
# REVUE D'INFORMATION JURIDIQUE.

Février 2003.

18/02/2003

# Le statut juridique du logiciel libre

Auteur : M. Julien Linsolas , *Juriste Cap Gemini*

Domaine : PROPRIETE_INTELLECTUELLE
Sous thème : Droit_d_auteur

**Déroutant, le logiciel libre reste pour de nombreux juristes un sujet de controverses. Or, loin d'être révolutionnaire son statut juridique pose néanmoins de nombreuses intérrogations.**

L'association pour le développement de l'informatique juridique (L'ADIJ) avait choisi pour son dernier « mardi » en date, le 4 février 2003, le thème suivant : « Le logiciel open source : quel statut juridique ? ». Cet article se fonde et s'inspire librement des interventions de Mme Mélanie Clément-Fontaine et Mme Valérie Sédallian.

Nés il y a près d'un quart de siècle, les logiciels libres ont forgé leur réputation dans la construction des infrastructures du Web (Apache, webmail, php ou encore Samba). Aujourd'hui, le mouvement se « libéralise » et s'étend à des domaines aussi variés que l'administration (avec l'Os Linux) et les arts (l'artistic licence). Les grands constructeurs ne sont plus aussi réticent à proposer des solutions sous logiciels libres à leur clients (IBM, Fujitsu ou Oracle). Plus récemment encore, l'ATICA dans son guide, recommande l'usage de tels produits dans les institutions publiques .

Pour autant le logiciel libre reste un objet juridique mal identifié. A ce titre, il est souvent considéré comme inadapté au droit français. Selon la Free Software Fondation (ou FSF), le logiciel libre se définit comme un logiciel disponible sous forme de code source librement modifiable et adaptable. Ce qui lui confère un particularisme propre dont l'essence est radicalement opposé au modèle propriétaire dans lequel une autorisation préalable est nécessaire. 4 critères fondent cet esprit Lamarckien . Tout d'abord une liberté d'exécuter le programme pour tout usage, ensuite une liberté d'étude et d'adaptation de celui ci, une liberté de diffusion et enfin une liberté de modification et de publication. Cette organisation de la liberté au travers des licences qui régissent le logiciel libre suppose nécessairement une accessibilité totale du code source.

Ce qui fait la force du libre, repose sur le modèle coopératif retenu. En d'autres termes l'existence d'une communauté qui contribue à l'amélioration perpétuelle et continue du logiciel. Ainsi, il est possible de dégager les nombreux avantages qu'offrent le logiciel libre. La disponibilité du code source supprime toute entrave liées aux fournisseurs. Cette indépendance permet dès lors une gestion de la maintenance et du support accrue. En outre le mode coopératif permet une détection et une correction des anomalies plus rapide. Il en résulte des logiciels de meilleure qualité et plus sûr. Les logiciels libres font valoir également un coût de revient moindre des propriétaires.

Non dénué d'inconvénients, le logiciel libre souffre d'un système a priori anarchique. La coopération trouve sa contrepartie dans la multitude et l'abondance des versions laissant alors planer un doute quant à la fiabilité et la pérennité du produit. Cette fragmentation des application peut également entraîner des problèmes de compatibilité. De surcroît,

une garantie n'est pas toujours offerte avec la livraison des codes. A cela s'ajoute une difficulté certaine à déterminer l'auteur de l'œuvre logicielle et une adéquation toute relative avec les principes de bases instaurés par le code de propriété intellectuelle.

Le logiciel libre répond à un nouveau mode d'exploitation. Les outils sont identiques (principe de licence et œuvre logicielle) mais l'exploitation est libre sans réservation du logiciel. La licence n'est là que pour organiser cette liberté et l'accès au code source. Néanmoins, il ne faut pas conclure rapidement à une homogénéité. Il existe en effet une multitude de licences différentes tant sur le fond que sur la forme.

Se pose donc le problème de leur compatibilité entre elles.
Dans la forme, elles se distinguent des classiques par l'absence certaines clauses (telle le droit applicable ou la compétence juridictionnelle) ou la grande importance accordée à d'autre (l'objet ou le préambule). Floues, imprécises parfois incomplètes, les licences libres créent une relative insécurité juridique. Leur besoin de crédibilité passe donc nécessairement par une plus grande rigueur dans le formalisme.

