



LE DROIT DE L'INFORMATIQUE, DES  
RESEAUX ET DES TECHNIQUES DE  
L'INFORMATION ET DE LA  
COMMUNICATION

---

SEPTEMBRE 2004

---

## Sommaire

Les majors livrent un combat planétaire contre le P2P ! - 27/09/2004.....	2
La loi Informatique et Libertés -20/09/2004.....	4
La marque prend de la bouteille : la protection des formes par le droit des marques -14/09/2004 .....	11
L'impact de la LEN sur la relation client (2) -13/09/2004.....	15
L'impact de la LEN sur la relation client (1) -04/09/2004.....	17
Fichiers de police : Lorsque la sécurité nie le droit au travail - 02/09/2004.....	20

---

## Propriétés intellectuelles, Droit d'auteur

---

### Les majors livrent un combat planétaire contre le P2P ! - 27/09/2004

*Par Me. Nicole Bondois, Avocate .*



Le 19 août dernier, la Cour d'Appel de Los Angeles a confirmé que les éditeurs des logiciels peer to peer Grokster et Morpheus ne pouvaient être considérés comme responsables des utilisations illicites de leur logiciel par les internautes.

Le 19 août dernier, la Cour d'Appel de Los Angeles a confirmé que les éditeurs des logiciels peer to peer Grokster et Morpheus ne pouvaient être considérés comme responsables des utilisations illicites de leur logiciel par les internautes.

En effet, leurs services étant déconcentrés (absence de serveur centralisant les fichiers échangés), il est techniquement impossible de contrôler les téléchargements violant les droits d'auteur.

La Cour fédérale américaine ne s'est bornée ici qu'à reprendre la motivation d'un jugement qui avait déjà permis, en son temps, de poursuivre la commercialisation des magnétoscopes Betamax (Sony), au motif qu'il était techniquement impossible d'empêcher les consommateurs de les utiliser à des fins de contrefaçon (Cour Suprême des Etats-Unis, SONY CORPORATION OF AMERICA ET AL c/ UNIVERSAL CITY STUDIOS, INC., ET AL., 17 janvier 1984).

En référence aux mêmes principes, la Cour suprême des Pays-Bas avait estimé, elle aussi, que le logiciel de partage de fichier Kazaa était légal (19 décembre 2003).

Mais les Majors ne désarment pas, la société australienne Sharman Networks, éditrice de Kazaa (toujours en litige aux Etats-Unis), est aujourd'hui poursuivie par l'industrie musicale australienne (via le Mipi).

Le Mipi (Music Industry Piracy Investigations<sup>1</sup>) a en effet obtenu, en février dernier, un mandat pour perquisitionner le siège de Sharman Networks, les domiciles de sa présidente, de son responsable technologique ainsi que celui de certains partenaires

commerciaux.

Ce nouveau procès contre Kazaa est annoncé comme l'un des plus importants en matière de violation de copyrights ; près d'un demi-million de fichiers électroniques ont été saisis<sup>2</sup> et une centaine de cas devraient être soumis au juge australien. Il devrait débiter fin novembre à Sydney.

Précisons enfin que l'industrie du disque se défend sur tous les fronts de la contrefaçon. En France, elle dispose depuis le 6 août dernier d'une disposition lui permettant de collecter en toute légalité les adresses IP des internautes soupçonnés de piratage<sup>3</sup>. Aux Etats-Unis un projet de loi<sup>4</sup> vise à sanctionner les éditeurs de logiciels peer to peer pour toute utilisation illicite effectuée par leurs clients !!!

**Par Me. Nicole Bondois, Avocate .**

1Section anti-piratage de l'association australienne de l'industrie du disque (Aria).

2Selon Me Ellicott, avocat de Sharman Networks.

3Loi 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 – 6 août 2004.

4Inducing Infringement of Copyrights Act.

---

## Informatique et libertés, Droits de la personnalité

---

### La loi Informatique et Libertés -20/09/2004

*Par Me. Murielle-Isabelle Cahen, Avocate .*



**« 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 ».**

► Ainsi commence la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, dite « loi Informatique et Libertés » (LIL).

Véritable pierre angulaire de la société française informatisée depuis 26 ans, la LIL a été instituée en réponse au projet SAFARI de 1974. Le ministère de l'Intérieur désirait mettre en place un système automatisé pour les fichiers administratifs et le répertoire des individus. Grâce à un identifiant unique, l'administration pourrait interroger le système et disposer de la totalité des informations enregistrées sur une même personne.

Face au scandale suscité par le projet SAFARI, le gouvernement a créé une autorité indépendante administrative : la Commission Informatique et liberté. La loi Informatique et Libertés est donc née : il s'agissait de réguler le phénomène informatique pour endiguer les abus possibles.

Une modification de la LIL était nécessaire pour permettre une meilleure adaptation aux situations actuelles. Le 18 juillet 2001, un projet de loi voit le jour. Le 15 juillet 2004, les Sénateurs ont adopté définitivement, en deuxième lecture, le projet de loi. Le 29 juillet 2004, le Conseil constitutionnel a validé la LIL modifiée.

La refonte de la LIL a pour principal objectif de transposer en droit interne la directive européenne du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel.

L'objet de la Directive était d'établir « une procédure équivalente de haut niveau dans tous les Etats membres de la Communauté afin d'éliminer les obstacles aux échanges de données nécessaires au fonctionnement du marché intérieur ».

Cette directive aurait dû être transposée en droit français depuis octobre 1998 : la France restait le dernier pays de l'Union européenne à ne pas l'avoir fait.

Par ailleurs, le projet de loi a également pour ambition d'adapter la LIL « au développement du traitement automatisé d'informations nominatives dans le secteur privé comme dans le secteur public et plus largement aux nombreuses évolutions technologiques de notre société de l'information ».

