en plus souvent dans les conversations. Il y eut enfin le rapport parlementaire d'*Arthur Paecht et l'enquête de l'Union européenne* : il faut donc bien aujourd'hui se rendre à l'évidence, Echelon existe et les États-Unis, au début de la guerre froide, ont bien mis en place un *immense réseau d'écoute* qui s'est perfectionné au fil du temps.

Capable aujourd'hui d'intercepter les communications téléphoniques, les télécopies et les courriers électroniques, Echelon reste l'objet de multiples interrogations dans la mesure où l'on possède très peu de renseignements à son sujet. On est cependant certain qu'une partie de son activité est consacrée à l'*espionnage économique*, les sociétés Airbus et Thomson ayant notamment été privées d'importants contrats internationaux grâce à son utilisation.
Les révélations sur le *logiciel Carnivore du FBI* chargé de surveiller les Américains ne sont pas tellement plus rassurantes. Mais l'Union européenne n'est pas totalement en reste puisqu'elle a décidé, dans le cadre de son *projet de convention sur le cybercrime*, le stockage systématique, pendant 90 jours, des données du trafic de chaque internaute. Quand on vous dit que tout ce que vous écrivez pourra être retenu contre vous, vous commencez maintenant à y croire ?

3.2. Internet et la confidentialité

Il est clair qu'Internet n'a pas été conçu à l'origine pour empêcher l'espionnage des conversations qui s'y déroulent.



Rappel

Il faut ici rappeler que la structure même du réseau a été élaborée par le ministère de la Défense américain pour pouvoir résister à une attaque nucléaire : si une partie du réseau était endommagée, les communications devaient pouvoir continuer à fonctionner sur l'autre partie. De même, le réseau n'était pas conçu pour le grand public.

Le *protocole IP* prend donc en compte, grâce notamment au concept de *routage*, *l'acheminement des paquets par des voies de communication différentes*, mais il n'est *pas prévu à la base pour garantir la confidentialité des informations qui circulent sur le réseau*.

Il est donc très facile d'installer un logiciel (qu'on appelle *sniffer*) qui intercepte les paquets transitant par le réseau.
Bien évidemment, au fur et à mesure de l'ampleur que prenait Internet, les spécialistes de la sécurité ont pris la mesure du problème et de nouveaux protocoles de communication sécurisée ont vu le jour. *Il est donc désormais possible de crypter les paquets IP*, ce qui rend, en cas d'interception, leur *décodage plus complexe*.
Mais il faut cependant reconnaître que le mode de transmission des courriers électroniques n'est pas un modèle de confidentialité : le fait qu'un courriel passe par de multiples bureaux de poste virtuels, où il peut facilement être copié, n'est pas de nature à rassurer ceux qui veulent conserver le secret de leur correspondance électronique. Pour ceux-là, la seule solution demeure le *cryptage*.

3.3. Identifier les menaces

Tous les grands stratèges le savent bien : pour combattre l'ennemi, il faut tout d'abord l'identifier. En ce qui concerne la confidentialité du courrier électronique, nous allons malheureusement voir que les menaces viennent de toutes parts.

Le *premier danger*, c'est bien évidemment l'autre, *celui à qui l'on écrit* ; l'échange que l'on croyait privé peut faire le tour de la planète en quelques minutes si votre correspondant décide de rendre public le contenu de votre message. Sans tomber dans la paranoïa aiguë (qui, en matière de sécurité informatique, doit être une seconde nature), cette éventualité n'est pas à négliger.



Si vous écrivez vos courriels à partir de votre lieu de travail, sachez que votre employeur a la capacité technique d'espionner tout le courrier que vous écrivez et recevez.
Une étude récente montre que 74 % des entreprises américaines surveillent les communications électroniques de leurs employés. On commence à voir apparaître en France quelques affaires de licenciements à la suite de courriers électroniques qui n'ont pas plu à la direction d'une entreprise.
La situation est cependant un peu plus complexe aujourd'hui car une jurisprudence récente a attribué *le caractère de correspondance privée à un courrier électronique personnel envoyé depuis l'ordinateur d'un salarié d'une entreprise*. Mais cette jurisprudence pose plus de problèmes qu'elle n'en résout.



Remarque

Votre fournisseur d'accès à Internet (FAI), s'il gère votre compte de courrier électronique, a aussi fatalement la capacité de lire tous les courriels que vous recevez et envoyez.

Enfin, et il ne s'agit malheureusement pas de science-fiction, vous pouvez être victime d'un hacker qui pirate votre ordinateur ou le serveur de messagerie de votre FAI.

3.4. Confidentialité et fournisseur d'accès



Avant de vous abonner chez un fournisseur d'accès à Internet (FAI), nous vous recommandons de bien lire les *clauses du contrat qui concernent la confidentialité des courriers électroniques que vous écrivez ou que vous recevez.*

En théorie, la *loi protège la vie privée* (*article 9 du code civil*), ainsi que *le secret des correspondances* (*loi n° 91- 646 du 10 juillet 1991*). Toute clause restreignant ces droits fondamentaux serait donc considérée comme nulle ; mais comme il vaut mieux être prudent, si le contrat est flou en la matière, demandez des précisions par écrit avant de signer quoi que ce soit.



Le problème se pose notamment pour les *messageries gratuites*, comme Hotmail. Même s'il n'y a pas de contrepartie financière, l'utilisateur signe tout de même en ligne un contrat qui le lie au prestataire de services. Or, dans la majorité des cas, *ce contrat est très désavantageux pour l'internaute*.

Si l'on prend la peine de lire l'intégralité du contrat de la messagerie Hotmail, on peut y découvrir la clause suivante : *"Microsoft n'est pas tenue de surveiller les Services de communication. Toutefois, Microsoft se réserve le droit de prendre connaissance des documents postés sur un Service de communication et de supprimer tout élément, à sa seule convenance. Microsoft se réserve le droit de vous retirer à tout moment l'accès à l'une ou à l'ensemble de ces Services de communication, sans notification, et pour quelque motif que ce soit. Microsoft se réserve le droit de divulguer toute information pour se conformer à toute loi ou réglementation en vigueur, ou pour obéir à une injonction judiciaire ou administrative, ou d'éditer, de refuser de poster, ou de supprimer tout ou partie de documents ou d'informations, à la seule convenance de Microsoft. "*

Qui a dit que le gratuit était encore trop cher ?

4. Méthodes de cryptage de ses courriers électroniques

La seule solution pour assurer le secret de vos correspondances est de crypter vos messages. Et, pour ce faire, vous devez adopter un système basé sur le principe de la cryptographie à clé publique.

Deux méthodes s'offrent à vous :

- *acquérir un logiciel de cryptographie* qui s'interface avec votre logiciel de messagerie (par exemple, Outlook Express) ;
- *acquérir un certificat numérique (ou identité numérique)* qui vous servira à recevoir des messages cryptés.



Remarque
Dans la seconde méthode, votre clé publique fait partie de votre identité numérique qui est garantie par une autorité de certification.

5. Le cryptage des fichiers

Si vous avez des fichiers confidentiels, vous pouvez les crypter, ce qui interdira leur accès aux personnes non autorisées qui ne possèdent pas le mot de passe. Nous allons étudier quelques-unes des multiples possibilités de cryptage de fichiers qui existent. Signalons que la libéralisation de la cryptographie en France a dynamisé ce marché ; il existe aujourd'hui plusieurs logiciels gratuits qui proposent des fonctionnalités de cryptage fort.



Exemple
Le logiciel Security Box permet de chiffrer vos fichiers en *triple-DES* avec une clé de 128 bits. Bien évidemment, le *logiciel PGP* permet également de crypter des fichiers.



Comment crypter les fichiers Office ?
Les logiciels de la suite Office de Microsoft offrent aussi la possibilité de protéger par un mot de passe les documents pour en interdire la lecture ou la modification. Il est ainsi très facile de protéger ses fichiers Word ou Excel des regards indiscrets. Dans les versions anciennes d'Office, le cryptage des fichiers était vraiment sommaire et on trouvait de nombreux outils sur Internet qui permettaient de craquer les mots de passe des logiciels d'Office.



Utiliser le cryptage de Windows
Si vous utilisez Windows 2000 ou bien Windows XP et avez un disque dur formaté avec le *système de fichiers NTFS*, vous avez la possibilité d'utiliser le *cryptage EFS* (*Encrypting File System*) intégré à Windows.

Partie D. La signature électronique

Préambule

Il y a encore peu de temps, la *signature électronique* n'était qu'un concept que la plupart des gens appréhendaient mal ; or, aujourd'hui, il s'agit d'une réalité qui va révolutionner la vie quotidienne des particuliers et des entreprises.



Attention
Commençons tout d'abord par lever une ambiguïté : de nombreuses personnes (et même certains auteurs) pensent à tort qu'une signature électronique est le fichier de signature qui est rajouté automatiquement à la fin d'un courrier électronique ou bien un fichier graphique créé par la numérisation (à l'aide d'un scanner) d'une signature manuscrite. Or, la signature électronique (ou numérique) est un concept totalement différent.

La signature électronique est un *dispositif cryptographique* qui permet de *s'assurer de l'identité de la personne qui signe le courrier*.
En fait, signer un courrier électroniquement, c'est fournir un code secret qui authentifie l'auteur du message, de la même manière que le code secret de votre carte bancaire permet au distributeur de billets de savoir que c'est bien vous qui retirez de l'argent.
Ce nouveau concept est rendu possible grâce à l'évolution des moyens cryptographiques, ainsi qu'à l'adaptation de la législation.
L'application la plus immédiate de la signature électronique est que l'on peut signer un document numériquement et l'envoyer par courrier électronique, là où il fallait auparavant prendre un stylo, signer au bas de la feuille et envoyer le document papier par la Poste.

1. Modifications législatives

Pour que le concept de signature électronique devienne une réalité, il a fallu modifier plusieurs lois. *Il a tout d'abord été nécessaire d'autoriser la cryptographie*. Se rendant compte que cette absence de libéralisation demeurait le frein principal à l'essor du commerce électronique, le gouvernement de Lionel Jospin décida alors d'autoriser l'usage de la cryptographie avec des clés de 40 bits[La longueur de la clé d'un système cryptographique se mesure en bits, bit étant l'acronyme de binary digit, ou chiffre binaire, c'est-à-dire zéro ou un ; plus la clé est longue, plus le décryptement est long et difficile]. Face aux doléances des professionnels d'Internet qui s'insurgeaient contre ces mesures jugées trop timides, le gouvernement publia le 17 mars 1999, au Journal officiel, *deux décrets (99 199 et 99 200) qui légalisaient l'utilisation de la cryptographie avec des clés de 128 bits*.

Les débuts de la signature électronique ont commencé au mois de mars 2000 lorsque la *loi n° 2000-230*, portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique, a été publiée au Journal officiel. Pour tous les nostalgiques du papier, ce fut un jour noir car cette loi stipule que *"l'écrit sous forme électronique est admis en preuve au même titre que l'écrit sur support papier, sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité "* .
Un peu plus loin, le texte assène : *"l'écrit sur support électronique a la même force probante que l'écrit sur support papier. "*
Il a encore fallu attendre un an pour que le décret d'application de cette loi soit publié (un an pour rédiger quatre pages, quelle productivité !) mais, depuis le 31 mars 2001, c'est chose faite.

Remarque :
Vous pouvez donc désormais envoyer un courrier électronique signé numériquement chaque fois que l'on exige de vous une signature manuscrite.
Mais attention, armez-vous de patience et de persuasion car les réactionnaires de tout poil et les ignorants courent les rues et il faut encore pas mal ferrailler pour qu'une administration accepte un courriel signé numériquement à la place d'un courrier papier. Que cela ne vous empêche pas de persévérer car il arrivera bien un jour où le bon sens informatique triomphera de la bureaucratie.

2. La certification numérique

2.1. Les autorités de certification

Comment fait-on en pratique pour signer numériquement un courrier électronique ?

Pour ce faire, il faut se procurer au préalable un *certificat numérique* que la loi définit comme *"un document sous forme électronique attestant du lien entre les données de vérification de signature électronique et un signataire"* .
On trouve ce genre d'ustensile auprès d'une *autorité de certification* (ou *AC*), ou d'un *prestataire de services de certification électronique*, soit « *" toute personne qui délivre des certificats électroniques ou fournit d'autres services en matière de signature électronique" ()* ».



