

mce

maison de la consommation et de l'environnement

centre technique départemental de la consommation

***Infractions et sanctions  
liées à l'utilisation de l'Internet***



Juillet 2001

<http://www.mce-info.org>

# Sommaire

A - La protection des logiciels :

B - Le respect des droits d'auteur sur une œuvre  
multimédia (cd-rom ou site web) :

C - La diffusion de contenus illicites et le droit  
de la presse :

D - Atteintes aux systèmes de traitement  
automatisé de données (STAD) :

E - Falsification de documents informatisés :

F - Le recel de données :

G - La correspondance privée :

H - La protection de l'intimité de la vie privée  
et la loi "informatique et libertés" :

I - Lexique et sources :

## A - La protection des logiciels

### ► Textes applicables :

*Loi n° 85660 du 3 juill. 1985* applicable au 1<sup>er</sup> janvier 1986. Antérieurement, les tribunaux s'étaient déjà prononcés sur la soumission des logiciels à la loi de 1957 sur la propriété littéraire et artistique.

Une *directive du conseil des communautés européennes du 14 mai 1991* instaure un régime juridique unifié pour les logiciels. Ce texte constitue le fondement et le système fédérateur des législations actuelles des états membres en matière de protection des logiciels.

La *loi du 10 mai 1994* a transposé en droit français cette directive. Cet ensemble législatif est intégré dans la première partie du code de la propriété intellectuelle (art L 111-1 à L 335-10).

La Commission européenne a lancé en octobre 2000 une consultation au sujet de la brevetabilité des logiciels. Les Etats membres de l'Office européen des brevets sont plutôt favorables à cette évolution à la différence des tenants du logiciel libre qui sont partisans d'un statut quo. La modification du traité de Munich interviendra en principe fin novembre 2000.

L'enjeu est de taille puisqu'un brevet confère une plus grande protection au créateur et beaucoup moins de droits aux tiers que le droit d'auteur.

### ► Sanctions et procédures :

**La contrefaçon** : La violation de l'un des droits de l'auteur d'un logiciel tels que définis à l'art L 122-6 du CPI est un délit de contrefaçon (L 335-2 al 2). La sanction de la contrefaçon a été considérablement aggravée par la *loi n° 94102 du 5 février 1994* prise dans le cadre de la lutte contre la contrefaçon (CPI L 335-2 à L 335-10). Ce délit est passible d'une peine d'emprisonnement de 2 ans et une peine d'amende de 1 million de FF. En cas de récidive, les peines sont portées au double (art L 335-9). En outre, des peines complémentaires peuvent être ordonnées : fermeture de l'établissement (L 335-5), la confiscation des recettes procurées (L 335-6), l'affichage de la condamnation (L 335-7).

L'administration des douanes peut en outre, sur demande écrite du titulaire d'un droit d'auteur assortie de justifications de son droit, retenir dans le cadre de ses contrôles les marchandises contrefaisantes.

Enfin, la contrefaçon constitue une faute délictuelle, de nature à engager la responsabilité civile de son auteur. La victime pourra donc agir soit devant la juridiction civile, soit devant la juridiction pénale en se constituant partie civile.

**La saisie-contrefaçon** : Procédure préventive permettant au titulaire des droits d'auteur sur un logiciel de rapporter la preuve des faits de contrefaçon invoqués, et d'obtenir avant toute décision au fond la saisie d'exemplaires contrefaisants.

Elle peut être effectuée en vertu d'une ordonnance du président du Tribunal de grande instance ou sur demande du titulaire des droits à un commissaire de police afin qu'il effectue une saisie-description ou copie du logiciel contrefait.

## B - Le respect des droits d'auteur sur une œuvre multimédia (cd –rom ou site internet)

Les composants d'une œuvre multimédia : le scénario, les données textuelles, sonores, audiovisuelles, graphiques et informatiques.

Cette œuvre se trouve par conséquent au carrefour des œuvres audiovisuelles, littéraires et artistiques, logicielles et des techniques de télécommunications.

Sa protection au titre des droits d'auteurs ne fait aucun doute.