La LIL version 2004 apporte de nombreuses modifications qui sont vivement discutées par les professionnels du droit et de l'informatique :

- . son champ d'application est précisé pour permettre une meilleure adaptation aux enjeux juridiques actuels de la société française informatisée (1),
- . la procédure de déclaration des fichiers et traitements automatisés se veut allégée et simplifiée (2),
- . la CNIL se voit dotée de nouveaux pouvoirs de contrôle et de sanction (3).

## 1. Un champ d'application de la LIL précisé

### . Abandon du terme : « informations nominatives »

Lorsque la loi de 1978 est instituée, le chapitre 1 « Principes et définitions » parle essentiellement d' « informations nominatives ».

La LIL version 2004 transpose la directive européenne de 1995 et opte pour un terme plus général (« données à caractère personnel ») afin d'englober le plus de situations possibles.

Une définition est donnée à l'article 2 nouveau de la loi : « 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 ».

L'emploi de ce terme permet de viser toutes les données permettant l'identification d'une personne : nom, numéro d'identification, voix, image et empreintes digitales.

### . Des précisions textuelles

La nouvelle loi détaille de nombreuses notions : les données à caractère personnel, les traitements automatisés, les fichiers, la personne concernée par les traitements, le responsable des traitements.

L'article 4 nouveau précise que les copies temporaires faites dans le cadre d'activités techniques de transmission ou de fourniture d'accès à un réseau pour permettre le meilleur accès possible aux informations transmises ne sont pas concernées par la présente loi.

Par ailleurs, la LIL version 2004 indique qu'elle trouve à s'appliquer dès lors qu'un élément se rattache au territoire français : responsable du traitement automatisé établi en France, moyens de traitements situés en France ou encore représentant en France.

La loi crée un nouveau chapitre 2 relatif aux « conditions de licéité des traitements de données à caractère personnel ». Les données à caractère personnel doivent remplir plusieurs conditions, prévues à l'article 6 nouveau, pour être licites :

- .être collectées et traitées de manière loyale et licite,
- .être collectées pour des finalités déterminées,
- .être adéquates, pertinentes et non excessives face à leur finalité,
- .être exactes, complètes et mises à jour,
- .être conservées en respectant les délais de conservations.

L'accent est mis sur le consentement de la personne concernée par la collecte et le traitement de ses données à caractère personnel (article 7 nouveau).

## **. Responsabilité et droits**

Le chapitre 5 (articles 32 à 42 nouveaux) est entièrement consacré à la responsabilité incombant aux responsables des traitements de données et aux droits des personnes concernées par ces traitements.

Le responsable des traitements a l'obligation d'informer les personnes concernées, notamment lorsque les données les concernant ne sont pas recueillis directement auprès d'elles. L'obligation d'information est donc renforcée. De plus, le projet de loi précise que le responsable des traitements se doit de conserver les données et d'en préserver la

sécurité sous peine de sanction.

Les personnes concernées par le traitement disposent de droits nouveaux. La loi de 1978 subordonnait le droit d'opposition à la justification de « raisons légitimes ». La LIL version 2004 maintient ce droit (article 38 nouveau) mais précise que ce droit d'opposition sera discrétionnaire et sans frais lorsque les données seront utilisées à des fins de prospection, notamment commerciale.

Par ailleurs, les fichiers relatifs à la sûreté de l'Etat, la défense et la sécurité publique et accessibles que par l'intermédiaire de la CNIL pourront être communiqués à la personne concernée si les intérêts publics ne sont pas mis en cause (articles 41 et 42).

Enfin, la loi prévoit, sans changement, le droit d'accès et à rectification des données à caractère personnel par les intéressés : il s'agit de l'article 40 nouveau.

Toutes ces précisions permettent de mieux encadrer l'application de la LIL.

## **2. Une procédure de déclaration des fichiers allégée et simplifiée**

### **. Le correspondant à la protection des données**

Le projet de loi propose de simplifier les formalités préalables de déclaration lorsque les fichiers ne concernent pas des données sensibles.

Les personnes morales seront dispensées de toute déclaration si elles se dotent d'un correspondant à la protection des données, une personne qui servira d'intermédiaire entre l'entreprise et la CNIL et veillera ainsi au respect des dispositions de la loi (article 22 nouveau).

Le projet de loi transpose l'article 18 de la directive européenne de 1995. Cet article énonce, en effet, que le responsable du traitement peut désigner « un détaché à la protection des données à caractère personnel chargé notamment d'assurer, d'une manière indépendante, l'application interne des dispositions nationales prises en application de la présente directive, de tenir un registre des traitements effectués par le responsable du traitement, et garantissant de la sorte que les traitements ne sont pas susceptibles de porter atteinte aux droits et libertés des personnes concernées ».

Alex Türk, président de la CNIL, a déclaré que la mise en place de ces correspondants à la protection des données permettra de « jeter d'avantages de passerelles entre une série d'acteurs (entreprises, collectivités locales, associations) et la CNIL ». Il précise que

ces correspondants « feront de la pédagogie et de la formation interne, ils seront à même de tirer les signaux d'alarme » et seront en liaison systématiquement avec la CNIL.

Le Conseil constitutionnel a précisé, dans sa décision du 29 juillet 2004, que la désignation d'un correspondant dispense uniquement des déclarations mais ne concernent pas les traitements soumis à autorisation ou les transferts de fichiers hors de l'Union européenne. Cette désignation ne soustrait d'ailleurs pas les traitements non déclarés aux autres obligations prévues par la loi dont le non respect sera sanctionné.

### **. Fichiers publics et privés**

Jusque là, les fichiers publics et privés n'avaient pas le même régime : les premiers devaient être autorisés préalablement par la CNIL, les seconds devaient être seulement déclarés.

La CNIL effectuait donc un contrôle a priori des fichiers publics et un contrôle a posteriori des fichiers privés.