Sur le fond, le seuil de liberté varie en fonction des licences. Là non plus, il n'y pas unicité. Chacune d'elles retranscrit plus ou moins l'esprit de liberté de l'auteur. La GPL est de ce point de vue très claire là où la licence artistique reste vague.

Cette variété devient alors un obstacle à leur compatibilité. Pour l'utilisateur qui souhaite incorporer des codes entre eux, cela soulève quelques difficultés. Deux cas de figure peuvent se présenter : En premier lieu, l'intégration de codes soumis chacun à une licence libre différente. En second lieu, cette intégration peut inclure du code propriétaire. Or, parfois certaines licences posent des restrictions, et une autorisation s'impose. Cette dernière n'étant pas évidente à obtenir, la GNU dresse donc une liste des licences compatibles avec les préceptes qu'elle défend. Autrement dit la sauvegarde du statut libre et le partage .L'utilisateur, à défaut d'un accord, se réfère à cette énumération pour déterminer la compatibilité des licences sous lesquelles il désire divulguer son œuvre. Ce principe à le mérite de la simplicité mais restreint d'autant la liberté des utilisateurs. Ce qui paraît de prime abord antinomique avec l'essence du logiciel libre. Cependant, il s'avère être un procédé efficace contre le parasitisme qui peut résulter de licences antithétiques. Aussi, lorsque qu'une licence propriétaire est en jeu, la GPL pour ne citer qu'elle, interdit toute utilisation au contraire de la licence Netscape qui se révèle plus souple.

Dans la pratique cela se traduit par une diffusion de l'œuvre logicielle sous au moins une double licence. Cela ne signifie pas pour autant qu'il existe un cumul. L'auteur offre au licencié une alternative en fonction de ses besoins propres. Soit 2 licences préexistantes sont proposées soit dans le cas d'une licence entièrement originale, une autre vient y suppléer telle la GPL plus reconnue. L'utilisateur, qui a le choix, sans mixte, peut se prévaloir de l'une comme de l'autre.

Pouvons nous considérer les licences libres comme une négation de la propriété littéraire et artistique ? Cette conclusion est par trop rapide. L'auteur reste maître de ses droits patrimoniaux et moraux. Certes, en matière de logiciel, le législateur a restreint au strict minimum les prérogatives du droit moral. Seul subsiste les droits de divulgation et de paternité. Par ailleurs, leur caractère inaliénable exclut tout abandon par l'auteur. En ce qui concerne les droits patrimoniaux, aux termes de l'article L122-6 CPI l'auteur interdit et autorise à son gré. A ce titre, il n'existe aucune objection à la l'ouverture du code source de son œuvre logicielle. Toutefois, la validité de la licence repose sur le respect du formalisme imposé par l'article L131-3 CPI. A cet égard, la cession d'un droit doit faire l'objet d'une délimitation expresse quant à son étendue, sa destination ou sa durée. Le non respect de ces dispositions est sanctionné par la nullité relative.

La licence GNU, et dans une moindre mesure l'open source, inclut régulièrement des clauses exonératoire de responsabilité. En effet, parce que l'utilisation du logiciel est libre et souvent gratuite, aucune garantie n'est fournie. Les détenteurs des droits sur le logiciel fournissent le programme en l'état, sans aucune sorte de garantie explicite ou implicite. L'utilisateur assume dès lors tous les risques quant à la qualité du produit. La totalité des coûts pour la remise en l'état conforme d'un logiciel défectueux lui incombe. Cette absence garantie a pour conséquence d'exonérer de sa responsabilité l'auteur du fait des dommages liés au dysfonctionnement de son logiciel. Ces dispositions sont donc contraires à la directive européenne du 25 juillet 1985 sur la protection des consommateurs. Toutefois ces licences s'adressent à un public averti et non dénué d'expérience. Un simple avertissement du caractère hautement technique de l'utilisation de ces licences et un encadrement strict des indemnisations envisageables permettraient de remédier au manque de garantie et ne pas tomber ainsi sous le coup de la réglementation sur les clauses abusives.