Remarque
Dans *Outlook Express*, vous pouvez obtenir l'adresse d'autorités de certification grâce au bouton Obtenir un identificateur de la commande *Outils* > *Options* > *Sécurité*. Malheureusement, toutes les autorités de certification proposées par Microsoft sont des autorités étrangères qui offrent leurs services en anglais.



Complément
Cliquez sur le lien ci-dessous afin de visualiser l'animation correspondante.
De quoi avons-nous besoin ?

2.2. Comment obtenir en pratique un certificat numérique

Le certificat numérique est donc le sésame de la signature électronique ; sans lui, impossible de signer un courrier numériquement. Pour l'obtenir, vous devez faire appel à une *autorité de certification* ; nous vous conseillons de choisir une autorité française car, en cas de problème, le dialogue sera plus facile.



Exemple
La société Certinomis propose pour une vingtaine d'euros le certificat baptisé *Personae*. Vous pouvez juger du professionnalisme de l'autorité de certification au vu de la procédure d'obtention du certificat numérique. La procédure doit être écrite et exiger des preuves de votre identité ; n'oubliez pas que cette lourdeur est un gage de sérieux et que, à l'issue de cette épreuve, tous vos échanges pourront être dématérialisés.

Pour obtenir votre certificat numérique, connectez-vous au site web d'une autorité de certification et remplissez un formulaire d'inscription en ligne.



Exemple

Sur le site de *Certinomis*, vous devez fournir des renseignements personnels, puis envoyer, par la Poste :

- une photocopie de votre pièce d'identité ;
- une facture de téléphone ou une quittance de loyer, ;
- un chèque et un contrat régissant les rapports entre l'utilisateur et l'AC.

Après avoir vérifié votre dossier, *l'AC valide votre certificat numérique*, que vous devez *télécharger sur votre ordinateur. Son utilisation est subordonnée à une clé privée* qui vous est envoyée par la Poste.

2.3. Sauvegarder votre certificat numérique

La première des choses à faire, quand vous avez saisi la clé privée qui sert à activer votre certificat numérique, n'est pas d'essayer d'envoyer immédiatement un message signé numériquement, mais d'*effectuer une copie de sauvegarde de votre certificat*.

Cette copie vous servira à restaurer votre système de courrier électronique en cas de panne, ou bien à exporter votre certificat numérique, si vous changez d'ordinateur, par exemple.
Pour copier votre certificat, cliquez sur le bouton *Identificateurs numériques* dans la *commande Outils > Options > Sécurité*. La *boîte de dialogue Certificats* apparaît : cliquez sur *l'onglet Personnel* et sélectionnez le certificat que vous voulez sauvegarder.
Cliquez ensuite sur le *bouton Exporter*. *L'Assistant Exportation de certificat* apparaît :

- Cliquez sur le bouton *Suivant* ;
- Choisissez sur la deuxième page *l'option Oui, exporter la clé privée* ;
- Sur la troisième page, validez les options sélectionnées par défaut en cliquant sur le bouton *Suivant*.



Conseil

Choisissez soigneusement un mot de passe et ne l'oubliez pas !
Ce mot de passe protège votre clé privée d'une utilisation frauduleuse. Si vous êtes dans un environnement protégé, ce mot de passe est superflu.
Ensuite, indiquez un emplacement et un nom de fichier, et validez l'exportation de votre clé en cliquant sur le bouton *Terminer* de la dernière page de l'assistant.



Remarque : Clé publique et clé privée

Vous devez bien faire la *différence entre votre clé privée et votre clé publique*.
La *clé publique*, comme son nom l'indique, n'est pas secrète, et vous devez la distribuer à tous les correspondants qui souhaitent vous envoyer des courriers cryptés.
La *clé privée*, quant à elle, ne doit jamais sortir de votre coffre-fort. Les internautes mélangent encore trop souvent leurs deux clés et diffusent leur clé privée au lieu de leur clé publique, ce qui est particulièrement fâcheux. Dans ce cas-là, on peut, par exemple, lire les courriers cryptés que l'on vous envoie et

usurper votre identité. *La clé privée est vraiment le garant de votre identité numérique et vous devez la protéger*. Pour ce faire, vous pouvez *choisir un mot de passe* ; cela est une précaution indispensable si votre ordinateur est accessible à d'autres personnes.



L'authenticité des certificats numériques

Si votre certificat numérique est bien protégé et au-dessus de tout soupçon, en est-il de même de celui de tous vos correspondants ? Dans tout système sécurisé, il existe un maillon faible, notamment quand l'être humain intervient. Il convient donc de rester vigilant et de ne pas accorder sa confiance systématiquement à tous les certificats numériques.

Dans la mesure où certaines autorités de certification (AC) accordent un certificat numérique sans vérifier sérieusement l'identité du demandeur, on peut mettre en doute certaines identités numériques. De la même manière, la clé privée qui protège le certificat numérique peut être volée ou bien devinée si le mot de passe qui la verrouille est mal choisi. *Si cette mésaventure vous arrive, vous devez avertir immédiatement votre AC qui placera votre certificat sur une liste de révocation*. Chaque fois que vous utilisez un certificat numérique, *Outlook Express* vérifie, auprès de l'AC qui l'a émis, qu'il est valide et ne figure pas sur sa liste de révocation. Vos correspondants seront alors avisés de l'invalidation de votre certificat numérique.

2.4. Animations

Cliquez sur les liens ci-dessous afin de visualiser les animations correspondantes.



Pourquoi un certificat ?

- Pourquoi un certificat ?
- A qui faire confiance ?
- A quoi tout cela ressemble-t-il ?
- Serez-vous assez prudent ?

3. La signature numérique

3.1. Signer numériquement un courriel

Quand vous avez votre certificat numérique en poche, vous pouvez alors signer électroniquement les courriers que vous envoyez.



Attention

Faites cependant bien attention au fait qu'un certificat numérique (ou identité numérique) est associé à une seule adresse électronique. Cela signifie que si vous possédez plusieurs comptes de courrier électronique, vous devez posséder plusieurs certificats numériques. Si vous ne possédez qu'un seul certificat, vous ne pouvez envoyer des courriers signés numériquement qu'à partir du compte auquel est associé votre certificat.

Dans le même ordre d'idées, l'adresse de réponse de votre compte de courrier

électronique (spécifiée dans *Outils > Comptes > Courrier > Propriétés*) doit être identique à l'adresse spécifiée dans votre certificat numérique.

Pour signer numériquement un courriel, vous devez composer un nouveau message, puis choisir la *commande Signer numériquement* à partir du *menu Outils* de la fenêtre de composition du message. Vous pouvez également cliquer sur le *bouton Sign Mes.* de la barre d'outils. Un ruban rouge apparaît alors dans la partie droite de la fenêtre de message.

En cliquant sur le *bouton Envoyer*, vous signez numériquement votre message et envoyez en même temps à votre correspondant une copie de votre identité numérique (votre clé publique).
Vous pouvez configurer *Outlook Express* pour que tous vos messages soient par défaut signés numériquement. Pour ce faire, choisissez la *commande Outils > Options > Sécurité* et cochez la *case Signer numériquement tous les messages sortants*.

3.2. Recevoir un message signé numériquement

Quand vous recevez un message signé numériquement dans *Outlook Express*, un ruban rouge apparaît dans la liste des messages de la boîte de réception, ainsi que dans la fenêtre de message. La première fois que l'on ouvre un message signé numériquement, *Outlook Express* affiche un message d'aide de sécurité qui explique la nature du courrier. Si vous cochez la *case Ne plus afficher cet écran d'aide*, *Outlook Express* n'affichera plus cet avertissement lors de la réception des prochains messages signés numériquement. Pour pouvoir prendre connaissance du courrier, vous devez faire défiler le message d'aide et cliquer sur le *bouton Continuer* ; le message signé numériquement apparaît ensuite.

À moins que vous n'ayez désactivé la *case Ajouter le certificat des expéditeurs au Carnet d'adresses de la commande Outils > Options > Sécurité > Options avancées*, *Outlook Express* ajoute automatiquement le certificat numérique de votre correspondant quand vous recevez un courrier signé numériquement. Ce dernier se voit alors affublé d'un ruban rouge dans le Carnet d'adresses.
Si l'option est désactivée, vous pouvez ajouter manuellement au Carnet d'adresses le certificat numérique en ouvrant le message, puis en choisissant la *commande Fichier > Propriétés*. La *boîte de dialogue Message signé numériquement* apparaît. Cliquez sur le *bouton Afficher les certificats de l'onglet Sécurité*, puis sur *Ajouter au Carnet d'adresses*. Le certificat numérique est ajouté à tous les contacts dont l'adresse électronique correspond.

3.3. Autres fonctions de la signature électronique

La signature électronique est ainsi devenue possible grâce à l'invention de la cryptographie à clé publique. Avec cette technologie, une personne qui envoie un courrier signé numériquement peut être authentifiée de manière fiable, et on est donc vraiment certain qu'elle est bien celle qu'elle prétend être. Dans la mesure où il est très facile de falsifier son identité quand on envoie un courrier électronique, *un courrier signé numériquement authentifie de manière absolue son expéditeur*.

L'usage de la signature électronique permet également trois autres fonctionnalités :

- *L'intégrité*. Si un message signé numériquement a été modifié, que ce soit à la suite d'une erreur de transmission, ou bien intentionnellement par un pirate qui a intercepté le courrier, Outlook Express le détectera et en avertira le destinataire.
- *La non-répudiation*. Quand on a signé un courrier électronique numériquement, on ne peut pas prétendre par la suite que l'on ne l'a pas envoyé. Cette fonctionnalité est importante dans le cadre d'un contrat, et notamment pour le commerce électronique.
- *La confidentialité*. Le certificat numérique sert de clé publique, ce qui signifie que si vous possédez une signature électronique, on est susceptible de vous envoyer des messages cryptés que vous pourrez déchiffrer à l'aide de votre clé privée. La section suivante expose en détail le cryptage des courriers électroniques.



Quelle est la valeur juridique de la signature électronique?

Juridiquement, la signature électronique a la même valeur que la signature manuscrite, dès lors qu'elle permet de garantir :

- *l'identité du signataire* : la signature d'une personne exprimant son consentement, il est essentiel de pouvoir affirmer avec certitude que la signature électronique a bien été apposée par cette personne (et non par une autre) ;
- *l'intégrité du document sur lequel a été apposé la signature* : une personne ne signe un document que parce qu'elle est d'accord avec ce qu'il contient. Il est donc impératif de garantir que le contenu ne pourra pas être modifié après signature ;
- *l'indissociabilité de la signature et du document signé* : il ne doit pas être possible d'extraire la signature électronique apposée par une personne sur un document pour l'intégrer à un autre document.

3.4. Animations

Cliquez sur les liens ci-dessous afin de visualiser les animations correspondantes.



Principes de la signature numérique

- Comment signer un document numérique ?
- Qu'est-ce que le chiffrement asymétrique ?
- Sauriez-vous signer un mel, un contrat sur disquette, un achat par carte bancaire ?
- Quels avantages attendre de la signature numérique ?
- A vous de jouer !

Partie E. Le SPAM et la loi

1. L'adresse électronique...

1.1. ... une donnée à caractère personnel

La loi du 6 janvier 1978 protège les citoyens contre les abus de l'informatisation à outrance et encadre notamment la collecte des informations nominatives et leur utilisation.

Si l'on reprend la définition que fait l'*article 2 du caractère personnel d'une donnée*, il apparaît clairement que *cette définition englobe l'adresse électronique*. Cette dernière est *directement nominative* quand elle se présente *sous la forme prénom.nom* et *indirectement nominative dans le cas contraire* puisqu'*une adresse électronique est toujours reliée à une personne physique*.



Remarque
Cette distinction ne vaut pas pour les messageries gratuites comme Hotmail où aucune vérification du nom et de l'adresse du titulaire de l'abonnement n'est effectuée.



Rappel
Il faut également noter qu'une adresse électronique fournit souvent d'autres renseignements comme l'*origine géographique*, le *nom du FAI* ou le *nom de l'entreprise*.

* *
*

Le fait que l'adresse électronique soit perçue comme une information à caractère personnel a donc des conséquences juridiques puisque sa collecte et son utilisation sont réglementées.

1.2. ... une donnée marchande

Comme envoyer un courrier électronique à une personne ou à cent mille coûte le même prix, c'est-à-dire presque rien, il est bien évident que faire du publipostage électronique devient on ne peut plus tentant pour toutes les entreprises qui ont à vendre quelque chose (que ce soit un bien de consommation, un service ou une religion).