Désormais, les fichiers créés par les pouvoirs publics relèvent du régime des fichiers privés. Le gouvernement fait valoir que la distinction entre fichiers publics et fichiers privés est dépassée : nombre de fichiers publics collectent des données anodines mises en œuvre, la plupart du temps, par des opérateurs privés, ce qui présente des risques d'atteinte à la liberté individuelle et à la protection de la vie privée.

Par ailleurs, il est à noter qu'avant ce projet de loi, la CNIL disposait pourtant d'un pouvoir d'autorisation sur les fichiers administratifs mais n'a jamais pu asseoir son autorité. Par exemple, le STIC (fichier informatisé comprenant des données sur les auteurs et les victimes de crimes et délits) a été mis en place et utilisé en 1996 mais n'a obtenu de reconnaissance légale par décret qu'en juillet 2001.

Avec le projet de loi, l'avis de la CNIL ne sera que purement facultatif, le gouvernement n'aura plus à en tenir compte. La Commission ne pourra donc plus s'opposer aux nouveaux fichiers de l'Etat. Les fichiers policiers n'auront plus besoin d'obtenir l'aval de la CNIL pour être activés.

La Fédération Informatique et Libertés (FIL) qui rassemble plusieurs associations, le collectif Délis (Droits et libertés face à l'informatisation de la société) et la ligue des Droits de l'Homme dénoncent ces dispositions qui, selon eux, « constituent un abaissement très sérieux du niveau de protection des citoyens face aux traitements de leurs données personnelles ».



## **. Fichiers relatifs aux données sensibles**

Désormais, c'est la finalité du fichier et la nature des données collectées qui détermineront le régime applicable, peu importe qu'il s'agisse d'un fichier public ou privé.

La LIL prévoit deux régimes : la déclaration des fichiers relatifs à des données anodines et l'autorisation par la CNIL pour les fichiers portant sur des données plus sensibles tels que des données génétiques ou relatives aux infractions et condamnations (article 25 nouveau).

De même, les données qui ont pour finalité l'exclusion du bénéfice d'un droit, d'une prestation ou d'un contrat dès lors que cette exclusion ne repose pas sur une condition légale ou réglementaire ou qui ont pour finalité l'interconnexion des fichiers de nature différente seront également soumis à autorisation de la CNIL (article 25 nouveau).

Par ailleurs, il est à noter que l'article 8 nouveau énonce qu'il est interdit de collecter et d'enregistrer des données sensibles telles que des données relatives à l'origine ethnique, les opinions politiques, les convictions religieuses, les mœurs de la personne.

Seulement il pourra être dérogé à cette interdiction sur les traitements de données s'ils sont justifiés par l'intérêt public (article 8-IV nouveau) et autorisés (articles 25-I et 26-II nouveaux).

Il faut savoir que ces fichiers relatifs aux données sensibles devaient être autorisés par décret après avis conforme de la CNIL et du Conseil d'Etat. La LIL version 2004 indique que l'avis de la CNIL pour ces fichiers sensibles ne liera plus le Conseil d'Etat et le gouvernement. En effet, l'avis de la CNIL n'aura plus besoin d'être « conforme » pour que le décret autorise le fichier sensible ; ce qui traduit un manque de garantie évident lors de l'établissement et l'autorisation de ces fichiers sensibles.

## **. Les fichiers d'infractions et de condamnations**

Seules les juridictions et certaines autorités publiques pouvaient jusqu'à présent constituer de tels fichiers. Mais un amendement initié par Alex Türk permet également aux personnes morales de recourir à ces fichiers d'infractions et de condamnations.

En effet, l'article 9 nouveau, 3° dispose que les traitements de données à caractère personnel relatives aux infractions, condamnations et mesures de sûreté peuvent désormais être mises en œuvre par « les personnes morales victimes d'infractions ou

agissant pour le compte desdites victimes pour les stricts besoins de la prévention et de la lutte contre la fraude ainsi que de la réparation du préjudice subi ». Ce 3° de l'article 9 a été annulé par le Conseil constitutionnel estimant qu'en « raison de l'ampleur que pourraient revêtir les traitements de données personnelles ainsi mis en œuvre et de la nature des informations traitées, cette disposition pourrait affecter le droit au respect de la vie privée et les garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques ». Par ailleurs, le terme de « fraude » a été jugé trop large. Cette disposition était trop imprécise pour être entérinée par le Conseil constitutionnel.

Par contre, le Conseil constitutionnel maintient la disposition 4° de l'article 9 : des fichiers pourront être créés dans une situation précise : la lutte contre le piratage sur Internet.

La LIL prévoit donc la légalisation des « listes noires » constituées notamment par les sociétés de perception de droit d'auteur, les organismes professionnels qui soupçonnent des personnes de piratage sur Internet, via des réseaux peer-to-peer, par exemple.

Ces casiers judiciaires privés devront être autorisés par la CNIL. Il sera nécessaire de contrôler efficacement ces fichiers pour éviter toute dérive.

### **3. Des nouveaux pouvoirs de contrôle et de sanction pour la CNIL**

Avec la nouvelle LIL, la CNIL voit ses pouvoirs de contrôle réduits de manière importante en ce qui concerne les fichiers publics. Néanmoins, la LIL prévoit également la mise en place de nouveaux pouvoirs de contrôle et de sanction pour la CNIL (articles 44 à 49 nouveaux).

Il faut savoir qu'à l'heure actuelle, la CNIL peut enquêter mais ne dispose d'aucun moyen contraignant pour mettre en œuvre ses investigations. Si elle constate la non conformité d'un traitement avec la loi, elle ne peut émettre qu'un avertissement ou transmettre le dossier au Parquet qui se charge de déterminer l'opportunité d'une poursuite.

Avec la LIL version 2004, les pouvoirs de contrôle de la CNIL sont renforcés : en cas d'opposition du propriétaire des lieux, elle pourra désormais, sur autorisation judiciaire, accéder à tout local professionnel et aux matériels qui permettent le traitement des données (article 44 nouveau).