**Auteur : : M. Julien Linsolas | Source : |**

**NOTES**

http://www.atica.pm.gouv.fr/pages/documents/fiche.php?id=95&id_chapitre=2&id_theme=35&letype=1
Pour parapher E.Moglen in l'anarchisme triomphant, http://emoglen.law.columbia.edu

14/02/2003

# La Commission des Clauses Abusives dénonce les pratiques des FAI

**Auteur : M. Nicolas Samarcq ,** ***Juriste BRM AVOCATS***

Domaine : COMMERCE_ELECTRONIQUE
Sous thème : Protection_du_consommateur

Abstract :
Protection du consommateur - Contrat de fourniture d'accès Internet - Clauses abusives - Modification unilatérale - Conditions subtsancielles - Attribution de compétence - Exclusion de responsabilité -

**Le 31 janvier dernier la Commission des clauses abusives a rendu publique sa recommandation relative aux contrats de fourniture d'accès à l'internet (1) (adoptée le 26 septembre 2002).**

**Selon cette étude, sur l'ensemble des contrats de fourniture d'accès examinés, 28 clauses relatives aux conditions générales d'utilisation pourraient être considérées comme " abusives " au sens de l'article L. 132-1 du Code de la Consommation (2).**

Bien que ce texte ne revêt aucune valeur juridique contraignante, si certaines de ces clauses étaient soumises au pouvoir d'appréciation des juges du fond, elles seraient probablement " réputées non écrites " et par conséquent déclaré nulles.

Il en serait ainsi de la **clause permettant aux fournisseurs d'accès de modifier unilatéralement les conditions générales d'utilisation**, sauf bien entendu dans le cas où cette évolution est favorable au consommateur.

Ainsi, comme le souligne le Forum des droits sur l'internet (3), c'est à juste titre que les juges de la Cour d'Appel de Versailles (4) ont sanctionné le célèbre FAI AOL pour avoir utilisé cette clause au détriment de ses abonnés (5).

A l'époque, le fournisseur avait installé des " *modulateurs de cession* " et des " *timers* " pour couper les connexions de ses abonnés à l'expiration d'une certaine durée afin de récupérer de la bande passante, et ainsi remédier aux avaries techniques qu'il subissait suite au succès de son " *offre de forfait internet illimité (...) à 199 F TCC par mois (...)* (6)".

La Cour, tout en affirmant que la suppression de ces mesures de restriction était indispensable pour permettre l'accès illimité à internet conformément au contrat, a néanmoins infirmé la décision du juge de l'urgence (7) en limitant l'obligation technique de supprimer les " *timers* " (ils peuvent subsister pour les " *périodes d'inaction absolue de l'ordinateur* (8)"), et en réduisant la condamnation d'AOL au paiement d'une indemnité provisionnelle de 15 000 € au profit de Que Choisir.

D'autres clauses non dénoncées devant les tribunaux à ce jour pourraient sans grande difficulté être " réputées non écrites ".

Tel est le cas notamment :

- Des **clauses attributives de compétence territoriale** qui sont prohibées par le Nouveau Code de Procédure Civile lorsque les parties au contrat sont des professionnels et des consommateurs (article 48 du NCPC).

En matière contractuelle le demandeur a en effet la possibilité d'assigner le défendeur soit :

- devant la juridiction du lieu de son domicile,
- devant la juridiction du lieu de livraison effective de la chose,
- devant la juridiction du lieu de l'exécution de la prestation de service.

- Des **clauses prévoyant que les conditions générales en ligne prévalent sur celles imprimées**, ce qui permet aux FAI de modifier unilatéralement leurs conditions générales au détriment du consommateur.

- Des **clauses qui limitent et parfois excluent la responsabilité du fournisseur** " *quant à la perte de données, à l'intégrité des messages déposés dans la boîte aux lettres électronique d'un client, à la défaillance momentanée (…) du réseau appartenant en propre au fournisseur ou, plus largement, à tout dommage subi par le client* ".