L'adresse électronique d'un individu est alors considérée comme un moyen d'atteindre à vil prix un client potentiel.
De la même manière que certaines sociétés se sont fait une spécialité de vendre ou louer des fichiers d'adresses postales, on voit apparaître des entreprises qui recueillent et revendent des adresses électroniques. Ces nouveaux chercheurs d'or font flèche de tout bois : cartes de visite, annuaires d'entreprises, annuaires de FAI, contributions dans les forums publics de discussion (newsgroups) ; tout est bon pour récupérer des

adresses électroniques. Si, de surcroît, l'adresse est qualifiée, parce que vous avez, par exemple, posté une contribution sur un forum consacré aux sous-vêtements en latex, elle prend tout de suite de la valeur.



Conseil 1

Il convient donc de veiller à ne pas laisser traîner son adresse électronique n'importe où.

La première des précautions est de *ne pas la confier à n'importe qui*. De la même manière, quand vous diffusez un courriel en nombre, rien ne vous oblige à diffuser l'adresse électronique de vos correspondants à tous les destinataires de l'envoi. Après tout, le *champ Cci* a été inventé pour cela, mais il assez étonnant de voir que très peu de personnes l'utilisent et encore moins se rendent compte qu'elles commettent un traitement automatisé de données à caractère personnel quand elles mettent tout leur carnet d'adresses dans le *champ Vers* d'un courriel...

La moindre des courtoisies, si vous ne voulez pas que l'on diffuse à tout va votre adresses électronique, est donc bien de commencer par *ne pas répandre l'adresse électronique de vos correspondants*.



Conseil 2

Il est également prudent de *ne jamais poster de message sur un forum en utilisant sa véritable adresse*. Les marchands d'adresses électroniques scrutent les forums et ont conçu des logiciels qui récupèrent automatiquement toutes les adresses électroniques qui s'y trouvent. Le plus simple, quand cela est possible, est de *déclarer une adresse inexistante* ou bien de *créer une adresse sur un serveur de Webmail gratuit qui ne servira qu'à cet effet*.

Au final, moins vous diffusez votre adresse électronique, moins vous recevrez de spam.

2. Les aspects juridiques du spamming

2.1. L'ampleur du spamming

De la même manière que votre boîte aux lettres est envahie de publicités en tous genres, votre BAL électronique peut regorger de messages que vous n'avez pas vraiment demandé à recevoir. Il s'agit le plus souvent de courriers vous incitant à acheter des produits.

Marginal aux débuts d'Internet, ce phénomène a pris aujourd'hui une ampleur considérable. Dès le mois d'octobre 1999, la CNIL avait établi un rapport, « *Le publipostage électronique et la protection des données personnelles* », qui est disponible à l'adresse suivante : www.cnil.fr/fileadmin/documents/approfondir/rapports/publpost.pdf



Dans l'étude NetValue/Datatrader réalisée en mai 2001, 56 % des hommes et 48 % des femmes interrogés perçoivent un e-mail sur deux comme étant promotionnel ou commercial.

À la fin de l'année 2004, différentes études estimaient que trois courriels sur

quatre étaient du spam. Le phénomène n'arrête pas de progresser et on pourra s'en persuader en lisant toute une série de chiffres disponibles à l'adresse suivante : http://www.journaldunet.com/cc/03_internetmonde/spam.shtml

Les entreprises commencent à prendre cette réalité très au sérieux, car le trafic généré par ces courriers non sollicités crée un engorgement des serveurs de messagerie.

2.2. Le droit applicable en France

La loi du 6 janvier 1978 encadre la collecte des adresses électroniques qui est une condition sine qua non du spam. Conscients du problème grandissant du spam, les hommes politiques ont cependant voulu réagir et la nouvelle loi du 21 juin 2004, baptisée LEN[Loi pour la confiance dans l'économie numérique], vient renforcer l'arsenal législatif.
En effet, l'*article 22 de cette nouvelle loi* modifie le code des postes et télécommunications et précise les éléments suivants.



Extrait de texte légal

Est interdite la prospection directe au moyen d'un automate d'appel, d'un télécopieur ou d'un courrier électronique utilisant, sous quelque forme que ce soit, les coordonnées d'une personne physique qui n'a pas exprimé son consentement préalable à recevoir des prospections directes par ce moyen.
Pour l'application du présent article, on entend par consentement toute manifestation de volonté libre, spécifique et informée par laquelle une personne accepte que des données à caractère personnel la concernant soient utilisées à fin de prospection directe.
Constitue une prospection directe l'envoi de tout message destiné à promouvoir, directement ou indirectement, des biens, des services ou l'image d'une personne vendant des biens ou fournissant des services.
Toutefois, la prospection directe par courrier électronique est autorisée si les coordonnées du destinataire ont été recueillies directement auprès de lui, dans le respect des dispositions de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, à l'occasion d'une vente ou d'une prestation de services, si la prospection directe concerne des produits ou services analogues fournis par la même personne physique ou morale, et si le destinataire se voit offrir, de manière expresse et dénuée d'ambiguïté, la possibilité de s'opposer, sans frais, hormis ceux liés à la transmission du refus, et de manière simple, à l'utilisation de ses coordonnées lorsque celles-ci sont recueillies et chaque fois qu'un courrier électronique de prospection lui est adressé.
Dans tous les cas, il est interdit d'émettre, à des fins de prospection directe, des messages au moyen d'automates d'appel, télécopieurs et courriers électroniques, sans indiquer de coordonnées valables auxquelles le destinataire puisse utilement transmettre une demande tendant à obtenir que ces communications cessent sans frais autres que ceux liés à la transmission de celle-ci. Il est également interdit de dissimuler l'identité de la personne pour le compte de laquelle la communication est émise et de mentionner un objet sans rapport avec la prestation ou le service proposé.

Remarque :
Cet article de loi durcit considérablement les textes en vigueur et supprime en théorie la possibilité du spam puisqu'il faut *obtenir le consentement préalable du destinataire avant de pouvoir lui envoyer un courrier qui sera donc, par définition, considéré comme sollicité*. Les entreprises avaient d'ailleurs six mois pour se mettre en conformité avec la loi et obtenir le consentement de leurs clients.
Certaines ont joué le jeu, mais elles ne sont pas majoritaires. On continue donc malgré tout à recevoir de nombreux courriers non sollicités en provenance d'entreprises françaises qui sont, par conséquent, en infraction manifeste avec la nouvelle loi.

Conseil
Quand cela vous arrive, nous vous conseillons, si cela est possible, de leur rappeler systématiquement la loi à l'aide d'un modèle tout prêt à l'emploi. Si tous les spammés s'unissent pour protester, on peut espérer que cela fera bouger les choses, au moins en France.
Il faut malheureusement avoir l'honnêteté de reconnaître que, pour le spam en provenance de l'étranger, nous n'avons pratiquement aucun moyen d'action.

Remarque
Signalons enfin que les tribunaux commencent à condamner le spam, et parfois très lourdement. Ainsi, au mois de mai 2004, un entrepreneur du sud de la France a été condamné par le tribunal de commerce de Paris à verser 22 000 euros de dommages et intérêts à Microsoft et AOL qui avaient poursuivi le spammeur, ce dernier ayant quand même envoyé plus d'un million de courriers non sollicités.

2.3. L'OPT-IN et l'OPT-OUT

La réglementation du spamming est traditionnellement envisagée à travers deux approches : l'« *opt-in* » et l'« *opt-out* ».

Par ces deux termes anglais, on désigne la *politique de diffusion des informations adoptée par les services Internet* avec lesquels on est en contact.

Exemple
Par exemple, quand vous commandez un produit sur Internet, il n'est pas rare que le cyber-commerçant souhaite vous abonner à une lettre commerciale qu'il diffuse chaque semaine à ses clients. Dans ce cas de figure, il existe deux solutions :

- soit vous êtes *abonné par défaut* à cette lettre,
- soit vous devez *donner votre accord*.

Dans le premier cas, c'est le système du *opt-out* (qui signifie en anglais "*refuser*") car c#est à vous de signifier que vous ne voulez pas recevoir d'informations. Dans lapratique,il faudra en général désélectionner une case à cocher ou bien envoyer un courriel pour se désabonner.

Dans le deuxième cas, c#est le système du *opt-in* (qui signifie en anglais "*accepter*") et c'#est à vous de donner explicitement votre accord pour recevoir des informations.Pratiquement,c'est à vous de cocher une case qui ne l'est pas a priori ou bien vous devez envoyer un courriel pour vous abonner.

On comprendra que le système du opt-out est plus avantageux pour le commerçant alors que le système du opt-in est plus respectueux des libertés du consommateur.



Remarque
Comme nous l'avons vu précédemment, la loi sur la confiance dans l'économie numérique (LCEN) a précisé les choses sur le plan juridique et c'#est clairement le *système du opt-in qui a été adopté en France*, mais vous devez noter que dans d#'autres pays c'#est le système du opt-out qui prime.



Complément
Nous vous invitons à consulter le site suivant, présentant des élément sintéressants sur ce sujet : http://www.journaldunet.com/dossiers/mailing/

3. Conseils pratiques

Malgré les protections juridiques, de nombreux internautes demeurent victimes d'envois abusifs. Des solutions pratiques et techniques existent pour vous prémunir de la réception des courriers électroniques indésirables.
Voici 5 conseils fréquemment dispensés.

3.1. Evitez de répondre aux spams dont le contenu vous semble réellement abusif

Les expéditeurs cherchent à savoir si votre adresse électronique est bien valide. Leur répondre, c'est leur donner l'occasion de vérifier sa validité. Ils pourront alors les revendre à d'autres spammeurs.

3.2. Evitez de mettre votre adresse électronique habituelle sur des sites web ou dans les groupes de discussion

Les adresses électroniques affichées dans les espaces publics d'internet sont susceptibles d'être collectées à votre insu par les logiciels dont se servent les spammeurs pour vous inscrire sur leurs fichiers. Vous pouvez utiliser une adresse auxiliaire ou encore cryptez votre adresse habituelle.



Complément
Pour encrypter vos adresses, voir : http://www.caspam.org/cas_cryptemail.html

3.3. Eviter de délivrer votre adresse mél sans connaître la finalité pour laquelle elle est collectée

Lorsqu'un site vous demande votre adresse de courrier électronique, c'est bien entendu pour communiquer avec vous. Avant de la délivrer, *assurez-vous que le site en question respecte les principes relatifs à la protection des données personnelles*.

Plusieurs indices pourront vous orienter :

- apposition d'un label ;
- appartenance à un organisme professionnel respectueux des données personnelles ;
- références aux lois en vigueur (loi de 1978 en France, directive de 1995...) ;
- indications précises sur l'utilisation qui sera faite de votre adresse de courrier électronique.



Conseil

Observer bien également les éventuelles cases à cocher ou à décocher pour éviter, par exemple, que l'on vous envoie des informations à caractère promotionnel.

3.4. Filtrez les spams

Certains logiciels de courrier électronique et certains webmails[services de courrier électronique disponibles sur le web] vous permettent d'organiser la réception de vos courriels en fonction de mots clés ou de l'adresse de l'expéditeur. Vous pouvez donc prédéfinir vous-même les courriers qui vous paraissent indésirables et faire en sorte qu'ils tombent directement dans votre corbeille.



Conseil

Des logiciels dits « *anti-spam* » peuvent vous faciliter la tâche.

Vous trouverez un liste de logiciels anti-spam à l'adresse suivante : http://www.caspam.org/outils_anti_spam.html

3.5. Dénoncer les courriels abusifs

Il n'est pas toujours possible d'identifier le véritable expéditeur d'un courriel abusif. Un même expéditeur peut d'ailleurs déjouer les techniques de filtrage en changeant systématiquement d'adresse d'envoi.

Vous pouvez dénoncer à la CNIL[En écrivant à l'adresse électronique spam@cnil.fr] les courriels publicitaires qui ne respectent pas les dépositions légales. Vous pouvez également transférer les spams à des organismes tels que Spamcop ou Spamrecycle (en anglais uniquement), qui se chargent de les dénoncer auprès des fournisseurs d'accès.



Remarque

CASPAM vous offre des explications en français sur la procédure à suivre pour recourir aux services de Spamcop.



Conseil

Il est recommandé de signaler les messages abusifs auprès de votre fournisseur d'accès, ce qui lui permettra d'opérer un filtrage généralisé pour l'ensemble de ses abonnés.