Par ailleurs, outre un possible avertissement (article 45 nouveau), la CNIL pourra mettre en demeure le responsable du traitement de se conformer aux dispositions de la loi sous peine de sanctions administratives et notamment pécuniaires importantes pouvant aller jusqu'à 300 000 euros (article 47 nouveau).

La CNIL sera donc désormais dotée de pouvoirs de contrôle a posteriori effectifs lui permettant de vérifier si les fichiers existants sont conformes aux obligations prévues par la loi. Elle pourra sanctionner la méconnaissance de ces obligations.

Par Me. Murielle-Isabelle Cahen, Avocate .

---

## Propriétés intellectuelles, Propriétés industrielles et commerciales

---

### La marque prend de la bouteille : la protection des formes par le droit des marques -14/09/2004

Par Me. Henri Leben, Avocat à la cour .



*A quelques mois d'intervalle, une décision de la Cour de cassation d'une part, et un arrêt rendu par le Tribunal de Première Instance des Communautés européennes d'autre part, permettent de faire le p...*

▶ A quelques mois d'intervalle, une décision de la Cour de cassation d'une part, et un arrêt rendu par le Tribunal de Première Instance des Communautés européennes d'autre part, permettent de faire le point sur les régimes envisageables pour protéger une forme.

Dans un arrêt du 7 juillet 2004<sup>1</sup>, la chambre commerciale de la Cour de cassation s'est prononcée sur la protection dont peut bénéficier la forme d'une bouteille de champagne. Saisie sur l'application des articles L.511-1 et suivants du Code de la propriété intellectuelle (CPI), la Cour approuve l'analyse des juges du fond ayant prononcé la nullité du dépôt du modèle, au motif que « la forme de bouteille ne porte pas la marque d'un effort créatif, sa forme ne se distinguant de la bouteille champenoise classique que par d'infimes détails ne lui conférant aucun profil original mais s'inscrit au contraire dans la ligne des formes très répandues au XVIIIe siècle ».

Cet arrêt est à rapprocher d'une décision du Tribunal de Première Instance des

Communautés européennes (TPICE) en date du 3 décembre 2003<sup>2</sup> qui, se prononçant également sur la protection applicable au design d'une bouteille, reconnaissait son caractère protégeable non pas sur le fondement des dessins et modèles ou du droit d'auteur, mais sur le fondement du droit des marques.

L'apposition d'une marque peut donc se révéler plus efficace pour protéger une forme que le régime des dessins et modèles, pourtant plus adéquat. Un designer (en l'espèce, le créateur de la forme de la bouteille) dispose ainsi d'une option pour protéger son oeuvre, entre le droit des dessins et modèles et le droit des marques (1). Chacun de ces régimes recouvre cependant une fonction différente (2).

### 1. L'option offerte au créateur de forme

La protection du design d'une bouteille relève naturellement du droit des dessins et modèles. L'article L.511-1 du CPI indique en effet que « peut être protégé à titre de dessin ou modèle l'apparence d'un produit, ou d'une partie de produit, caractérisée en particulier par ses lignes, ses contours, sa forme, sa texture ou ses matériaux (...) ». Au sens de l'article L.511-1 « est regardé comme un produit tout objet industriel ou artisanal, notamment les pièces conçues pour être assemblées en un produit complexe, les emballages, les présentations, les symboles (...) ».

Pour être protégeable, il est cependant nécessaire que le dessin ou modèle soit nouveau et présente un caractère propre (art. L.511-2 CPI). Pour cette raison, les juges du fond, approuvés par la Cour de cassation, ont refusé dans l'espèce commentée, d'accorder la protection des articles L.511-1 et suivants du CPI à la forme de la bouteille de champagne objet du litige, dès lors que celle-ci ne présentait aucun profil original.

L'exigence de la nouveauté ne se retrouve pas, *stricto sensu*, dans la protection par la marque.

L'arrêt du 3 décembre 2003 rendu par le TPICE, a d'abord le mérite de rappeler qu'une forme (en l'espèce, le *design* d'une bouteille) peut être protégée à titre de marque, faisant ainsi application de l'article 4 du règlement (CE) n° 40/94 du 20 décembre 1993 sur la marque communautaire.

L'article 4 précise en effet que : « *peuvent constituer des marques communautaires tous signes susceptibles d'une représentation graphique, notamment les mots, y compris les noms de personnes, les dessins, les lettres, les chiffres, la forme du produit ou de son conditionnement, à condition que de tels signes soient propres à distinguer les produits ou les services d'une entreprise de ceux d'autres entreprises* ».

Cette solution est également transposable au droit français, dont les dispositions indiquent (article L.711-1 c) que peuvent notamment constituer une marque « *les signes figuratifs tels que : dessins, étiquettes, cachets, lisières, reliefs, hologrammes, logos, images de synthèse ; les formes, notamment celles du produit ou de son conditionnement ou celles caractérisant un service ; les dispositions, combinaisons ou nuances de couleurs* ».

L'article L.711-2 c précise néanmoins que « *les signes constitués exclusivement par la forme imposée par la nature ou la fonction du produit, ou conférant à ce dernier sa valeur substantielle* » sont dépourvues de caractère distinctif, et à ce titre, ne peuvent pas être enregistrés comme marque.

Cette restriction est conforme aux dispositions du règlement (CE) n°40/94 qui indique à l'article 7, 1<sup>o</sup>e que « *sont refusés à l'enregistrement les signes constitués exclusivement par la forme imposée par la nature même du produit ou par la forme du produit nécessaire à l'obtention d'un résultat technique ou par la forme qui donne une valeur substantielle au produit* ».

Il s'en suit qu'en droit communautaire, comme en droit français, et sous réserve du respect de certaines conditions, une forme peut être protégée tant sur le fondement du régime des dessins et modèles, que sur celui des marques<sup>3</sup>.