• • •

La Commission des Clauses Abusives, à l'instar de sa précédente recommandation relative aux contrats de téléphonie mobile9, recommande donc aux FAI français de supprimer l'ensemble des clauses qu'elle considère comme « abusives ».

Cette recommandation sur la téléphonie mobile, ainsi que quelques décisions de justice, avaient permis aux consommateurs de remettre en cause des abonnements dont les clauses étaient léonines.

Pour les connexions internet, le rééquilibrage au profit des consommateurs ne fait que commencer !

**Auteur :** : **M. Nicolas Samarcq** **| Source :** **www.brmavocats.com** **|**

**NOTES**

1 http://www.clauses-abusives.fr
2 Clauses ayant pour objet ou pour effet de créer, au détriment du non-professionnel ou du consommateur, un déséquilibre significatif entre les droits et obligations des parties au contrat.
3 http://www.foruminternet.org/actualites/lire.phtml?id=495
4 Cour d'Appel de Versailles, 14 ème chambre, 14 mars 2001, SNC AOL Bertelsmann Online France c/ UFC « Que Choisir ».
5 Clause 2 des Conditions Générales d'Utilisation : « AOL se réserve le droit de modifier ou interrompre à tout moment certains aspects du service AOL, y compris des contenus et service ».
6 « en offre standard et 99 F TTC dans le cadre d'une offre promotionnelle exceptionnelle liée à un engagement de 24 mois avec prélèvement automatique.».
7 Tribunal de Grande Instance de Nanterre, ordonnance de référé, 20 février 2001, UFC « Que Choisir » c/ SNC AOL Bertelsmann Online France.

8 « … c'est-à-dire au moment où aucun signal d'entrée ou de sortie de l'ordinateur n'est émis ; ».
9 http://www.clauses-abusives.fr/util/index_recommandations.htm

**LIENS**

http://www.clauses-abusives.fr/util/index_recommandations.htm
http://www.clauses-abusives.fr
http://www.foruminternet.org/actualites/lire.phtml?id=495

11/02/2003

# L'exploitant de site doit protéger l'accès aux données personnelles qu'il collecte

## Auteur : M. Webconseil , *Société de conseil*

**Domaine : INFORMATIQUE_ET_LIBERTES**
**Sous thème : Criminalité_informatique**

**Abstract :**
**Obligation de sécurité - Atteinte à un système automatisé de données par le biais d'un navigateur - Faute (oui) -** Cet article a été lu 89 fois

**Si l'obligation de déclarer les traitements de données personnelles réalisés sur Internet est connu de tous, il en va différemment de l'obligation de protéger l'accès aux données personnelles collectées en ligne.**
**Cette dernière obligation, pourtant extrêmement importante, a été réaffirmée par la Cour d'Appel de Paris dans un arrêt rendu le 30 octobre 2002.**

Dans cette affaire, un particulier avait réussi à accéder au système de traitement automatisé des données d'une grande enseigne d'habillement, grâce à une faille de sécurité dans le serveur de celle-ci.

Le particulier avait été condamné en première instance par le TGI de Paris car selon lui, la faille ne pouvait légitimer ou constituer une excuse pour accéder de manière consciente et délibérée à ces données.

L'internaute condamné décidait de faire appel en soutenant qu'il ne pouvait lui être reproché l'accès au système de traitement automatisé des données via un simple navigateur Internet grand public.

La Cour d'Appel, sur la base de cet argument a reconnu que l'accès à un système de traitement automatisé des données, réalisé grâce à un simple navigateur, retirait tout caractère de confidentialité aux données de l'entreprise.
Elle a surtout précisé que l'entreprise se devait, conformément à la loi, de prendre les mesures nécessaires à l'indication et à la protection de la confidentialité des données collectées sur son site. L'internaute a donc été déclaré non coupable.

Cette affaire permet d'illustrer l'obligation de sécurité des données qui est à la charge de tout responsable de traitement de données, et donc de tout exploitant de site web collectant des données personnelles.

**Auteur :** : **M. Webconseil** **| Source :** **Webconseil** **|**

Pour en savoir plus: contact@webconseil.fr

06/02/2003

# Intrusion dans un système de traitement automatisé de données et aspiration d'un site web : quels enjeux pour le droit ?