Les éléments qui la composent (texte, son, image, scénario) bénéficient de la même protection et **tout utilisateur de l'Internet qui souhaite les employer doit au préalable en demander l'autorisation aux auteurs sous peine de sanction du code de la propriété intellectuelle.**

L'œuvre multimédia est également protégeable comme peut l'être une base de données.

### ► *Droits des auteurs des composants de l'œuvre multimédia :*

- **Texte** : autorisation préalable doit être demandée à l'auteur sous condition d'originalité et sauf s'il s'agit d'une utilisation à caractère privé ou dans le cadre d'une copie de sauvegarde (Art L 122-6-1 du CPI). La question des droits d'auteur appartenant aux journalistes, cédés dans le cadre de l'édition "papier" du journal mais ne prévoyant pas l'édition online de ces mêmes textes, a fait l'objet de plusieurs décisions, qui affirment leur droit à percevoir une rémunération supplémentaire pour toute publication en ligne [voir en annexe TGI de Lyon - 21/07/1999 : SNJ/Progrès de Lyon].
- **Son** : toute œuvre musicale est protégée par des droits d'auteur. A ce titre, l'auteur jouit des droits moraux et patrimoniaux et toute exploitation aux fins d'intégration nécessite son accord. Toute reproduction est constitutive de contrefaçon.

**Le tribunal correctionnel d'Epinal a condamné le 26 octobre 2000 un responsable de site à quatre mois de prison avec sursis et 20.000 F de dommages et intérêts pour avoir créé des liens hypertextes vers des sites proposant le téléchargement de fichiers MP3 pirates. Le fait que les fichiers concernés étaient hébergés à l'étranger n'a pas permis d'écarter la compétence du tribunal, la mise à disposition du public se faisant en France.**

**En septembre 1999 le tribunal correctionnel de Montpellier avait déjà condamné un jeune informaticien qui proposait des compilations sur cd audio au prix de 50 FF à une peine de 25.000 FF de dommages et intérêts au profit de la SSCP et la SDRM et à 200 heures de TIG. [ TGI Montpellier - 24/09/1999 - voir en annexe ]. Il est évident que ces décisions aux peines extrêmement lourdes sont destinées à dissuader les jeunes utilisateurs de pratiquer un trafic lucratif de contrefaçon de CD et autres téléchargements de fichiers MP3.**

- **Image** : des photographies, des dessins, des vidéos, infographies, illustrations, schémas, cartes et autres images réalisées par ordinateur sont des créations soumises au statut d'œuvre intellectuelle à condition de répondre au critère d'originalité. Pour toute numérisation d'une image, le producteur de l'œuvre multimédia doit obtenir la cession du droit de reproduction.
- **Bases de données** : elle sont également protégées par le code de la propriété intellectuelle (art. L. 122-5). Le code de la propriété intellectuelle prévoit que sont interdites les extractions substantielles tant d'un point de vue qualitatif que d'un point de vue quantitatif (art. L. 342-1). Pour exemple : T.Com Nanterre, 7<sup>ème</sup> chambre, 16 mai 2000, SA Pr Line c/ SARL Newsinvest.

## C - La diffusion de contenus illicites et le droit de la presse

Imaginons que dans le cadre de l'activité du site Cybercommune, un groupe structuré souhaite mettre en ligne un "e-zine", et que sur l'une des pages apparaisse la photographie de nu d'un mannequin célèbre, qui peut être déclaré responsable du contenu à titre principal ?

Base juridique : que le produit multimédia soit diffusé sur un réseau fermé ou ouvert, le droit de la presse et de la communication a vocation à s'appliquer à son contenu.