Pour cela, il est nécessaire de leur envoyer copie de l'en-tête du courrier abusif. Pour retrouver l'entête sur *Outlook Express*, appuyez en même temps sur les deux touches "*Alt*" + "*Entrée*" puis ciquez sur "*détails*". Sur *Outlook*, cliquez sur "*affichage*" puis "*options*".

4. Organismes de régulation et de lutte contre le spamming

4.1. Organismes professionnels de régulation

Plusieurs organismes professionnels s'intéressent de près à la régulation de l' « *e-mailing* », parmi lesquels :

- Le BVP

  Le Bureau de vérification de la publicité (BVP) a effectué des recommandations déontologiques à l'attention des annonceurs visant le respect de la vie privée des internautes et de l'utilisation des données.

- La FEVAD

  La Fédération des entreprises de vente à distance (FEVAD) a adopté un Code Professionnel et une Charte de qualité respectueux de la protection des données à caractère personnel.

  La FEVAD propose par ailleurs le service e-Robinson, un registre sur lequel vous pouvez inscrire votre adresse de courrier électronique afin « *de recevoir moins de propositions commerciales dans votre boîte aux lettres électronique* » : http://www.e-robinson.com/

- Le SNCD

  Le Syndicat national de la communication directe (SNCD) a élaboré un Code de déontologie relatif à de l'e-mailing.

- L@belsite

  L@belsite a été créé et développé par la FCD (Fédération des Entreprises du Commerce et de la Distribution) et la FEVAD (Fédération des Entreprises de Vente à Distance) qui en assurent l'ingéniérie technique, le financement et la communication. 27 règles applicables sont contenues dans les règles d'habilitation L@belsite.

  Elles s'articulent autour de 3 concepts :

  1. Réalité et identité du commerçant derrière le site ;
  2. Conformité à la réglementation et à la déontologie de la vente à distance adaptée au média internet ;
  3. Transparence et protection des données à caractère personnel.

4.2. Organismes de lutte contre le spamming

Il existe un certain nombre de mouvements en France, en Europe et ailleurs visant à protester contre le spam notamment à travers des campagnes de sensibilisation et la signatures de pétitions. Les organismes suivants figurent parmi les plus connus.

En France

- CNIL (Commission nationale de l'informatique et des libertés)
- CASPAM (Collectif anti spam)
- Campagne française anti-spam sur le serveur Cypango

A noter également, l'existence d'une liste de discussion destinée à combattre le spam par l'échange d'information sur le sujet, Spamcombat .

En Europe

- EuroCAUCE (The European Coalition Against Unsolicited Commercial Email)

Aux Etats-Unis

- CAUCE (The Coalition Against Unsolicited Commercial Email)
- SpamCon Foundation Law Center
- Boycott Internet Spam
- Emailabuse.org
- Junkbusters

Ressources


Cryptographie


Site "Comment ça marche?".


Vie privée


Site "Droit du Net".

Collecte des données personnelles

Site "Droit du Net".

Secret des correspondances

Site "Droit du Net".

Droit à l'image

Site "Droit du Net".

Chapitre

V

La loi sur la création et la protection des oeuvres

Les bases législatives

La législation sur l'information est liée à la *protection d'une oeuvre de création de l'esprit*, elle se rattache alors à la notion de *propriété intellectuelle* (issue d'une traduction de *intellectual property*).

Cependant, les mises en applications de cette propriété intellectuelle diffèrent selon les états. Dans la pays anglo-saxons, les Etats-Unis notamment, les législation est celle du *copyright*. En France, et dans la plus grande partie de l'Europe, c'est le *droit d'auteur* qui régit les droits liés aux TICs, quelles que soient le type d'oeuvre.
Les différences entre ces différents concepts peuvent être subtiles mais existent. Et les évolutions de la législation rendues obligatoires par les évolutions des TICs, ainsi que les enjeux économiques qu'elles représentent, peuvent être déterminantes.

Partie A. La propriété intellectuelle

1. Principes

S'il y a un domaine qui souffre le plus du succès d'Internet, c'est bien celui la propriété intellectuelle, et notamment la propriété littéraire et artistique. Nous n'allons pas faire ici un plaidoyer pro domo en faveur du respect du droit d'auteur, mais tenter de rappeler quelques règles juridiques simples à comprendre et montrer, grâce à quelques exemples de jurisprudence, que continuer à bafouer la législation peut s'avérer risqué.



La propriété intellectuelle

Le code la propriété intellectuelle est celui qui encadre le droit d'auteur dans la législation française, il se décompose en deux parties distinctes :

- la *propriété littéraire et artistique* (droit d'auteur, ...) ;
- la *propriété industrielle* (brevet, ...).



Remarque

Quand on parle ici d'auteur et de droit d'auteur, il faut prendre ce terme au sens large et lui attribuer plutôt la notion de *créateur*.
Au sens de la propriété intellectuelle, un auteur est celui qui crée des oeuvres de l'esprit.

2. Que sont les "oeuvres de l'esprit" ?

Plutôt que de donner une définition des oeuvres de l'esprit, le code de la propriété intellectuelle préfère en donner une liste :



Exemple

- les livres, brochures et autres écrits littéraires, artistiques et scientifiques ;
- les conférences, allocutions, sermons, plaidoiries et autres oeuvres de même nature ;
- les oeuvres dramatiques ou dramatico-musicales ;
- les oeuvres chorégraphiques, les numéros et tours de cirque, les pantomimes, dont la mise en oeuvre est fixée par écrit ou autrement ;
- les compositions musicales avec ou sans paroles ;
- les oeuvres cinématographiques et autres oeuvres consistant dans des séquences animées d'images, sonorisées ou non, dénommées ensemble oeuvres audiovisuelles ;
- les oeuvres de dessin, de peinture, d'architecture, de sculpture, de gravure, de lithographie ;
- les oeuvres graphiques et typographiques ;
- les oeuvres photographiques et celles réalisées à l'aide de techniques analogues à la photographie ;
- les oeuvres des arts appliqués ;
- les illustrations, les cartes géographiques ;
- les plans, croquis et ouvrages plastiques relatifs à la géographie, à la topographie, à l'architecture et aux sciences ;
- les logiciels, y compris le matériel de conception préparatoire ;

- les créations des industries saisonnières de l'habillement et de la parure.

Ce catalogue est assez hétéroclite et l'on y trouve aussi bien des oeuvres de l'esprit communément admises en tant que telles, mais également des choses plus surprenantes comme les logiciels.



Remarque
Dès qu'un auteur crée une oeuvre, celle-ci est protégée par le droit de la propriété intellectuelle, qu'elle ait été publiée ou non.

Partie B. Le droit d'auteur

1. Principes

En matière de droit d'auteur, on distingue traditionnellement deux types de droits : le *droit moral* et le *droit patrimonial*.



Le droit moral
Le droit moral permet notamment à l'auteur d'une oeuvre d'en *revendiquer la paternité* et aussi d'en faire *respecter l'intégrité*.



Exemple
Par exemple, le réalisateur d'un film en noir et blanc pourra s'opposer au distributeur du film qui souhaite en projeter une version colorisée.



Le droit patrimonial
Les droits patrimoniaux sont les droits qui permettent à un auteur de *retirer un bénéfice de son oeuvre*. Ils portent donc principalement sur *l'exploitation et la diffusion des oeuvres*. Les droits patrimoniaux protègent les *intérêts de l'auteur et du diffuseur de ses oeuvres*.
Si l'on prend la peine de lire les articles L122-1 à L122-12 qui définissent les droits patrimoniaux de l'auteur dans le Code de la propriété intellectuelle, on s'aperçoit que l'exploitation d'une oeuvre est extrêmement encadrée. En fait, *toute utilisation d'une oeuvre qui n'est pas prévue par l'auteur doit faire l'objet d'un accord direct avec l'auteur ou bien avec la personne qui est chargée par l'auteur d'exploiter ses oeuvres*.



Exemple
Prenons un exemple concret : si vous souhaitez afficher sur votre page personnelle un poème d'un auteur que vous appréciez particulièrement, vous devez *demander l'autorisation de le faire à l'auteur* de ce poème ou bien à son éditeur à qui l'auteur a accordé les droits de diffusion de cette oeuvre.
Cette démarche peut sembler contraignante, mais c'est la seule qui soit juridiquement valable.



Attention

Bien évidemment, *ce raisonnement vaut pour tous les types d'oeuvres, qu'il s'agit d'un texte, d'une image, d'une chanson, d'un logiciel ou bien encore d'un film. En cas de non respect de ces dispositions légales, vous risquez de vous faire condamner*. Ainsi, la mise à disposition sur un site Web de paroles de chansons, sans le consentement de l'auteur ou de son éditeur, a été plusieurs fois condamnée par les tribunaux.

- http://www.juriscom.net/jpc/visu.php?ID=155
- http://www.juriscom.net/jpc/visu.php?ID=250

Ce principe peut paraître réducteur et accorder trop d'importance au pouvoir de l'auteur sur son oeuvre, mais c'est la loi. Vous imaginerez bien que si le fait de recopier des paroles constitue une infraction, il en va de même pour la musique elle-même...



Remarque

Il existe cependant des exceptions prévues par la loi qui limitent le droit d'auteur (article L122-5), notamment le *droit à la copie privée* et le *droit de citation*.

En matière de citation, la loi stipule que *les citations doivent être courtes et le nom de l'auteur et la source doivent être indiqués clairement*.

A la fin de l'année 2005, une loi importante sur le droit d'auteur et les droits voisins dans la société de l'information (DADVSI) doit être votée. On peut légitimement s'attendre à un *durcissement des textes déjà en vigueur afin de lutter plus efficacement contre le piratage des oeuvres sur les réseaux d'échange P2P*.

- http://www.culture.gouv.fr/culture/cspla/conseil.htm

2. Droit d'auteur, copie privée et P2P

Il existe un principe fort simple en matière de droit d'auteur : *on n'a pas le droit d'utiliser une oeuvre sans l'autorisation de l'auteur en dehors des cas prévus par l'auteur*. Il faut bien comprendre que *l'auteur est propriétaire de son oeuvre* et qu'il en fait ce qu'il en veut.



Exemple

Quand un chanteur écrit des chansons et fait un disque, il accorde aux acheteurs de son disque uniquement le droit d'écouter la musique qu'il a créée dans le cadre qu'il a prévu, c'est-à-dire en écoutant son disque. Le simple fait d'acheter un disque n'accorde aucun autre droit. La matérialité du disque est notre propriété, mais cela ne confère absolument aucun droit sur l'oeuvre, si ce n'est le droit de l'écouter sur l'appareil de son choix.

Pour l'instant, la seule tolérance qu'accorde la loi, c'est de faire une *copie privée des oeuvres que l'on a acquises*. Beaucoup d'internautes ignorants ou de mauvaise foi

justifient le piratage de la musique au nom de l'*exception de copie privée*. Les choses sont pourtant extrêmement claires : *on a le droit de faire une copie d'un disque que l'on a acheté, uniquement pour son usage personnel*. Cela signifie que, lorsque vous achetez un disque, vous pouvez sans problème graver un CD-Rom pour l'écouter dans votre voiture ou votre maison de campagne. En revanche, cela ne vous autorise pas à en faire une copie pour votre voisin, votre cousin ou votre collègue de bureau.

Nous savons tous que peu de gens respectent cette loi à la lettre et il nous est tous arrivé de faire des copies qui dépassaient le cadre de la copie privée. Le problème actuel qui a fait réagir les professionnels de l'industrie du disque est que la généralisation d'Internet couplée à la montée en puissance des débits et à l'émergence des *logiciels de peer to peer* (*P2P*) qui autorisent le partage de fichiers entre milliers d'internautes a mis en place un système de copie pirate généralisé et à échelle industrielle.
En effet, dans le cadre d'un *système d'échange P2P*, l'équation est assez simple : la médiathèque accessible à tous est formée de l'ensemble des contributions de chacun. Si 100 internautes mettent chacun à la disposition de chaque membre du réseau un millier de chansons différentes, cela signifie que chaque internaute possède une bibliothèque virtuelle constituée de 100 000 chansons. Sur le papier, ce système paraît génial tellement il offre des possibilités vertigineuses, mais il a *deux inconvénients majeurs* :

- premièrement, *il contrevient aux dispositions du code de la propriété intellectuelle* ;
- deuxièmement, *les industriels du disque sont persuadés qu'ils vendent moins de CD à cause du P2P*.