**Auteur : Me. Murielle-Isabelle Cahen , *Avocate***

Domaine : COMMERCE_ELECTRONIQUE
Sous thème : Criminalité_informatique

Abstract :
Système informatique - Atteinte / intrusion - Responsabilité pénale / civile - Aspiration de site –

**Si le phénomène du piratage informatique a, d'ores et déjà, fait l'objet d'une intervention législative, conduisant à l'insertion, par le biais de la loi Godfrain du 5 janvier 1988, dans le code pénal des dispositions spécifiques à l'accès et maintien frauduleux dans un système de traitement automatisé de données (art. 323-1 et s. Code pénal), des nouveaux problèmes liés à la technologie de l'information ne cessent d'apparaître.**

C'est le cas, par exemple de la technique dite d'aspiration d'un site web, qui permet à l'internaute de récupérer partiellement ou entièrement le contenu d'une surface interactive et de l'archiver dans le disque dur de son ordinateur, afin de pouvoir y accéder hors connexion.
Les deux techniques -l'intrusion dans un système informatique et l'aspiration de site- présentent des similarités, en ce qui concerne, notamment leur mode d'exécution : des programmes spécifiques, voire des logiciels très élaborés, sont utilisés tant pour accéder dans un système de traitement automatisé de données que pour « aspirer » un site web. Ce fait, pourtant, ne suffit pas pour les assimiler.
En effet, dans le cas de l'accès et maintien frauduleux dans un système informatique, il s'agit bien d'une infraction pénale, qui consiste essentiellement à pénétrer sans droit dans un système en en forçant l'accès. Les dispositions du Code pénal permettent de lutter contre les intrusions frauduleuses (connexion pirate, appel d'un programme ou d'un fichier sans autorisation etc), le maintien frauduleux, l'entrave d'un système ou l'altération de son fonctionnement (virus, mail bombing etc), ainsi que l'altération, la suppression ou l'introduction de données pirates.
En revanche, dans le cas de l'aspiration de site, il s'agit d'une technique non appréhendée par une disposition spécifique de droit. Ceci dit, il pourrait s'agir d'une méthode tout à fait licite. Or, le fait de copier tout ou une partie du contenu d'un site web, afin de pouvoir le visualiser sans être connecté, est susceptible de porter atteinte aux droits d'auteur du créateur dudit site.

## A. L'intrusion dans un système informatique.

Il existe différents types de pirates informatiques : du *hacker* classique, qui s'introduit dans les systèmes par des moyens illégaux sans détruire les données ni utiliser les informations données, mais dans le seul but de faire savoir qu'il existe des failles de sécurité au *cracher* (casseur), appellation qui désigne le pirate le plus dangereux qui détruit dans un but précis ou pour le plaisir. Or, aux yeux de la loi, chacun d'entre eux peut être poursuivi au regard des dispositions du Code pénal en matière de fraude informatique.

L'intrusion peut s'effectuer par le biais d'un programme qui se cache lui-même dans un programme « net » (par exemple reçu dans la boite aux lettres ou téléchargé). L'un des plus connus est le *Back Office* qui permet d'administrer l'ordinateur à distance. En outre, le piratage peut avoir comme cible les mots de passe du système. Dans ce cas là, le pirate utilise souvent des programmes de déchiffrage qui fonctionnent avec des dictionnaires proposant de nombreux mots de passe à des fréquences très élevées (jusqu'à plusieurs milliers de mots de passe par seconde).
Après la prise de contrôle, souvent indécelable, le pirate peut introduire des programmes de corruption (virus, bombe etc), modifier des données (par exemple défigurer une page web), installer des programmes espions (*Sniffer*).
Quelle protection pour les entreprises victimes d'un piratage via réseaux ?