**La loi du 29 juillet 1881 sur la liberté de la presse et la loi du 30 septembre 1986 sur la liberté de communication, modifiée par la loi du 1<sup>er</sup> août 2000.**

En ce qui concerne les infractions au droit de la presse applicables au multimédia, on peut citer :

- ⇒ **La diffamation** : allégation ou imputation d'un fait qui porte atteinte à l'honneur ou à la considération de la personne ou du corps auquel le fait est imputé. Dans une décision du 27 août 1999, le Tribunal Correctionnel de Strasbourg a condamné un jeune homme de 20 ans à 10.000 FF d'amende pour avoir exprimé des propos racistes sur un forum de discussion [TGI Strasbourg - 27/08/1999].
- ⇒ Le **délit d'injure** désigne toute expression outrageante, terme de mépris ou invective qui ne renferme l'imputation d'aucun fait.
- ⇒ La **diffusion de fausses nouvelles**
- ⇒ La **publicité mensongère**
- ⇒ La **provocation aux délits et aux crimes**
- ⇒ La **violation de la vie privée** consécutive à la fixation, à l'enregistrement ou à la transmission de l'image d'une personne se trouvant dans un lieu privé, sans le consentement de cette dernière (art 226-1 et 226-2 du code pénal).
- ⇒ Si une œuvre véhicule un **message violent ou pornographique** ou de **nature à porter gravement atteinte à la dignité humaine**, susceptible d'être vu ou perçu par un mineur, les dispositions de l'art 226-24 du code pénal s'appliquent.

Les responsables des délits commis par voie de presse ou tout autre moyen de publication sont :

- les directeurs de publication ou éditeurs quelles que soient leurs professions ou leurs dénominations;
- ou en cascade : les auteurs, les imprimeurs, les vendeurs distributeurs et afficheurs ( loi du 29 juill. 1881 - art 42).

La prescription en matière de presse est en principe de 3 mois (art. 65 de la loi du 29 juill. 1881). Un arrêt de la Cour de Cassation du 21 mars 2000 précise néanmoins que les publications faites sur internet ne bénéficient pas de cette prescription particulière.

**Notre exemple** : dans ce cas, il a été jugé le 10 février 1999 que le responsable de la diffusion d'un contenu illicite est le propriétaire du site sur lequel les pages sont hébergées. Jurisprudence vivement contestée par les internautes et certains hommes politiques français (D. Strauss-Kahn et A. Madelin). Cette position tendait à assimiler le propriétaire du site d'hébergement à un directeur de publication responsable pénalement et civilement du contenu des pages hébergées.

[Sur ce point, voir le jugement du TGI de Paris - 28 janvier 1999 : affaire Costes / UEJF et l'arrêt de la Cour d'appel de Paris - 10 février 1999 : Estelle HALLIDAY / Valentin LACAMBRE]

Un arrêt de la Cour d'Appel de Versailles (8 juin 2000 – S.A. Multimania Production / Mme L., France Cybermedia, SPPI, Esterel) est venu préciser l'étendue de la responsabilité des hébergeurs.

Aux termes de cet arrêt il appartient à l'éditeur de site de « prendre les précautions nécessaires pour éviter de léser les droits des tiers et mettre en œuvre à cette fin des moyens raisonnables d'information (attirer l'attention des créateurs), de vigilance (surveillances des sites hébergés) et d'action (la fermeture des sites illégaux) ».

La loi du 30 septembre 1986 qui régleme l'audiovisuel a été modifiée depuis cet arrêt par la loi du 1<sup>er</sup> août 2000. Cette nouvelle loi prévoit dans son article 43-8 que les hébergeurs engagent leur responsabilité civile quand, saisis par un tiers estimant que le contenu lui cause un préjudice, ils n'ont pas procédé aux « diligences appropriées ».

Cette notion de diligence appropriée » a été censurée par le Conseil Constitutionnel dans une décision du 27 juillet 2000 car elle est trop imprécise. La décision du Conseil Constitutionnel remet en cause l'évolution que chacun appelait de ses vœux.

## D - Atteintes aux systèmes de traitement automatisé de données (STAD)

1er exemple : Un individu, à partir d'une des machines mises à sa disposition, se connecte sur le serveur d'une grande banque étrangère, arrive à pénétrer à l'intérieur de son système informatique et détruit ou détourne des données, puis quitte le local sans avoir été repéré.

2<sup>ème</sup> exemple : Ce même individu crée chez lui un virus capable d'encombrer l'ensemble du réseau et de créer un préjudice mondial, il se rend au local Cybercommune et envoie à partir d'une disquette ce virus par mail sur le réseau. Il quitte le site une fois sa besogne accomplie.