Remarque
Bien évidemment, le raisonnement que nous venons de tenir pour la musique vaut également pour les *logiciels* et les *films*.



Face à l'importance prise par le phénomène du P2P, il était somme toute assez logique que les industries phonographiques réagissent, ce qu'elles ont fini par faire.

Elles ont d'abord commencé par rappeler le volet pénal du code de la propriété intellectuelle dont nous reproduisons ci-dessous quelques articles :

- *Article L335-2*
  - Toute édition d'écrits, de composition musicale, de dessin, de peinture ou de toute autre production, imprimée ou gravée en entier ou en partie, au mépris des lois et règlements relatifs à la propriété des auteurs, est une contrefaçon et toute contrefaçon est un délit.
  - La contrefaçon en France d'ouvrages publiés en France ou à l'étranger est punie de trois ans d'emprisonnement et de 300 000 euros d'amende.
  - Seront punis des mêmes peines le débit, l'exportation et l'importation des ouvrages contrefaits.
  - Lorsque les délits prévus par le présent article ont été commis en bande organisée, les peines sont portées à cinq ans d'emprisonnement et à 500 000 euros d'amende.

♦ *Article L335-3*

- Est également un délit de contrefaçon toute reproduction, représentation ou diffusion, par quelque moyen que ce soit, d'une oeuvre de l'esprit en violation des droits de l'auteur, tels qu'ils sont définis et réglementés par la loi.
- Est également un délit de contrefaçon la violation de l'un des droits de l'auteur d'un logiciel définis à l'article L. 122-6.

♦ *Article L335-4*

- Est punie de trois ans d'emprisonnement et de 300 000 euros d'amende toute fixation, reproduction, communication ou mise à disposition du public, à titre onéreux ou gratuit, ou toute télédiffusion d'une prestation, d'un phonogramme, d'un vidéogramme ou d'un programme, réalisée sans l'autorisation, lorsqu'elle est exigée, de l'artiste-interprète, du producteur de phonogrammes ou de vidéogrammes ou de l'entreprise de communication audiovisuelle.
- Est punie des mêmes peines toute importation ou exportation de phonogrammes ou de vidéogrammes réalisée sans l'autorisation du producteur ou de l'artiste-interprète, lorsqu'elle est exigée.

Dans la mesure où les campagnes de sensibilisation n'ont pas vraiment bien marché, les éditeurs sont passés à la vitesse supérieure et ont décidé de porter plainte. Au début du mois de février 2005 a eu lieu la première condamnation d'un internaute ayant téléchargé massivement de la musique grâce à un logiciel de P2P. Cliquez sur le lien ci-dessous afin d'accéder aux extraits de la décision du tribunal de Pontoise.

➤ Voir annexe C en fin de fascicule



Complément

Pour en savoir plus, nou svous invitons à consulter le site suivant : http://www.juriscom.net/int/visu.php?ID=173

Ressources



Tout sur les droits et les obligations des créateurs de sites, de la page personnelle au portail.



Site "Droit du Net".



La propriété intellectuelle



Site "Droit du Net".

Chapitre

VI

Les chartes d'utilisation et de bon comportement

Internet, un autre monde ?

Internet, tout comme tout nouveau médium de communication, nous offre un nouveau moyen d'échanger des informations. Il ne faut cependant pas perdre de vue que la majeur partie des outils de communication sur Internet restent des *outils de communication de personne à personne* (courrier électronique, chat, IRC, forums, ...).

Il est très dommageable de voir la *dépersonnalisation* l'emporter dans les échanges entre personnes sur Internet, cela est en partie dûe à la *distance entre les individus* que crée ce médium. Il n'est pas rare de voir des comportements qui seraient considérés comme inadmissibles s'ils étaient tenus « en personne ».
Si Internet est un nouveau médium de communication, *les interlocuteurs restent des personnes humaines* ! Pour ce faire, les *chartes d'utilisation et de comportement* ont pour objectif de *fixer les règles liées à l'usage des TICs* qu'aucun autre texte national ne peut définir et qu'il incombe à chaque établissement ou école de préciser compte tenu de la grande variété d'utilisation des ressources liées aux TICs.
Compléments indispensables de la réglementation, les chartes ont l'avantage de *s'adresser directement aux usagers* et d'*encadrer une liberté d'usage du réseau*, au plus près des pratiques.

Partie A. Les chartes

1. Définition et principes



Le terme charte est un très vieux mot français (XIème siècle) qui au Moyen-âge désignait un document juridique (titre de propriété, de vente, etc.).
Dans sons sens moderne, une charte est un texte qui fixe le *règlement d'une organisation* (par exemple, la charte des Nations unies). Une charte n'est donc pas à proprement parler un texte de loi, mais un *guide du bon usage*, un *règlement intérieur*, un *recueil des bonnes pratiques*, bref un *mode d'emploi* qui indique ce qu'il faut faire et ne pas faire quand on appartient à une communauté d'utilisateurs.

On trouve des chartes qui réglementent la vie de multiples organisations, qu'il s'agisse d'un syndicat, d'une association sportive ou bien encore d'un établissement scolaire. Internet regroupant de multiples communautés d'utilisateurs, il est par conséquent normal que l'on y rencontre aussi des chartes d'utilisation.

En matière d'Internet, les chartes constituent plus un *accord moral entre deux parties* (l'organisation et ses membres, par exemple, une université avec ses étudiants) qu'une loi ; néanmoins, le rôle des chartes est de *rappeler l'existence de la loi* et d'éventuellement *l'expliquer et la commenter*.
Le but d'une charte est également de *responsabiliser les usagers d'Internet en attirant leur attention sur tous les dangers qu'il y a à utiliser un service en ligne de manière incorrecte*.

2. Les établissements universitaires et les chartes

Aujourd'hui, *la plupart des universités font signer une charte d'utilisation à toutes les personnes* (étudiants, personnel administratif et enseignant) à qui elles offrent un accès à leur réseau informatique.



Application
Si une telle charte existe dans votre université, nous vous encourageons à la rechercher afin de la lire attentivement et de la respecter.



Remarque
De toutes les manières, même si votre université ne possède pas de charte, il faut savoir que l'ensemble des universités françaises utilise les services de communication d'un réseau baptisé *RENATER* (*Réseau National de télécommunications pour la Technologie l'Enseignement et la Recherche*), établissement qui s'est doté d'une charte déontologique. Par conséquent, si vous utilisez le réseau informatique de votre université pour accéder à Internet, vous êtes donc soumis à la *charte Renater*.



Téléchargement et lecture de la charte RENATER
Cette charte est disponible en téléchargement sur le site Web de Renater et nous vous conseillons de la lire.

Partie B. La charte RENATER

1. Présentation et principes



La charte Renater a pour but de fixer les règles d'usage qui s'imposent à tous les utilisateurs du Réseau Renater. En exposant clairement les *risques inhérents à l'utilisation d'un réseau informatique*, cette charte a pour objectif de sensibiliser et de responsabiliser chaque utilisateur du réseau.

La charte rappelle les grandes orientations de l'utilisation du réseau Internet dans les universités :

- Utilisation à des fins d'enseignement, de recherche, de développements techniques, de transfert de technologies, de diffusion d'informations scientifiques, techniques et culturelles .
- Utilisation rationnelle des ressources du réseau ;
- Utilisation loyale des ressources du réseau ;
- Mise à la disposition sur le réseau de données licites ;
- Pas d'accès au réseau Renater à des tiers non autorisés à titre commercial ou non, rémunéré ou non.



Attention
Renater procède régulièrement à des contrôles de la bonne utilisation de son réseau et en cas de violation des règles de la charte, *l'accès au réseau peut être suspendu*.

2. Liste des infractions

Dans son annexe 4, la charte Renater rappelle la liste de toutes les infractions qui peuvent être commises lors de la mauvaise utilisation d'un réseau informatique.
1. Infractions prévues par le Nouveau Code pénal

1. Crimes et délits contre les personnes
   - Atteintes à la personnalité (Respect de la vie privée art. 9 du code civil) :
     - Atteintes à la vie privée (*art. 226-1 al. 2 ; 226-2 al. 2, art.432-9 modifié par la loi nº2004-669 du 9 juillet 2004*) ;
     - Atteintes à la représentation de la personne (*art. 226-8*)
     - Dénonciation calomnieuse (*art. 226-10*)
     - Atteinte au secret professionnel (*art. 226-13*)
     - Atteintes aux droits de la personne résultant des fichiers ou des traitements

informatiques (*art. 226-16 à 226-24, issus de la loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*)

- - Atteintes aux mineurs : *art. 227-23 ; 227-24 et 227-28 et Loi 2004-575 du 21 juin 2004 (LCEN)*.

2. Crimes et délits contre les biens
   - Escroquerie (*art. 313-1 et suite*) ;
   - Atteintes aux systèmes de traitement automatisé de données (*art. 323- 1 à 323-7 modifiés par la loi nº 2004-575 du 21 juin 2004*).
3. Cryptologie
   - *Art. 132-79*(inséré par *loi nº 2004-575 du 21 juin 2004 art. 37*).

2. Infractions de presse (*loi 29 juillet 1881, modifiée*)

- Provocation aux crimes et délits (*art.23 et 24*) ;
- Apologie des crimes contre l'humanité (*art. 24*) ;
- Apologie et provocation au terrorisme (*art. 24*) ;
- Provocation à la haine raciale (*art. 24*) ;
- « *Négationnisme* »: contestation des crimes contre l'humanité (*art.24 bis*) ;
- Diffamation (*art. 30.31 et 32*) ;
- Injure (*art. 33*).

3. Infraction au Code de la propriété intellectuelle

- Contrefaçon d'une oeuvre de l'esprit (y compris d'un logiciel) (*art. 335-2 modifié par la loi nº 2004-204 du 9 mars 2004, art. 34 - et art. 335-3*) ;
- Contrefaçon d'un dessin ou d'un modèle (*art. L521-4 modifiée par la loi nº 2004-204 du 9 mars 2004, art. 34*) ;
- Contrefaçon de marque (*art. L716-9 - modifié par la loi nº 2004-204 du 9 mars 2004, art.34 -et suivants*).

4. Participation à la tenue d'une maison de jeux de hasard (« *cyber-casino* »)

- *Art.1 de la loi du 12 juillet 1983*, modifié par la *loi du 16 décembre 1992*.

Partie C. La netiquette

1. Présentation et principes



« *Netiquette* » signifie plus simplement l'*Etiquette des Réseaux*.

Il s'agit d'une *charte de bon comportement établie en 1996 par l'ETF* (*Internet Engineering TaskForce*). Elle est proposée comme base pour toutes les chartes futures que celles-ci vous engagent vis-à-vis d'un fournisseur d'accès privé.

La netiquette rappelle les *règles de comportement et de courtoisie élémentaires* à avoir dans le cadre de communications :

- *entre 2 individus* : courrier électronique, chat,...
- *entre plusieurs individus* : IRC, forums, chat, courrier électronique,...



Remarque
Pour plus d'informations, nous vous invitons à consulter la définition fournie par Wikipédia en cliquant sur ce lien.

2. Respecter la loi

Si la nétiquette décrit le bon usage et le savoir-vivre sur Internet, il ne faut pas non plus oublier qu'il existe des lois qui encadrent la *liberté d'expression sur Internet*.

La Toile étant considéré comme un outil de communication au même titre que les grands médias d'information, c'est principalement la *loi sur la presse* qui s'appliquera (loi du 29 juillet1881).
Même si cela peut paraître superflu, nous préférons rappeler quelques évidences que la loi interdit :

- Contenus faisant l'apologie des crimes contre l'humanité ;
- Informations incitant à la haine raciale ou à la discrimination ;
- Photo ou film pornographiques représentant un mineur.



Attention
De la même manière la *diffamation* (porter atteinte à l'honneur d'une personne) et l'*injure publique* sont prohibées sur Internet.



Attention
Si vous tenez un blog sur Internet et donnez la possibilité à vos lecteurs de déposer des commentaires, vous devenez en quelque sorte directeur de cette publication et vous êtes donc *tenu pour responsable des propos qui s'affichent sur votre blog*.
Si certains commentaires vous paraissent contraires à la loi, vous avez tout intérêt à les supprimer sans délai.