## **2. Le choix du régime de protection dépend de la fonction attachée à la forme**

Le choix du régime de protection dépend de la fonction attachée à la forme. Le *design* d'un objet peut en effet avoir une fonction purement esthétique, constituer un signe de reconnaissance, ou éventuellement, correspondre à des exigences techniques<sup>4</sup>.

L'esthétisme n'est protégé que s'il témoigne d'un effort créateur. On retrouve d'ailleurs la même exigence, que la protection soit envisagée sur le terrain du droit d'auteur ou sur celui des dessins et modèles.

Inversement, la marque ne vient pas récompenser un effort créateur mais garantir l'origine du produit auquel elle s'applique. Une forme utilisée comme marque n'a donc pas à être, en soi, innovante. Le caractère distinctif de la marque ne vient en effet pas tant du signe utilisé, mais de son association à un produit dont elle devient le symbole. Comme le rappelle en ce sens un auteur<sup>5</sup>, la marque est « *un instrument d'individualisation des produits* ».

Pour cette raison, les articles L.711-1 et suivants du CPI n'exigent pas du signe

enregistré comme marque, qu'il soit novateur. Les seules restrictions posées reposent sur l'exigence du caractère distinctif, sur la non contradiction à l'ordre public, et sur le respect des droits détenus par des tiers.

Il n'est donc ainsi pas impossible de protéger un modèle de bouteille datant du XVIIIème siècle par l'enregistrement d'une marque, dès lors que le modèle est tombé dans le domaine public.

Une telle protection n'est cependant envisageable que si, comme le rappelle le TPICE dans son arrêt Nestlé, « *le consommateur moyen est pleinement apte à percevoir la forme de l'emballage des produits concernés comme une indication de l'origine commerciale de ces derniers, pour autant que cette forme présente des caractéristiques suffisantes pour retenir son attention*<sup>6</sup> ».

Autrement dit, n'importe quel modèle n'est pas susceptible d'être protégé par une marque. Le Tribunal précise en ce sens que « *la combinaison confère à la bouteille en cause une apparence qui, compte tenu également du résultat esthétique d'ensemble, est de nature à retenir l'attention du public concerné et à permettre à ce dernier, sensibilisé à la forme de l'emballage des produits en cause, de distinguer les produits visés par la demande d'enregistrement de ceux ayant une autre origine commerciale* »<sup>7</sup>.

Quel que soit le régime envisagé, le titulaire des droits protégeant une forme doit veiller à ce que les conditions de la protection soient réunies. Une protection par dessin et modèle ne peut être envisagée que si la forme est réellement nouvelle. Moins restrictive en apparence, la protection par la marque exige « seulement » que la forme ne soit pas protégée par un droit antérieur. Mais surtout, la forme ne peut être enregistrée comme marque que si elle est distinctive. Le titulaire des droits doit donc être en mesure de faire d'une apparence, le symbole de ses produits. Une telle démarche est loin d'être évidente tant pour des raisons de stratégie commerciale que pour des raisons de coût. La protection des bouteilles par le droit des dessins et modèles a donc encore de beau jour devant elle.

**Par Me. Henri Leben, Avocat à la cour .**

1 Pourvoi n°02-13934, société autonome de verreries c/ société Cave

2 TPICE, 3 décembre 2003, aff. T-305/02 Nestlé Waters France c/OHMI

3 Une protection sur le terrain des brevets peut également être envisagée dès lors que la forme revêt des caractéristiques techniques.

4 Ce dernier aspect n'est pas abordé dans le présent article.

5 Frédéric Pollaud-Dulian, Les marques tridimensionnelles en droit communautaire, RJDA 8-9/03 page 707

6 Point 34 arrêt TPICE 3 décembre 2003, aff. T-305/02 Nestlé Waters France c/OHMI, nous soulignons.

7 Point 41, arrêt précité.

---

## Economie numérique, Droit des contrats

---

### L'impact de la LEN sur la relation client (2) -13/09/2004

*Par Me. Franklin BROUSSE, Avocat, Cabinet FBA .*



**A la définition de commerce électronique, à la présomption de responsabilité du cybermarchand et à l'encadrement de la publicité par voie électronique, il faut ajouter le contrat électronique et l'évolution de la conformité légale et contractuelle de l'activité des marchands en ligne.**

► A la définition de commerce électronique, à la présomption de responsabilité du cybermarchand et à l'encadrement de la publicité par voie électronique, il faut ajouter le contrat électronique et l'évolution de la conformité légale et contractuelle de l'activité des marchands en ligne.

#### **Les contrats sous forme électronique**

Toujours dans le même objectif d'assurer une protection renforcée des consommateurs, la LEN introduit des dispositions spécifiques concernant les contrats conclus à distance sous forme électronique. Tout cyber-marchand a l'obligation de mettre à disposition des consommateurs les conditions contractuelles applicables de manière à ce que ces derniers puisse les conserver et les reproduire.

Le consommateur doit pouvoir bénéficier d'un accès permanent à ces conditions, incluant la possibilité de télécharger et d'imprimer ces conditions. Au-delà du respect des conditions de validité mentionnées dans l'offre, tout cyber-marchand restera engagé par l'offre tant qu'elle sera accessible par voie électronique de son fait. En clair, chaque cyber-marchand devra veiller à une mise à jour attentive des supports de commercialisation de son offre, notamment s'il s'agit d'un site web.

Par ailleurs, chaque cyber-marchand devra respecter un processus spécifique de présentation de l'offre incluant des mentions spécifiques à l'offre en ligne telles que les différentes étapes à suivre pour conclure le contrat, les moyens techniques permettant à l'utilisateur d'identifier les erreurs commises dans la saisie des données et de les corriger avant la conclusion du contrat, le moyen de consulter par voie électronique les règles professionnelles et commerciales auxquelles le cyber-marchand entend, le cas échéant, se soumettre.