Toutes les pénétrations non autorisées dans un système informatique par quelque moyen que ce soit sont sanctionnées par les articles **323-1 et 323-7 du code pénal**.

Des services ont été créés au sein de la sous-direction des affaires économiques et financières de la police judiciaire, tel le **service d'enquête sur les fraudes aux technologies de l'information** (SEFTI - 20 fonctionnaires) et au sein de la gendarmerie, la **brigade centrale de répression de la criminalité informatique** (BCRCI - 10 fonctionnaires). Dans 8 cas sur 10, l'auteur de la fraude appartient à l'entreprise ou à l'organisme qui en est victime.

### ***1 - accès frauduleux dans un système de traitement automatisé des données (STAD) :***

L'action de pénétration ou d'intrusion dans un système de traitement automatisé de données est sanctionnée dès lors qu'il est opéré sans droit. La sanction est de 1 an d'emprisonnement et 100.000 F d'amende (**art 323-1 du code pénal**). Il est sanctionné même en l'absence de préjudice, la tentative est punie de la même manière que le délit lui-même. Ces peines sont aggravées lorsque le fait a causé un dommage même involontaire au système soit 2 ans d'emprisonnement et 200.000 F d'amende s'il y a eu suppression, modification ou altération de données du système.

### ***2 - Maintien frauduleux dans un STAD :***

Il y a infraction dès lors que le délinquant a eu conscience de se maintenir anormalement dans le système. Il n'est en revanche pas nécessaire qu'il ait eu l'intention de nuire. La sanction est de 1 an d'emprisonnement et 100.000 F d'amende (**art 323-1 du code pénal**). Il est sanctionné même en l'absence de préjudice, la tentative est punie de la même manière que le délit lui-même. Ces peines sont aggravées lorsque le fait a causé un dommage même involontaire au système soit 2 ans d'emprisonnement et 200.000 F d'amende s'il y a eu suppression, modification ou altération de données du système. Dans un jugement du 16 décembre 1997, le TGI de Paris s'est prononcé sur un accès frauduleux au réseau Internet. Le prévenu, s'était rendu coupable d'accès frauduleux dans un système de traitement automatisé de données ainsi que d'introduction frauduleuse de données dans ce même système, du fait de la mise en œuvre d'un programme "sniffer" à l'intérieur d'un serveur connecté au réseau Internet [TGI Paris - 16 décembre 1997 - Ministère public/G.].

### ***3 - Atteinte volontaire au fonctionnement d'un STAD :***

L'entrave au fonctionnement d'un STAD n'est pénalement sanctionnée que lorsqu'il y a prise de conscience de l'individu qui a intentionnellement entravé le fonctionnement du système en ne respectant pas le droit d'autrui. Ex : les bombes logiques qui introduisent des instructions parasites, occupations de capacité mémoire dans le but de saturer le système.

La sanction est de 3 ans d'emprisonnement et 300.000 d'amende (art 323-2 du code pénal). La tentative est punie de la même manière que le délit lui-même.

Il est toutefois à noter que ces infractions sont souvent accompagnées d'une plainte pour escroquerie. (Libé.)

### Le virus informatique

Un virus est un programme informatique qui possède la capacité d'introduire dans d'autres programmes des copies exécutables de lui-même mais légèrement altérées. Ce phénomène étant récurrent, l'infection se propage. Le délit n'est constitué que si ces opérations sont faites avec une intention délictueuse et hors de l'usage autorisé. L'intention frauduleuse est constituée dès le moment où l'introduction des données s'effectue avec une volonté de modifier l'état du système. La sanction est de 3 ans d'emprisonnement et 300.000 d'amende (art 323-2 du code pénal). La tentative est punie de la même manière que le délit lui-même.

#### ***4 - Les personnes responsables :***

► **Le responsable physique** est l'auteur de l'infraction, c'est à dire celui qui en a commis l'élément matériel.