3. Extraits de la netiquette

La RFC, portant le numéro 1855, fournit un guide d'usage de la *netiquette*. Comme son nom le laisse supposer, la nétiquette est l'étiquette du Net, c'est-à-dire les règles du bon usage en vigueur sur les réseaux électroniques. Tout utilisateur d'Internet devrait avoir lu ce texte avant de se lancer dans l'exploration des multiples facettes de ce réseau. En voici quelques extraits, mais nous vous conseillons d'aller directement consulter vous-même l'original de ce texte ou l'une de ses nombreuses traductions en français qui sont publiées sur Internet.

Quelques extraits de la RFC 1855

3.1. Extrait 1

À moins d'avoir votre propre accès à Internet grâce à un fournisseur d'accès, veillez à demander à votre employeur, qui est propriétaire du courrier électronique, les règles concernant la propriété du courrier électronique diffèrent d'un endroit à l'autre. À moins d'utiliser un outil de cryptage (matériel ou logiciel), vous supposerez que le courrier électronique n'est pas sûr. Ne mettez jamais dans un message électronique quelque chose que vous ne mettriez pas sur une carte postale.

3.2. Extrait 2

Respectez les droits d'auteur de ce que vous reproduisez. Presque tous les pays ont des lois sur les droits d'auteur. Pensez aux Cc lorsque vous répondez. Ne continuez pas à inclure des gens si les messages deviennent une conversation bilatérale.

3.3. Extrait 3

Souvenez-vous que les gens avec lesquels vous communiquez sont situés partout dans le monde. Si vous envoyez un message auquel vous désirez une réponse immédiate, il se peut que la personne qui le reçoit soit chez elle, en train de dormir. Laissez-lui une chance de se réveiller, d'aller au travail et de se connecter, avant de supposer que le courrier n'est pas arrivé ou qu'il a été négligé.

3.4. Extrait 4

Vérifiez toutes les adresses avant de commencer des discours longs ou personnels. Il est de bonne pratique aussi de mettre le mot « Long » dans la ligne d'entête Objet, pour permettre au destinataire de savoir que le message va demander un temps certain de lecture et de réponse. À partir d'une centaine de lignes, un message est considéré comme long.

3.5. Extrait 5

Souvenez-vous que le destinataire est un humain dont la culture, la langue et l'humour ont d'autres références que les vôtres. Rappelez-vous que les formats de date, les unités de mesure et les idiomes peuvent mal s'exporter. Soyez particulièrement prudent avec les sarcasmes.

3.6. Extrait 6

Sachez utiliser les minuscules et les majuscules. LES MAJUSCULES DONNENT L'IMPRESSION QUE VOUS CRIEZ.

3.7. Extrait 7

Soyez concis, sans être excessivement bref. Lorsque vous répondez à un message, citez suffisamment du texte original pour être compris, mais pas plus. Il est de très mauvais goût de répondre simplement à un message en reprenant tout le message reçu : supprimez tout ce qui est hors propos.

Si vous estimez que l'importance d'un message le justifie, répondez brièvement immédiatement pour signaler à l'expéditeur que vous l'avez reçu, même si vous allez répondre plus longuement ultérieurement.

Partie D. Illustrations et exemples de chartes

1. Chartes d'établissement

Aujourd'hui, *la plupart des universités font signer une charte d'utilisation à toutes les personnes* (étudiants, personnel administratif et enseignant) à qui elles offrent un accès à leur réseau informatique.



Application
Si une telle charte existe dans votre université, nous vous encourageons à la rechercher afin de la lire attentivement et de la respecter.



Complément
Si votre établissement n'en dispose pas, n'hésitez pas à rechercher la charte RENATER et à la consulter. http://www.cru.fr/droit-deonto/deontologie/chartes/index.html
N'hésitez pas à consulter le lien suivant qui offre une liste de chartes de différentes universités : http://www.cru.fr/droit-deonto/deontologie/chartes/index.html

2. Règles de conduite dans un forum de discussion

Charte de comportement

Avant de poster un message sur un newsgroup, il est préférable de lire la charte du forum. La charte du forum est un document qui fixe les règles du bon usage sur le forum ; c'est un peu la nétiquette du forum dont souvent elle reprend des éléments. Si le forum ne possède de charte, il existe en général une FAQ (Foire Aux Questions) qui répond aux principales questions que se posent les utilisateurs qui fréquentent le forum pour la première fois. En l'absence d'un tel document, vous pouvez adopter les principes suivants sur un forum de discussion :

- Exprimez-vous dans un langage correct et clair ;
- Avant de poser une question, cherchez sur le forum si la réponse ne s'y trouve pas déjà ;
- Ne prenez pas part aux polémiques et ne répondez pas aux provocations ;
- Quand vous rédigez un message, ne mentionnez pas votre adresse électronique car vous pourriez après être victime de spam.

Forum modéré

Certains forums de discussion sont modérés ; cela signifie qu'il existe des modérateurs qui surveillent le contenu des messages. En pratique, tous les messages sont lus par une ou plusieurs personnes qui contrôlent si les messages sont bien conformes aux règles du forum. Les messages qui ne respectent pas la ligne éditoriale du forum sont censurés et ne sont donc pas publiés. Les messages censurés sont ceux qui sont hors sujet, publicitaires, incorrects ou bien diffamatoires.

Sur les forums qui ne sont pas modérés, il n'y a donc aucun contrôle a priori des messages qui sont postés.

Attention

Ce n'est pas parce qu'il n'y a pas de censure sur un forum non modéré que vous êtes autorisé à écrire n'importe quoi. N'oubliez pas que les forums de discussion sont des forums publics ; la loi les considère comme des organes de presse et c'est par conséquent la loi sur la presse qui s'y applique. Cela signifie que les propos discriminatoires, diffamatoires ou menaçants constituent un délit pénal qui est sévèrement réprimé.

Pour aller plus loin...

Site présentant une sélection de chartes, codes, labels, clauses contractuelles et autres usages relatifs à l'internet élaborés par des organismes privés ou publics. L'ensemble des textes et des usages non formalisés répertoriés ici illustre une même dynamique : la régulation des différents secteurs de l'internet par les acteurs des réseaux.
Cliquez ici pour accéder à ce site.

- Chartes, codes et labels.
- Clauses et contrats.
- Autres usages.

Conclusion

Les chartes d'utilisation organisent les *règles de savoir-vivre* sur le réseau Internet et éventuellement dans les salles d'accès libre informatique ; il est *important de les lire*, de *les comprendre* et de *les respecter*.



Remarque

Dans certaines universités, vous ne pourrez pas utiliser les services du réseau informatique tant que vous n'aurez pas signé une charte d'utilisation.



Remarque

Il peut coexister plusieurs chartes différentes (Renater, charte de votre université, etc.), mais toutes ces chartes ont le même objectif : *favoriser la vie dans les communautés électroniques et optimiser l'usage du réseau tout en respectant les lois*. La nétiquette est également une charte du bon usage du réseau Internet.

Bibliographie

Annexes

- **AnnexeA. Cliquez ici pour avoir le texte de loi intégralement**
- **AnnexeB. Cliquez ici pour avoir le texte de loi intégralement**
- **AnnexeC. Cliquez ici pour avoir les extraits de la décision du tribunal de Pontoise**

ANNEXE A

Cliquez ici pour avoir le texte de loi intégralement



Loi du 6 janvier 1978

La loi du 6 janvier 1978 tâche de répondre à ces questions et ses principes sont résumés dans le premier article :

« 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. »

Pour garantir le respect des règles qu'elle édicte, la loi crée une institution de contrôle : la Commission Nationale de l'Informatique et des Libertés. Pour assurer la transparence des fichiers informatisés, la loi instaure un système de formalités préalables à la mise en oeuvre des traitements automatisés.

Note

La loi du 6 janvier 1978 fut une des premières lois au monde à encadrer l'usage des fichiers informatiques. En 1995, l'Union européenne accoucha d'une directive (n° 95/46 CE du 24 octobre) sur la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation des données. La France avait trois ans pour transcrire cette directive européenne et dans la mesure où nos gouvernements successifs ont quelque peu tardé dans la transposition, la directive européenne est entrée automatiquement en vigueur le 25 octobre 1998. En effet, peu de gens le savent, mais il faut ici rappeler que tout individu qui subit des dommages suite au manquement d'un État membre de transposer une directive, est autorisé à obtenir des réparations devant les tribunaux nationaux, aux termes d'une jurisprudence de la Cour de Justice (affaire Francovich).

La France s'est enfin décidée à transposer la directive européenne, presque dix ans après sa publication, avec la loi du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel. Pour autant, on a gardé la référence originale à la loi du 6 janvier 1978.

La loi de 1978 comportait 48 articles et la loi de 2004 en compte 72. Pour résumer, on peut dire que la nouvelle a renforcé les pouvoirs de la CNIL, élargi son champ d'application, augmenté les droits des personnes tout en simplifiant les procédures administratives. Vous trouverez une analyse détaillée des différences entre les deux lois sur le site de la CNIL à l'adresse suivante :

http://www.cnil.fr/index.php?id=1744

Vous trouverez une version du texte consolidé (c'est-à-dire prenant en compte toutes les modifications législatives) de la loi du 6 janvier 1978 à l'adresse suivante :

http://www.cnil.fr/index.php?id=301

La loi réglemente la collecte l'enregistrement et la conservation des informations nominatives; elle reconnaît des droits aux individus et met des obligations à la charge des détenteurs de fichiers informatiques ou manuels.

Attention
Beaucoup de gens pensent que la loi ne concerne que les fichiers automatisés, c'est-à-dire

informatiques. En fait, la loi s'applique à tous les fichiers nominatifs, même ceux qui figurent sur de bonnes vieilles fiches bristol.

Le grand mérite de la loi (dans son article 2) est de définir précisément ce qu'est une donnée personnelle ainsi que les traitements qui s'y appliquent.

« Constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne.

Constitue un traitement de données à caractère personnel toute opération ou tout ensemble d'opérations portant sur de telles données, quel que soit le procédé utilisé, et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction. »

Note

Que les possesseurs d'agenda électronique se rassurent : le champ d'application de la loi écarte les traitements mis en oeuvre pour l'exercice d'activités exclusivement personnelles, ce qui signifie que les contacts de votre carnet d'adresses ne sont pas pris en compte par cette loi.

Bien que l'on parle en général de données nominatives, il convient de bien comprendre que toute information qui permet d'identifier une personne est une donnée nominative. Cela signifie qu'une adresse électronique, l'adresse IP que vous attribue votre fournisseur d'accès à Internet ou bien encore votre numéro de téléphone sont des données à caractère personnel dont l'utilisation est encadrée par la loi.

L'article 6 de la loi définit la manière dont les données à caractère personnel peuvent être traitées ; il définit notamment les points suivants :

- Les données sont collectées et traitées de manière loyale et licite ;

- Elles sont collectées pour des finalités déterminées, explicites et légitimes et ne sont pas traitées ultérieurement de manière incompatible avec ces finalités ;

- Elles sont adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et de leurs traitements ultérieurs ;

- Elles sont exactes, complètes et, si nécessaire, mises à jour ; les mesures appropriées doivent être prises pour que les données inexactes ou incomplètes au regard des finalités pour lesquelles elles sont collectées ou traitées soient effacées ou rectifiées ;

- Elles sont conservées sous une forme permettant l'identification des personnes concernées pendant une durée qui n'excède pas la durée nécessaire aux finalités pour lesquelles elles sont collectées et traitées.

L'article 7 de la loi précise qu'un traitement de données à caractère personnel doit avoir reçu le consentement de la personne concernée. Il existe bien évidemment des cas où l'on ne vous demande pas votre avis, mais ces exceptions sont bien définies et encadrées par la loi (obligation légale, exécution d'une mission de service public, intérêt légitime poursuivi par le responsable du traitement, etc.)

L'article 8 précise qu'il est interdit de collecter ou de traiter des données à caractère personnel qui font apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes,

ou qui sont relatives à la santé ou à la vie sexuelle de celles-ci. Bien évidemment, la loi prévoit des exceptions et l'on comprend bien qu'un chercheur en médecine puisse réaliser une enquête comportant des questions relatives à la santé.