Pour que le contrat soit valablement conclu, le consommateur devra avoir eu "la possibilité de vérifier le détail de sa commande et son prix total, et de corriger d'éventuelles erreurs, avant de confirmer celle-ci pour exprimer son acceptation". Le cyber-marchand devra accuser réception sans délai injustifié et par voie électronique de la commande qui lui a été ainsi adressée, comme le font la plupart des sites de commerce électronique à ce jour.

Ces mentions spécifiques ne sont pas nécessaires pour les contrats de fourniture de biens ou de prestation de services conclus exclusivement par échange de courriers électroniques ainsi que pour les contrats conclus en ligne entre professionnels. Enfin, lorsque le contrat est conclu par voie électronique et qu'il porte sur une somme égale ou supérieure à un montant fixé par décret, le cyber- marchand doit assurer la conservation de l'écrit qui le constate pendant un délai qui sera déterminé par ce même décret et en garantir à tout moment l'accès au consommateur si celui-ci en fait la demande.

Par ailleurs, on notera que la LEN a prévu qu'un décret fixerait les obligations d'information et de transmission des conditions contractuelles spécifiques pour les terminaux mobiles, créant ainsi un droit spécifique pour le "m-commerce".

### **Evolution de la conformité légale et contractuelle de l'activité des Cyber-marchands**

Il apparaît manifeste que la LEN entraîne une évolution de la conformité légale et contractuelle des différents types d'activités liées au commerce électronique.

Cette évolution passe notamment par le respect des informations relatives aux communications commerciales (régularisation des process de recueil du consentement préalable des internautes, régularisation/mise à jour de la présentation des offres, vérification des conditions de mise en ligne de l'offre) et par la régularisation des conditions générales de vente en fonction de la volonté des cyber-marchands certains aspects introduits par la LEN dans le périmètre contractuel de leur offre.

Elle relance également l'intérêt de mettre en oeuvre des outils de régulation et de gestion de la relation client tels que les chartes de confiance, de qualité, d'engagements du Cyber- marchand.

En conclusion que, il est recommandé d'intégrer le renforcement de la protection du consommateur dans l'évaluation de la conformité des process de commercialisation existant ou à créer, le cas échéant, en vue de les régulariser et de mieux réguler la relation client.

Par Me. Franklin BROUSSE, Avocat, Cabinet FBA .



---

## Economie numérique, Responsabilité

---

### L'impact de la LEN sur la relation client (1) -04/09/2004

*Par Me. Franklin BROUSSE, Avocat, Cabinet FBA .*



**Définition du terme "commerce électronique", présomption de responsabilité du cyber-marchand, nouvel encadrement de l'e-publicité... autant de thématiques qui prennent une nouvelle dimension avec la LEN. Explications.**

La loi pour la confiance dans l'économie numérique (LEN) du 21 juin dernier est notamment venue compléter l'arsenal juridique régissant les relations entre les cyber-marchands et les internautes. Cela se traduit par l'ajout de nombreuses dispositions au sein de différentes réglementations telles que la loi "Informatique et Libertés", le Code de commerce, le Code de la consommation, le Code des postes et télécommunications, ou le Code civil. La LEN traduit également la prise en compte de la notion de convergence ainsi que des spécificités des différentes formes du commerce électronique. Enfer juridique pour les uns, moteur de confiance et de transparence pour les autres, la LEN a un impact indiscutable sur la "relation client" dans le cadre d'une activité de commerce électronique.

#### **Ce qu'il faut entendre par "commerce électronique"**

La LEN définit pour la première fois en droit français la notion de commerce électronique comme "l'activité économique par laquelle une personne propose ou assure à distance et par voie électronique la fourniture de biens ou de services". Cette activité est définie de manière très large puisqu'elle comprend à la fois les services de fournitures d'informations en ligne, de communications commerciales et les 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.

Au-delà de l'activité de vente de produits ou de services payants en ligne, le commerce électronique couvre donc un panel de services étendu qui touche les services d'information ou de presse en ligne, les services de promotion ou d'annonces publicitaires, ainsi que les moteurs de recherches et la fourniture d'accès à Internet ou d'hébergement de sites web.

#### **Principe de présomption de responsabilité du cyber-marchand**

La LEN introduit le principe d'une présomption de responsabilité du cyber-marchand

selon lequel ce dernier est "responsable de plein droit à l'égard de l'acheteur de la bonne exécution des obligations résultant du contrat, que ces obligations soient à exécuter par elle-même ou par d'autres prestataires de services, sans préjudice de son droit de recours contre ceux-ci".

Le cyber-marchand pourra toutefois exonérer tout ou partie de sa responsabilité s'il apporte la preuve que l'inexécution ou la mauvaise exécution du contrat est imputable à l'acheteur, du fait de sa mauvaise foi, de l'endommagement du produit ou d'une mauvaise utilisation du service.

Il en sera de même s'il démontre qu'elle est imputable au fait d'un tiers étranger à la fourniture des prestations prévues au contrat, tel qu'un intermédiaire technique, ou à un cas de force majeure. Au delà de l'application de ce principe de présomption de responsabilité, la protection des consommateurs se trouve renforcée par la nécessité de respecter un certain nombre d'obligations accrues par rapport à une activité de commerce traditionnelle.

Tout d'abord, la loi offre la faculté à l'Etat de prendre, au cas par cas, des mesures restreignant une activité de commerce électronique, si celle-ci porte notamment atteinte à la sécurité publique, à la protection des mineurs ou à la protection des personnes physiques. Cette faculté devra être prise en compte dans le cadre d'un avertissement contractuel par les cyber-marchands proposant des produits ou des services susceptibles de faire l'objet de telles mesures.