**La responsabilité du chef d'entreprise est un principe : il est responsable des conséquences pénales des infractions commises dans le cours de l'activité de l'entreprise. Même s'il n'a pas matériellement participé au délit, il peut être condamné au motif qu'il a manqué à l'obligation lui incombant personnellement en qualité de dirigeant légal, d'exercer les contrôles nécessaires sur la pratique de ses préposés sauf s'il a accompli des diligences normales compte tenu des moyens dont il dispose (article 121-3 du code pénal).**

**IL EST PROBABLE QUE DANS LE CADRE D'UNE PLAINTE REPOSANT SUR DE TELS FAITS, LE JUGE VERIFIERA SI EN L'ESPECE, LE REPRESENTANT LEGAL DE LA COMMUNE A ACCOMPLI LES DILIGENCES NORMALES OU S'IL A COMMIS UNE IMPRUDENCE PREJUDICIABLE.**

En matière d'atteintes aux STAD, 7 peines complémentaires sont encourues pour les infractions commises par des personnes physiques (article 323-1 du code pénal) :

- ⇒ Interdiction pour 5 ans au plus d'exercice des droits civiques
- ⇒ Interdiction pour 5 ans au plus d'exercer une fonction publique ou activité professionnelle dans l'exercice de laquelle l'infraction a été commise.
- ⇒ Confiscation de la chose qui a servi à commettre l'infraction.
- ⇒ Fermeture pour une durée de 5 ans au plus des établissements ayant servi à commettre les faits incriminés
- ⇒ Exclusion pour 5 ans au plus des marchés publics
- ⇒ Interdiction pour 5 ans au plus d'émission de chèques
- ⇒ Affichage ou diffusion de la décision prononcée.

► **Les personnes morales** : création récente (article 121-2 du code pénal). Elle ne fait pas échec à la responsabilité personnelle du chef d'entreprise dès lors qu'il est intervenu personnellement dans la décision ou dans la réalisation de l'infraction. Pour que cette responsabilité puisse être engagée, il faut que l'infraction ait été commise par un organe ou un représentant de la personne morale et pour le compte de cette personne morale.

Sanction : Le taux de l'amende encourue par les personnes morales est fixé au quintuple de l'amende encourue par les personnes physiques pour la même infraction.

Peines complémentaires : article **131-39 du code pénal**.

**La délégation est un moyen de se dégager de cette responsabilité** : procédé par lequel un dirigeant transfère à l'un de ses salariés une partie de ses fonctions, celui-ci s'accompagnant d'un transfert de responsabilité pénale. Les infractions peuvent avoir de très lourdes conséquences allant jusqu'à la disparition de l'entreprise quand il y a piratage par exemple, lorsque l'amende prononcée est de 150.000 FF et plus. Toutefois, la délégation doit rester partielle et limitée, et consentie à un délégué pourvu de la compétence, de l'autorité et des moyens nécessaires à l'exercice des pouvoirs délégués. (Par contrat de travail par exemple).

#### **Commentaire :**

**France Télécom avoue connaître environ 900 attaques de son système informatique par week-end, et il est de plus en plus fréquent de voir dans la presse les confessions ou découvertes a posteriori d'actes de piratage.**

**De l'aveu même d'un dirigeant du CLUSIF (Club de la sécurité des systèmes d'information français), l'an 2000 crée de très belles opportunités de fraudes, extorsions, malveillances.**

**Il convient par conséquent d'être très vigilant face à ce fléau et de mettre en place des outils techniques et juridiques afin de parer à toute éventualité. En outre, une récente déclaration de Michael Vatis, qui dirige pour le FBI un centre de surveillance des secteurs stratégiques explique qu'en un an, les actes criminels liés à l'Internet ont doublé, notamment en matière de fraude financière.**

[Voir à ce sujet le jugement du Tribunal correctionnel de Limoges du 14 mars 1994 ainsi que ceux du Tribunal correctionnel de Paris du 14 juin 1994 et du 2 avril 1992]

## E - falsification de documents informatisés :

Incrimination générale de **faux et usage de faux** : *article 411-1 du code pénal*. Le délit d'usage de faux est constitué par toute utilisation d'un document falsifié en connaissance de son caractère altéré.

Sanction de **3 ans d'emprisonnement** et **300.000 F d'amende**.