L'article 9 de la loi est intéressant à plus d'un titre et nous le reproduisons ci-dessous intégralement:

Les traitements de données à caractère personnel relatives aux infractions, condamnations et mesures de sûreté ne peuvent être mis en œuvre que par:

1° Les juridictions, les autorités publiques et les personnes morales gérant un service public, agissant dans le cadre de leurs attributions légales ;

2° Les auxiliaires de justice, pour les stricts besoins de l'exercice des missions qui leur sont confiées par la loi ;

3° [Dispositions déclarées non conformes à la Constitution par décision du Conseil constitutionnel n° 2004-499 DC du 29 juillet 2004 ;]

4° Les personnes morales mentionnées aux articles L. 321-1 et L. 331-1 du code de la propriété intellectuelle, agissant au titre des droits dont elles assurent la gestion ou pour le compte des victimes d'atteintes aux droits prévus aux livres Ier, II et III du même code aux fins d'assurer la défense de ces droits.

Cet article encadre donc les fichiers de la police et de la justice. Il est intéressant de noter que l'article 3 a été censuré par le Conseil constitutionnel. Cela prouve, s'il en était encore besoin, que le problème de l'informatique et des libertés est un sujet sensible et qu'un certain nombre de députés ont cru bon d'interpeller le Conseil constitutionnel qui leur a donné en partie raison.

> Note
>
> La décision motivée du Conseil constitutionnel peut être consultée à l'adresse suivante:
>
> http://www.conseil-constitutionnel.fr/decision/2004/2004499/2004499dc.htm

La lecture de l'alinéa 4 pour les personnes qui ne sont pas habituées aux textes juridiques peut sembler complètement absconse. En fait, ces quelques phrases sont ce que l'on appelle un texte de circonstance car c'est sur sa base que les industriels du disque vont pouvoir poursuivre les internautes adeptes des échanges de fichiers grâce aux réseaux peer to peer (P2P). En clair, les maisons de disques vont pouvoir collecter les adresses IP de ceux qui s'adonnent aux joies du P2P et demander à un juge d'ordonner à un FAI de fournir l'identité du titulaire de l'abonnement Internet.

Les articles 11 à 21 de la loi définissent la composition et le rôle de la CNIL. Il faut noter que la CNIL n'est pas un tribunal, mais une autorité administrative indépendante. Son rôle est de regrouper et de contrôler l'ensemble des déclarations des traitements automatisés d'informations nominatives. Les articles 22 à 31 décrivent les formalités de ces déclarations.

Les articles 32 à 37 de la loi décrivent les obligations incombant aux responsables des traitements. Nous vous encourageons vivement à lire la totalité de ces articles, ce qui permettra de vous rendre compte que la majeure partie des questionnaires que vous remplissez en ligne ne respecte pas ces obligations.

Les articles 38 à 43 de la loi précisent les droits des personnes qui sont l'objet d'un traitement de données à caractère personnel.

Nous vous conseillons d'apprendre par cœur l'article 38 de cette loi et d'en user autant que vous le voulez :

«Toute personne physique a le droit de s'opposer, pour des motifs légitimes, à ce que des données à caractère personnel la concernant fassent l'objet d'un traitement.

Elle a le droit de s'opposer, sans frais, à ce que les données la concernant soient utilisées à des fins de prospection, notamment commerciale, par le responsable actuel du traitement ou celui d'un traitement ultérieur.»

C’est grâce au deuxième alinéa de cet article que l’on peut désormais faire figurer son numéro de téléphone en liste rouge sans avoir besoin de payer quoi que ce soit.

Pour résumer, une personne peut exercer les droits suivants face à un traitement de données à caractère personnel :

- **Droit d’être informé** sur la nature du traitement
- **Droit de s’opposer** au traitement
- **Droit d’accès** aux données collectées
- **Droit de rectification** des données

Les articles 45 à 49 de la loi définissent les sanctions que peut prendre la CNIL lorsqu’un responsable d’un traitement de données ne respecte pas ses obligations.

Les articles 50 à 52 précisent les sanctions pénales prévues par la loi en cas d’infraction. Ces infractions ont d’ailleurs été reprises dans le code pénal (*articles 226-16 à 226-24*). À titre indicatif, le fait, y compris par négligence, de procéder ou de faire procéder à des traitements de données à caractère personnel sans qu'aient été respectées les formalités préalables à leur mise en oeuvre prévues par la loi est puni de cinq ans d'emprisonnement et de 300 000 Euros d'amende.

ANNEXE B

Cliquez ici pour avoir le texte de loi intégralement



La LCEN

La loi du 21 juin 2004 pour la confiance dans l'économie numérique (ou LCEN) est un texte qui a mis du temps à aboutir. En effet, la LCEN est quelque part l'héritière du projet baptisé LSI (Loi sur la Société de l'Information) que le gouvernement de Lionel Jospin avait mis en chantier, mais qui n'a jamais vu le jour. Pourtant, dès le mois d'août 1997, le gouvernement avait fait de l'entrée de la France dans la société de l'information une de ses priorités. Malgré cette volonté affichée, les députés ont mis cinq ans (juin 2001) pour accoucher d'un projet de 32 pages qui n'a jamais pu passer devant l'Assemblée nationale. Arrivé au pouvoir, Jean-Pierre Raffarin a choisi d'abandonner ce projet pour en remettre un autre en route, la LCEN. Il aura également fallu deux ans pour que ce texte de loi voie le jour et soit publié au Journal Officiel...

La LCEN était attendue car il commençait à y avoir urgence sur plusieurs fronts. En effet, plusieurs problèmes comme celui de la responsabilité des hébergeurs, de la lutte contre le spam ou bien encore la question de la libéralisation totale de la cryptographie n'étaient pas réglés et les professionnels de l'Internet réclamaient à grands cris le vote d'une loi.

La LCEN est une loi qui compte 58 articles et qui est vraiment importante pour Internet. Il nous est impossible de citer tous les articles, mais nous vous conseillons d'aller sur le site de Legifrance pour la lire intégralement. Nous allons nous contenter ici d'indiquer les articles importants.

Dans son premier article, la LCEN affirme un principe de liberté :

La communication au public par voie électronique est libre.

L'exercice de cette liberté ne peut être limité que dans la mesure requise, d'une part, par le respect de la dignité de la personne humaine, de la liberté et de la propriété d'autrui, du caractère pluraliste de l'expression des courants de pensée et d'opinion et, d'autre part, par la sauvegarde de l'ordre public, par les besoins de la défense nationale, par les exigences de service public, par les contraintes techniques inhérentes aux moyens de communication, ainsi que par la nécessité, pour les services audiovisuels, de développer la production audiovisuelle.

L'article 2 de la LCEN précise des définitions qui n'avaient jamais été données auparavant :

On entend par communications électroniques les émissions, transmissions ou réceptions de signes, de signaux, d'écrits, d'images ou de sons, par voie électromagnétique.

On entend par communication au public par voie électronique toute mise à disposition du public ou de catégories de public, par un procédé de communication électronique, de signes, de signaux, d'écrits, d'images, de sons ou de messages de toute nature qui n'ont pas le caractère d'une correspondance privée.

C'est désormais le Conseil supérieur de l'audiovisuel (CSA) qui a la mission de garantir l'exercice de la liberté de communication audiovisuelle en matière de radio et de télévision par tout procédé de communication électronique.

Le Chapitre II de la LCEN traite des fournisseurs d'accès à Internet (FAI) appelés dans la loi prestataires techniques. L'article 6 règle le délicat problème de la responsabilité des hébergeurs. Il faut ici rappeler qu'en cas de contenu illicite publié sur un site Web, l'hébergeur pouvait être déclaré complice. Les hébergeurs prétendaient à juste titre qu'ils ne pouvaient pas

surveiller tous leurs clients étant donné leur grand nombre et que la mission de contrôle du contenu de ce qui passait dans leurs tuyaux ne pouvait pas leur incomber. Le législateur leur a donné satisfaction et précise que « les personnes physiques ou morales qui assurent, même à titre gratuit, pour mise à disposition du public par des services de communication au public en ligne, le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par des destinataires de ces services ne peuvent pas voir leur responsabilité civile engagée du fait des activités ou des informations stockées à la demande d'un destinataire de ces services si elles n'avaient pas effectivement connaissance de leur caractère illicite ou de faits et circonstances faisant apparaître ce caractère ou si, dès le moment où elles en ont eu cette connaissance, elles ont agi promptement pour retirer ces données ou en rendre l'accès impossible. »

Un autre alinéa précise que la responsabilité pénale de l'hébergeur n'est pas non plus engagée. Ce texte règle donc le problème de la responsabilité a priori de l'hébergeur. La loi précise clairement que les FAI ne sont pas soumis à une obligation générale de surveiller les informations qu'ils transmettent ou stockent, ni à une obligation générale de rechercher des faits ou des circonstances révélant des activités illicites.

En revanche, si un FAI est avisé d'un contenu illicite mis en ligne sur la page perso d'un de ces clients, il doit immédiatement faire cesser le trouble. Le législateur a quand même pris une mesure pour limiter les recours des personnes qui voudraient faire cesser la publication d'une information sur un site Web. Ainsi toute personne qui présenterait à un hébergeur un contenu ou une activité comme étant illicite dans le but d'en obtenir le retrait ou d'en faire cesser la diffusion, alors qu'elle sait cette information inexacte, serait punie d'une peine d'un an d'emprisonnement et de 15 000 euros d'amende.

Les FAI doivent conserver pendant un an les données de nature à permettre l'identification de quiconque a contribué à la création du contenu ou de l'un des contenus des services dont elles sont prestataires.

La LCEN tente de responsabiliser les FAI en matière de droit d'auteur. Ainsi lorsqu'un FAI évoque dans une publicité la possibilité de télécharger des fichiers dont il n'est pas le fournisseur, il doit faire figurer dans cette publicité une mention facilement identifiable et lisible rappelant que le piratage nuit à la création artistique.

Le FAI a également l'obligation de suspendre, par tout moyen, le contenu d'un site Web portant atteinte à l'un des droits de l'auteur, y compris en ordonnant de cesser de stocker ce contenu ou, à défaut, de cesser d'en permettre l'accès.

Le Titre II de la LCEN traite du commerce électronique qu'il définit comme l'activité économique par laquelle une personne propose ou assure à distance et par voie électronique la fourniture de biens ou de services. Le commerce électronique couvre aussi les services tels que ceux consistant à fournir des informations en ligne, des communications commerciales et des outils de recherche, d'accès et de récupération de données, d'accès à un réseau de communication ou d'hébergement d'informations, y compris lorsqu'ils ne sont pas rémunérés par ceux qui les reçoivent.

Le Chapitre II de la LCEN règlemente la publicité par voie électronique mais il s'agit là d'une tentative de régler les problèmes posés par l'inflation croissance du spam.

L'article 20 stipule que « toute publicité, sous quelque forme que ce soit, accessible par un service de communication au public en ligne, doit pouvoir être clairement identifiée comme telle. Elle doit rendre clairement identifiable la personne physique ou morale pour le compte de laquelle elle est réalisée. »

La loi enfonce le clou en précisant que « dans tous les cas, il est interdit d'émettre, à des fins de prospection directe, des messages au moyen d'automates d'appel, télécopieurs et courriers électroniques, sans indiquer de coordonnées valables auxquelles le destinataire puisse utilement transmettre une demande tendant à obtenir que ces communications cessent sans frais autres que ceux liés à la transmission de celle-ci. Il est également interdit de dissimuler l'identité de la personne pour le compte de laquelle la communication est émise et de mentionner un objet sans rapport avec la prestation ou le service proposé. »

Signalons un système pernicieux mis en place par certaines sociétés peu scrupuleuses : vous recevez un courriel publicitaire au bas duquel figure un lien permettant de vous désabonner et de ne plus recevoir ainsi de publicité. Vous cliquez sur ce lien qui affiche une page Web vous demandant de saisir votre adresse électronique. Si vous possédez plusieurs adresses électroniques grâce à des systèmes de redirection et que le champ Destinataire a été masqué par le spam, vous êtes alors incapable de savoir quelle adresse électronique il faut inscrire dans le formulaire de désabonnement. D'autre part, on peut légitimement se demander si une telle pratique n'est pas une méthode pour vérifier si votre adresse est bien valide. En général, quand on écrit à quelqu'un, on connaît son adresse électronique et si on souhaite lui donner la possibilité de ne plus lui envoyer de courrier, on n'a pas besoin de la lui demander.

Le Chapitre III de la LCEN consacre l'usage de l'écrit sous forme électronique grâce à la signature électronique. Ainsi, lorsqu'un écrit est exigé pour la validité d'un acte juridique, il peut être établi et conservé sous forme électronique. De la même manière, lorsqu'est exigée une mention écrite de la main même de celui qui s'oblige, ce dernier peut l'apposer sous forme électronique si les conditions de cette apposition sont de nature à garantir qu'elle ne peut être effectuée que par lui-même.