La protection des consommateurs se trouve également renforcée par l'application d'une obligation d'information étendue à la charge des cyber-marchands allant au-delà de l'obligation d'information visée au sein de textes existant. L'objectif est de permettre aux consommateurs d'avoir un accès facile, direct et permanent à des informations précises concernant l'identité du cyber-marchand, les conditions d'exercice de son activité, et les tarifs pratiqués de manière claire et non ambiguë, ce même en l'absence d'offre contractuelle. Le non-respect de cette obligation est sanctionné pénalement.

### **La publicité par voie électronique**

L'obligation d'identification renforcée du cyber-marchand et de ses produits et services se retrouvent au sein des dispositions de la LEN sur la publicité par voie électronique. En effet, la loi prévoit 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". La publicité doit rendre clairement identifiable la société pour le compte de laquelle elle est réalisée, ce qui nécessitera d'être particulièrement attentif pour toutes opérations publicitaires réalisées dans le cadre de co-branding ou de partenariats.

Cette exigence est applicable indépendamment des dispositions réprimant la publicité

trompeuse. De la même manière, la prospection par voie électronique est désormais très encadrée rendant impératif le consentement préalable du consommateur. Ainsi, la prospection directe électronique est interdite lorsqu'elle utilise "les coordonnées d'une personne physique qui n'a pas exprimé son consentement préalable à recevoir des prospections directes par ce moyen".

La prospection directe par courrier électronique est autorisée si les coordonnées du destinataire ont été recueillies directement auprès de lui, à l'occasion d'une vente ou d'une prestation de services concernant des produits ou services analogues à ceux visés par la prospection, sous réserve que le destinataire puisse s'opposer sans frais à l'utilisation de ses coordonnées chaque fois qu'un courrier électronique de prospection lui est adressé.

Dès lors, la prospection sera illicite si :

- elle utilise des coordonnées recueillies sans consentement préalable,
- elle utilise des coordonnées recueillies en dehors du cadre d'une vente ou d'une prestation,
- elle concerne des produits ou services distincts,
- elle est faite par une personne morale distincte
- l'internaute n'est pas informé clairement de son droit de s'opposer sans frais à l'utilisation de ses coordonnées.

Les dispositions relatives à la prospection par voie électronique se retrouvent à la fois au sein du code de la consommation et du code des postes et télécommunications. Compte tenu de l'impact de la nouvelle loi sur les conditions de prospection, des dispositions spécifiques ont été introduites pour permettre de s'assurer que les entreprises intéressées puissent disposer du consentement préalable de leurs prospects et clients dans le cadre d'une période de transition en vue de la régularisation des nombreux fichiers existants.

Ainsi, le consentement des personnes dont les coordonnées ont été recueillies avant le 22 juin 2004, date de publication de la loi, pour des fins de prospection directe pourra être sollicité, par voie de courrier électronique, pendant les six mois suivant cette date. A l'expiration de ce délai, ces personnes seront présumées avoir refusé l'utilisation ultérieure de leurs coordonnées personnelles à fin de prospection directe si elles n'ont pas manifesté expressément leur consentement.

**Par Me. Franklin BROUSSE, Avocat, Cabinet FBA .**

. Consultez le dossier de DROIT-TIC sur la loi sur la confiance dans l'économie numérique.

---

## Informatique et libertés, droit social, droit du travail

---

### Fichiers de police : Lorsque la sécurité nie le droit au travail -02/09/2004

*Par M. Fabrice FEVRIER, Etudiant .*



La loi reste le produit de son temps. C'est en 1995, année de l'attentat dans la station RER Saint-Michel, qu'est donné naissance au Système de Traitement des Infractions Constatées, plus communément appelé le STIC.

#### Ce fichier policie...

► La loi reste le produit de son temps. C'est en 1995, année de l'attentat dans la station RER Saint-Michel, qu'est donné naissance au Système de Traitement des Infractions Constatées, plus communément appelé le STIC.

Ce fichier policier, entièrement informatisé, a pour vocation de répertorier toute personne ayant été concernée de près ou de loin par une procédure judiciaire. Présenté comme un outil indispensable de lutte contre la criminalité, il a vu son contenu s'élargir à chaque événement réclamant le durcissement par le gouvernement de sa politique en matière de sécurité. C'est ainsi que le législateur a considérablement favorisé le développement de ces fichiers par la loi n°2001-1062 sur la sécurité quotidienne de 2001 promulguée quelques semaines après l'attentat du 11 septembre, et par la loi 2003-239 du 18 mars 2003 sur la sécurité intérieure s'inscrivant, quant à elle, dans le prolongement d'une campagne présidentielle centrée sur la hausse inquiétante de la délinquance.

Cependant, l'histoire se répète : chaque fois qu'un Etat fait le choix de privilégier les impératifs de sécurité, ce sont les libertés individuelles et les droits des citoyens qui en pâtissent. Des méfaits d'une politique sécuritaire, le STIC nous en fournit un grand nombre d'exemples : atteintes à la vie privée, à la présomption d'innocence, au droit à l'oubli,... et au droit au travail. Quelques mentions injustifiées, erronées figurant dans le STIC, et le salarié se voit privé d'emploi pour des raisons "opaques" de sécurité publique. Dès lors, les licenciements ou refus d'embauche suite à une enquête administrative défavorable reposant sur la consultation des fichiers de police se multiplient.

Au-delà du secteur public, de nombreux emplois au sein des entreprises privées nécessitent une autorisation, une habilitation ou un agrément de la part des autorités administratives aux fins, par exemple, de posséder un port d'arme ou de se voir autorisé

à pénétrer sur une zone aéroportuaire protégée. Ainsi, en vertu de la loi n°83-269 du 12 juillet 1983, l'accès aux postes de convoyeurs, agent de sécurité RATP, police ferroviaire de la SNCF, est contrôlé par l'autorité préfectorale compétente. L'agent d'entretien dans les zones aéroportuaires réglementées doit lui aussi obtenir ou conserver son autorisation d'accès.