*La falsification de cartes de paiement* relève du délit de faux et usage de faux mais son application est rare depuis l'entrée en vigueur de la *loi du 30 décembre 1991* relative à la sécurité des chèques et des cartes de paiement qui prévoit des sanctions spécifiques pour la falsification, la contrefaçon et l'usage en connaissance de cause d'une carte de paiement contrefaite ou falsifiée.

La sanction d'**emprisonnement prévue est de 1 à 7 ans** et de **3.600 à 500.000 F d'amende**.

Le magazine "Netsurf" dans son numéro consacré aux arnaques sur l'Internet indique qu'aux Etats-Unis, trois ou quatre commerçants se sont fait dépouiller par des "hackers" qui ont pénétré le système d'information des entreprises afin d'y dérober des listes entières de titulaires de cartes bancaires. Plus grave, la DGCCRF a récemment découvert sur le Net un fichier de 26000 noms comportant adresse postale, e-mail, numéro de carte bleue avec date d'expiration. Cette liste circule toujours sur le réseau, passant de site de "hacker" en site de "hacker". [SVM avril 1999]

## F - Le recel de données :

**Exemple : Un individu accède à des sites ou forums et charge dans la mémoire de l'ordinateur mis à disposition des images à caractère pédophile, faits réprimés par les articles L 227-22 et 227-23 du code pénal.**

[Sur ce point, voir le jugement du TGI du Mans - février 1998 : Ministère Public / Philippe H.]

Le fait de dissimuler, de détenir ou de transmettre une chose que l'on sait provenir d'un crime ou d'un délit est constitutif d'un recel de données. Ce délit est autonome. Ainsi, l'utilisateur Internet peut-il être poursuivi pour **recel** en chargeant des données sur son ordinateur personnel provenant d'un délit. L'élément intentionnel doit être prouvé.

La sanction prévue est de **5 ans d'emprisonnement** et de **2.500.000 F d'amende**, selon l'***article 321-1 du code pénal***.

Des peines complémentaires encourues pour le crime dont provient le bien recélé peuvent également être prononcées, sans qu'il soit exigé que l'auteur ait eu connaissance de l'infraction ou des circonstances aggravantes accompagnant celle-ci : ***article 321-10 du code pénal***.

La responsabilité des personnes morales est également encourue.

## G - La correspondance privée :

Le statut des correspondances privées est fixé et protégé par le code des postes et télécommunications, la convention de sauvegarde des droits de l'homme et des libertés fondamentales (art 8), et la déclaration universelle des droits de l'homme (art 12).

La **loi du 10 juillet 1991** réprime elle aussi dans l'article 226-15 du code pénal, le fait d'intercepter, de détourner, d'utiliser ou de divulguer des correspondances émises, transmises ou reçues par voie des télécommunications ou de procéder à l'installation d'appareils pour le faire.

La difficulté réside donc dans le fait de savoir s'il s'agit de correspondance privée ou communication audiovisuelle, selon la **loi du 30 septembre 1986** :

*"La communication audiovisuelle se définit par opposition à la correspondance privée. Il y a correspondance privée lorsque le message est exclusivement destiné à une ou plusieurs personnes physiques ou morales déterminées et individualisées. A l'inverse, il y a communication audiovisuelle lorsque :*

*Le message est destiné indifféremment au public en général ou à des catégories de public, c'est à dire un ensemble d'individus indifférenciés, sans que son contenu soit fonction de considérations fondées sur la personne".*

Un jugement du Tribunal Correctionnel de Paris en date du 2 novembre 2000 a confirmé que le courrier électronique relevait bien de la correspondance privée. Maintenant se pose la question de la limite à l'utilisation par les salariés des boîtes électroniques mises à leur disposition par leurs employeurs.

La sanction prévue par l'**article 226-15 du code pénal** : 1 an d'emprisonnement et 300.000 F d'amende.