La LCEN définit également la manière dont les contrats sous forme électronique peuvent être conclus.

Le Titre III de la LCEN, intitulé « *De la sécurité dans l'économie numérique* » traite des moyens et prestations de cryptologie.

L'article 29 propose les définitions suivantes :

On entend par moyen de cryptologie tout matériel ou logiciel conçu ou modifié pour transformer des données, qu'il s'agisse d'informations ou de signaux, à l'aide de conventions secrètes ou pour réaliser l'opération inverse avec ou sans convention secrète. Ces moyens de cryptologie ont principalement pour objet de garantir la sécurité du stockage ou de la transmission de données, en permettant d'assurer leur confidentialité, leur authentification ou le contrôle de leur intégrité.

On entend par prestation de cryptologie toute opération visant à la mise en oeuvre, pour le compte d'autrui, de moyens de cryptologie.

L'article 30 est une véritable révolution car il énonce que « l'utilisation des moyens de cryptologie est libre. » Les professionnels de la sécurité attendaient cette disposition réglementaire depuis des années et ils ont donc toutes les raisons de s'en satisfaire. Cela étant, l'alinéa suivant précise que « la fourniture, le transfert depuis ou vers un Etat membre de la Communauté européenne, l'importation et l'exportation des moyens de cryptologie assurant exclusivement des fonctions d'authentification ou de contrôle d'intégrité sont libres. »

On ne comprend pas bien à la lecture de ce texte pourquoi le législateur a tenu à préciser son propos dans la mesure où il indiqué plus que la cryptologie était libre. En y regardant de plus près, on s'aperçoit que sont libres l'utilisation de la cryptologie pour authentifier et contrôler l'intégrité. Quelle est donc l'autre fonction de la cryptologie qui manque dans cette énonciation ? Si vous avez suivi, vous savez que la cryptologie sert bien évidemment aussi à masquer, cacher, chiffrer des informations. Bizarrement, cette fonctionnalité de la cryptologie n'est pas indiquée dans cet alinéa. On comprend mieux pourquoi quand on lit le suivant :

« La fourniture, le transfert depuis un Etat membre de la Communauté européenne ou l'importation d'un moyen de cryptologie n'assurant pas exclusivement des fonctions d'authentification ou de contrôle d'intégrité sont soumis à une déclaration préalable auprès du Premier ministre, sauf dans les cas prévus au b du présent III. »

On reste dubitatif quand on considère un pareil énoncé : pourquoi ne pas appeler un chat un chat ? La cryptologie qui chiffre est donc désignée par la périphrase « moyen de cryptologie n'assurant pas exclusivement des fonctions d'authentification ou de contrôle d'intégrité ».

Au cas où le lecteur n'aurait pas compris, le législateur indique que les outils qui ne sont pas soumis à déclaration sont « les catégories de moyens dont les caractéristiques techniques ou les conditions d'utilisation sont telles que, au regard des intérêts de la défense nationale et de

la sécurité intérieure ou extérieure de l'Etat, leur fourniture, leur transfert depuis un Etat membre de la Communauté européenne ou leur importation peuvent être dispensés de toute formalité préalable. »

Bref, ce texte signifie que l'on peut chiffrer ses fichiers tant que cela ne nuit pas aux intérêts de l'armée et de la police. Dans ces conditions, la cryptologie est-elle vraiment libre ?

Pour tous ceux qui n'auraient encore pas compris, le législateur précise que « le fait de fournir des prestations de cryptologie visant à assurer des fonctions de confidentialité sans avoir satisfait à l'obligation de déclaration prévue à l'article 31 est puni de deux ans d'emprisonnement et de 30 000 euros d'amende. »

La LCEN modifie également le code pénal en indiquant que lorsqu'un moyen de cryptologie a été utilisé pour préparer ou commettre un crime ou un délit, ou pour en faciliter la préparation ou la commission, cela constitue une circonstance aggravante qui accroît le nombre d'années de prison de la peine prévue.

L'article 39 de la LCEN paraît tellement étonnant que nous ne résistons pas au plaisir de vous le soumettre :

Les dispositions du présent chapitre ne font pas obstacle à l'application du décret du 18 avril 1939 fixant le régime des matériels de guerre, armes et munitions, à ceux des moyens de cryptologie qui sont spécialement conçus ou modifiés pour porter, utiliser ou mettre en œuvre les armes, soutenir ou mettre en œuvre les forces armées, ainsi qu'à ceux spécialement conçus ou modifiés pour le compte du ministère de la défense en vue de protéger les secrets de la défense nationale.

La LCEN se termine sur des dispositions sur les systèmes satellitaires et la couverture du territoire par les services numériques.

Au final, la LCEN est un texte juridique complexe et incomplet dans la mesure où il manque de nombreux décrets d'application importants, ce qui semble être une véritable spécialité française. En effet, on ne compte plus le nombre de textes votés, mais inappliqués en raison de la non publication des décrets d'application. Encore récent, ce texte a également besoin que la jurisprudence en précise certaines orientations. Il n'en reste pas moins qu'il s'agit du texte principal qui régit le droit de l'Internet. En tant que tel, il paraît difficile de l'ignorer si l'on est internaute.

ANNEXE C

Cliquez ici pour avoir les extraits de la décision du tribunal de Pontoise



Extraits de la décision du tribunal de Pontoise

Nous reproduisons ci-dessous des extraits de la décision du tribunal de Pontoise.

Alain O. est prévenu :

Avoir à Pontoise, du 1er août 2003 au 31 août 2004, en tout cas sur le territoire national et depuis temps n'emportant pas prescription, gravé et téléchargé en entier ou en partie, 614 albums de musique sans respecter les droits d'auteur et notamment la Sacem, la Sdrm et la Sppf, commettant ainsi des contrefaçons.

DISCUSSION

Sur l'action publique :

Le 18 février 2004, les gendarmes du Services Technique de Recherches Judiciaires et de Documentation de Rosny sous Bois, dans le cadre de la surveillance du réseau internet, découvraient un serveur géré par un particulier et dédié à l'échange de supports informatiques;

Selon le rapport, un internaute sous le pseudonyme d'"Altapunkz" se livrait à la contrefaçon et à la distribution de musique hors les circuits commerciaux légaux;

Le propriétaire du Hub devenant l'administrateur d'un réseau autorise ou refuse l'accès à son ordinateur;

Les militaires avaient plus particulièrement axé leurs investigations sur les transactions via des Hub, permettant la connexion en étoile d'autre PC;

Pour y accéder, il suffit d'installer un logiciel gratuit de type DC++ sur son propre ordinateur ;

En l'espèce, le Hub identifié appartenait à la société Pegase Computer Ltd basée en Angleterre mais avec des numéros de téléphone et de télécopie français et plus particulièrement dans la zone sud-est, commençant par 04;

Les enquêteurs constataient que 302 internautes étaient connectés en étoile. Ils s'intéressaient plus particulièrement à l'internaute utilisant le pseudonyme "Altapunkz" en raison de l'espace partagé de son disque dur, 30 000 giga de données. Ils pouvaient visualiser le contenue de son PC, notamment de nombreux fichiers musicaux au format MP3;

Sur réquisition judiciaire, l'internaute concerné était identifié comme étant Elodie B. avec comme adresse email "alain.o @free.fr";

Les gendarmes de la brigade territoriale de Cergy opéraient une perquisition le 18 août 2004 au domicile d'Elodie B. Ils étaient reçus par son concubin Alain O. Immédiatement, celui-ci déclarait être l'unique utilisateur de cette ligne internet et donnait son assentiment express pour une perquisition en la forme préliminaire. 185 CD gravés étaient découverts. La tour d'ordinateur était saisie;

Entendu, Alain O. reconnaissait sur le champ les faits. Il avait téléchargé en 2003 le logiciel DC++ lui permettant de se connecter à des Hub. Il précisait textuellement "j'ai pu durant environ un an télécharger et mettre à disposition des autres participants, des musiques et des films... En outre j'ai pratiqué la gravure de certaines de ces musiques à des fins personnelles".

En conclusion, il avouait "Je savais que cela était interdit mais je ne me rendais pas compte de la gravité de ce que je faisais";

A l'audience, le prévenu tentait, fort maladroitement au demeurant, de contester les faits ;

S'il reconnaissait le téléchargement de musique il niait avoir mis à disposition ses fichiers sur internet ayant toujours désactivé le partage, contrairement à ce qu'il avait déclaré aux gendarmes. S'il avait diffusé la liste des œuvres musicales, c'était uniquement pour accéder aux ordinateurs des autres internautes;

Son conseil produisait un constat d'huissier de plus de 500 CD compacts originaux. Il n'est pas exclu que ces disques lui appartenaient même si aucune mention n'a été faite au procès verbal de perquisition des gendarmes;

En revanche, il ressort très clairement du même procès verbal que les originaux des 185 CD gravés ne se trouvaient pas au domicile d'Alain O., ce qui en soit permet d'établir la prévention;

L'ensemble des éléments constitutifs de contrefaçon est réuni;

L'élément matériel ressort du téléchargement d'environ 10 000 œuvres musicales provenant d'autres ordinateurs connectés pour la plupart de ce Hub et la mise à disposition des internautes;

L'élément légal consiste en le transfert de programmes ou de données d'un ordinateur vers un autre. La jurisprudence a précisé les contours de cette notion;

Il s'agit d'un acte de reproduction, chaque fichier d'une œuvre numérisée étant copié pour être stocké sur le disque dur de l'internaute qui le réceptionne et d'un acte de représentation consistant dans la communication de l'œuvre au public des internautes par télédiffusion;

Ainsi dans le réseau de "peer-to-peer" utilisé par Alain O., celui-ci accompli les deux opérations. Il convient de préciser que le logiciel DC++, contrairement à ce que la défense a soutenu à l'audience, impose aux utilisateurs d'ouvrir leurs disques durs aux autres internautes raccordés au Hub;

Enfin, l'élément intentionnel résulte de la simple matérialité de cet agissement telle que la jurisprudence l'a défini et confirmé à plusieurs reprises;

Il conviendra toutefois de faire une application très modérée de la loi pénale. En effet ce remarquable outil de communication et d'échanges qu'est internet s'est développé sur une incompréhension lourde de conséquences;

Nombre d'internautes ont considéré ou cru qu'il s'agissait d'un univers, lieu de liberté où les règles juridiques élémentaires ne s'appliqueraient pas. Or, les utilisateurs de ce système doivent prendre conscience notamment de la nécessaire protection des droits des auteurs, compositeurs ou producteurs des œuvres de l'esprit;

Il résulte des éléments du dossier et des débats qu'il convient de déclarer Alain O. coupable pour les faits qualifiés de:

Contrefaçon par édition ou reproduction d'une œuvre de l'esprit au mépris des droits de l'auteur, faits commis du 1er août 2003 au 31 août 2004 à Pontoise, et qu'il y a lieu d'entrer en voie de condamnation.

DECISION

Le tribunal statuant publiquement, en matière correctionnelle, en premier ressort et par jugement contradictoire à l'encontre de Alain O., prévenu, à l'égard de la Sacem, la Sppf, la Scpp, la Sdrm, parties civiles;

Sur l'action publique:

. Déclare Alain O. coupable pour les faits qualifiés de :

Contrefaçon par édition ou reproduction d'une œuvre de l'esprit au mépris des droits de l'auteur, faits commis du 1er août 2003 au 31 août 2004, à Pontoise.

Vu les articles susvisés :

. Condamne Alain O. à une amende délictuelle de 3000 €.

Vu les articles 132-29 à 132-34 du code pénal :

. Dit qu'il sera sursis totalement à l'exécution de cette peine dans les conditions prévues par ces articles.

Si le tribunal s'est montré relativement clément sur le volet pénal en condamnant le prévenu à une peine avec sursis et en n'inscrivant pas cette condamnation au casier judiciaire de l'intéressé (ce qui lui permet entre autres de poursuivre sa carrière d'enseignant), en revanche les dommages et intérêts accordés aux parties civiles sont d'un montant très élevés pour cette première condamnation car ils avoisinent les 15000 euros.

Cette affaire est intéressante car elle constitue une première en France, mais une bonne cinquantaine d'autres affaires sont en attente de jugement.

En conclusion, si vous vous adonnez aux joies du P2P, vous vivez désormais dangereusement.