On constate aujourd'hui que le STIC donne lieu à de condamnables dérives résultant de la combinaison malheureuse d'un pouvoir discrétionnaire laissé aux autorités publiques en matière de sécurité, à la gestion défectueuse, voire laxiste, de fichiers contenant des données extrêmement sensibles.

Le danger n'est pas anodin : les fichiers sont de plus en plus nombreux et diversifiés. Le STIC et le JUDEX (version de la gendarmerie) sont les plus connus, mais on peut citer aussi le STIC-Canonge (version photographique), les fichiers des renseignements généraux, de la direction de la surveillance du territoire (DST) ou de la direction générale de la sécurité extérieure (DGSE), le FAED (pour les empreintes digitales), le FNAEG (identification par empreintes génétiques) ou encore le SIS (Système d'information Schengen).

Si les fichiers se multiplient, leur utilisation est également de plus en plus fréquente. Pour exemple, le STIC a fait l'objet de 6.746.000 consultations en 2001 contre seulement 3.919.000 en 1998. Le nombre de saisine de la CNIL montre lui aussi une augmentation forte des demandes de droit d'accès direct puisqu'en 2003, 1163 requêtes ont été reçues contre 243 en 1995.

Avec la mise à contribution de plus en plus fréquente des fichiers policiers, les atteintes aux libertés deviennent légion. Le législateur a créé un instrument qui peut s'avérer dangereux par son utilisation obscure par les autorités publiques et les dysfonctionnements dans sa gestion.

En effet, le STIC comporte tout d'abord un système de collecte de données sensibles qui heurte nombre des principes fondant notre démocratie et notre Etat de droit. Ce fichier policier comporte des informations sur les suspects ou auteurs d'infraction, le mode opératoire des délinquants, ainsi que sur le type d'infraction, le dommage subi et l'identité des victimes. Les informations collectées sont donc très diverses.

Des personnes sont donc fichées alors même qu'elle n'ont pas été poursuivies par le ministère public ou reconnues coupables par les tribunaux, niant ainsi tout droit à la présomption d'innocence. Les mentions présentes ne sont pas alimentées par la justice mais par de simples comptes rendus d'enquête établis par les officiers de police ou gendarmerie de chaque unité se basant sur des « indices graves et concordants rendant vraisemblable la participation d'une personne à une infraction ». Vraisemblable...

La faiblesse du STIC n'est pas seulement présente au stade de son alimentation. Les difficultés persistent lors de son contrôle, de sa gestion dans le temps. En vertu du décret n°2001-583 du 5 juillet 1991, la mise à jour est contrôlée par le Parquet qui se trouve déjà surchargé par de nombreuses autres missions jugées à juste titre prioritaires. C'est ainsi que les erreurs se multiplient : de nombreuses condamnations amnistiées figurent encore dans les fichiers, les faits se trouvent parfois déformés (la perte d'un passeport se transforme en « falsification de documents administratifs »), certaines victimes se trouvent mentionnées en tant qu'auteur...etc. Il est difficilement concevable qu'un fichier aussi dangereux pour les libertés de chaque citoyen fasse l'objet d'une gestion aussi peu fiable...

Enfin, ces bases de données sensibles élaborées par la police font l'objet d'une utilisation très opaque par les autorités publiques qui se refusent de manière générale à communiquer à la personne concernée les motifs de sa décision.

Or, on doit rappeler le principe posé par l'article 2 de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés : « Aucune décision administrative ou privée impliquant une appréciation sur un comportement humain ne peut avoir pour seul fondement un traitement automatisé d'informations donnant une définition du profil ou de la personnalité de l'intéressé ». Le Conseil constitutionnel, dans sa décision du 13 mars 2003 sur les fichiers de la police judiciaire, pressentant les dangers de telles consultations administratives, a précisé clairement « que les données recueillies dans les fichiers ne constitueront donc, dans chaque cas, qu'un élément de la décision prise, sous le contrôle du juge, par l'autorité administrative ».

Face à l'inertie de l'administration et son utilisation controversée des fichiers policiers, que reste-t-il au travailleur licencié ou dans l'impossibilité d'accéder à son nouveau poste suite à une décision administrative négative ?

La patience et la persévérance...

Il doit tout d'abord s'adresser à la CNIL, ainsi qu'au procureur de la République afin de pouvoir accéder aux mentions le concernant et envisager une éventuelle rectification ou suppression de sa fiche. La démarche est longue et fastidieuse, mais semble-t-il incontournable.

Les demandes gracieuses et recours hiérarchiques se heurtant le plus souvent à un nouveau refus, seule la saisine en parallèle de la juridiction administrative aux fins d'obtenir l'annulation de la décision concernée reste envisageable. Même si les tribunaux administratifs ne sont pas toujours enclins à faire droit à de telles demandes, certains magistrats se montrent sensibles à la remise en cause de nos libertés... c'est ainsi que certains salariés ont pu retrouver leur emploi après plusieurs mois de bras de fer avec les

autorités publiques.

Fabrice FEVRIER

*Elève au Centre au Centre Régionale de Formation à la Profession d'Avocat (C.R.F.P.A.)  
de Versailles*

*D.E.A. de droit du travail et droit syndical de Paris X - Nanterre*

**Par M. Fabrice FEVRIER, Etudiant .**

**Pour plus d'informations consultez les travaux de recherche :**

F.FEVRIER, "LE POUVOIR DE CONTRÔLE DE L'EMPLOYEUR ET LES DROITS DES SALARIES À L'HEURE D'INTERNET (LES ENJEUX DE LA CYBERSURVEILLANCE DANS L'ENTREPRISE)", mémoire de DEA de Droit Social et Droit Syndical, Paris X Nanterre, 2003.

W. BAFFARD, "LE SYSTEME DE TRAITEMENT DES INFRACTIONS CONSTATEES (STIC) ET LA PROTECTION DES DONNEES PERSONNELLES", mémoire de DEA, Ecole de Recherche en Informatique et Droit (ERID), Montpellier I, 2004.