## H - Le respect de l'intimité de la vie privée et la loi "informatique et libertés" :

La loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés afin de concilier les droits des individus et la liberté de collecte des informations les concernant, fixe les obligations suivantes pour toute structure souhaitant ouvrir un fichier informatique contenant des données nominatives :

- Les données personnelles ne peuvent être collectées, traitées, conservées ou transmises à des tiers qu'en vue de réaliser des finalités déterminées, légitimes et compatibles entre elles.
- La collecte, le traitement, la conservation des données personnelles et leur transmission éventuelle à des tiers doit s'effectuer de manière loyale, c'est à dire que les personnes visées doivent être informées de l'identité et du lieu d'établissement de la personne qui traite les données, des finalités poursuivies, du caractère obligatoire ou facultatif du traitement des données, des destinataires des informations.
- Lorsqu'elles portent sur des données sensibles (opinion politique, religion...), elles ne peuvent être collectées qu'avec le consentement des personnes.
- Les personnes doivent se voir reconnaître les droits d'accéder à toutes les données les concernant, de les corriger.

La directive européenne du 24 octobre 1995 pose le principe que les transferts internationaux de données ne peuvent avoir lieu qu'à destination de pays assurant un niveau de protection adéquat. Cette disposition va peu à peu obliger les partenaires de l'Europe à adopter une législation aussi protectrice des droits des citoyens que l'est la loi de 1978, dont le législateur européen s'est fortement inspiré.

En outre, la Commission nationale informatique et libertés (CNIL), autorité administrative et indépendante créée par la loi du 6 juillet 1978 est chargée de veiller au respect de ses dispositions.

Depuis janvier 1999, la Cnil a permis d'effectuer par voie électronique sur son site web ([www.cnil.fr](http://www.cnil.fr)) une déclaration pour tout site web constituant des fichiers de données nominatives. Plus de 20.000 sites se sont déclarés de cette manière depuis la mise à disposition de ce formulaire.

### **Cryptage / Chiffrement**

Lionel Jospin s'était exprimé lors d'une conférence de presse le 19 janvier 1999 en direction des internautes français qui réclamaient depuis un an la libéralisation des moyens de cryptage ou de chiffrement des informations transmises sur l'Internet. C'est désormais chose faite grâce aux décrets du 17 mars 1999 qui assurent la confidentialité des transactions, en autorisant le cryptage jusqu'à la limite de 128 bits (au lieu de 40 bits auparavant).

# I - Lexique et sources :

## Lexique :

- **e-zine** : magazine rédigé et diffusé exclusivement sur l'Internet.
- **"Hacker" ou "hacking"** : fait de pénétrer à l'intérieur d'un système de traitement automatisé de données en ayant franchi la barrière de sécurité ou "firewall". Couramment appelé acte de piratage informatique et cyberpirate.
- **In concreto** : Contrôle exercé par le juge sur l'attitude du justiciable ; en tenant compte de ses propres capacités, de l'environnement
- **In abstracto** : contrôle opéré par le juge ne tenant pas compte des circonstances générales mais une appréciation sur la manière dont aurait agi l'homme moyen.
- **Hébergeur** : Offre des services comme le stockage de pages web, des serveurs de messagerie, des listes de diffusion. Il a un rôle strictement technique.
- **Serveur** : Ordinateur chargé de répondre aux demandes des ordinateurs clients, par exemple stocker des pages web ou aller les chercher sur l'Internet.
- **STAD** : système de traitement automatisé de données.
- **World Wide Web ou Web** : Toile d'araignée mondiale qui donne accès aux 1,2 milliards de pages HTML (estimation). Moins de la moitié de ces pages (525 millions) est indexée par le plus gros moteur de recherche Google.

## Sources :

### Ecrites :

"Informatique et Télécoms" d'Alain Bensoussan - Editions Francis Lefebvre

JCP Communication - Commerce électronique

Rapport du Conseiller d'état Isabelle Falque-Pierrotin : "Internet et les réseaux numériques"

Rapport d'Agnès BERTRAND : "La responsabilité pénale du maire et de la commune"

Rapport d'activité de la Cnil 1998/1999

Magazine "Pirates mag"

Magazine Netsurf

Magazine SVM

### Web :

[www.juriscom.net](http://www.juriscom.net)

[www.legalis.net](http://www.legalis.net)

[www.cnil.fr](http://www.cnil.fr)

[www.clusif.asso.fr](http://www.clusif.asso.fr)

[www.journaldunet.com](http://www.journaldunet.com)

[www.droit-technologie.com](http://www.droit-technologie.com)