## I. Les actions sur le plan juridique

### a) La responsabilité pénale

La loi Godfrain du 8 janvier 1988, bien qu'élaborée à une époque où on ne parlait pas encore d'Internet et dont les dispositions ont été reprises par le Code pénal dans un chapitre intitulé « *Des atteintes au système de traitement automatisé de données* », permet de sanctionner toutes les intrusions non autorisées dans un système informatique. Les sanctions prévues varient selon que l'intrusion a eu ou non une incidence sur le système en cause.

i. Les intrusions simples
L'article L.323-1 du Nouveau code pénal prévoit que « le *fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni d'un an d'emprisonnement et de 15 000 euros d'amende* ». Ces systèmes comprennent, entre autre, les sites web.

Accès frauduleux
La Cour d'appel de Paris a considéré dans un arrêt du 5 avril 1994 (1) que « *l'accès frauduleux, au sens de la loi, vise tous les modes de pénétration irréguliers d'un système de traitement automatisé de données, que l'accédant travaille déjà sur la même machine mais à un autre système, qu'il procède à distance ou qu'il se branche sur une ligne de communication* ».
*Quid*, pourtant, si le système n'est pas protégé ? La Cour d'appel de Paris, dans un arrêt en date du 30 octobre 2002 (2) , a jugé que la possibilité d'accéder à des données stockées sur un site avec un simple navigateur, en présence de nombreuses failles de sécurité, n'est pas répréhensible. Elle a, ainsi, reformé le jugement du Tribunal de grande instance de Paris, qui avait estimait que l'existence des failles de sécurité ne constituait « *en aucun cas une excuse ou un prétexte pour le prévenu d'accéder de manière consciente et délibérée à des données dont la non-protection pouvait être constitutive d'une infraction pénale* » (3). En effet, l'article 226-17 du Code Pénal réprime le fait de procéder ou de faire procéder à un traitement automatisé d'informations nominatives sans prendre toutes les précautions utiles pour préserver la sécurité de ces informations et notamment d'empêcher qu'elles ne soient communiquées à des tiers non-autorisés.

Le maintien frauduleux
La loi incrimine également le maintien frauduleux ou irrégulier dans un système de traitement automatisé de données de la part de celui qui y est entré par inadvertance ou de la part de celui qui, y ayant régulièrement pénétré, se serait maintenu frauduleusement ( Cour d'appel de Paris, jugement du 5 avril 1994 précité).

Quant à l'élément intentionnel de cette infraction, la doctrine et la jurisprudence s'accordent à admettre que l'adverbe « *frauduleusement* » n'est pas le dol général de l'attitude volontaire, ni le dol très spécial de l'intention de nuire, mais la conscience chez le délinquant que l'accès ou le maintien ne lui était pas autorisé.

ii. Les intrusions avec dommages

L'alinéa 2 de l'article 323-1 du nouveau Code pénal prévoit un renforcement des sanctions, lorsque l'intrusion et le maintien frauduleux ont certaines conséquences :

*« Lorsqu'il en résulte soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de deux ans d'emprisonnement et de 30 000 euros d'amende»*

Ne sont concernées par cet article que les altérations involontaires. L'entrave volontaire au système ou l'entrave volontaire aux données sont visés par les articles 323-2 et 323-3 du nouveau Code pénal.

iii. Les entraves volontaires au système ou aux données s'y trouvant.

L'article 323-2 du Nouveau Code pénal définit l'entrave volontaire au système comme « *Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données* ». Le peine encourue est de trois ans d'emprisonnement et de 45.000 euros d'amende. Cette infraction vise, notamment, l'introduction des programmes susceptibles d'entraîner une perturbation au système, tels que les virus, les bombes logiques etc.

L'article 323-3 du Nouveau Code pénal sanctionne, par ailleurs, l'introduction, la suppression ou la modification frauduleuses de données dans un système informatique. Les applications illicites visées par cet article sont nombreuses. Elles peuvent aller de la réduction du prix des marchandises sur un site de commerce électronique, la modification ou la suppression du contenu des bases de données à la modification du statut fiscal de l'entreprise.

En tout cas, ces agissements sont susceptibles d'entraîner une perte financière considérable au sein de l'entreprise.

**b. La responsabilité civile délictuelle.**

Le droit commun de la responsabilité civile délictuelle est fondé sur la nation de la faute au sens de l'article 1382 du Code civil. Elle nécessite une faute, un dommage et un lien de causalité entre les deux. La faute consiste ici en une intrusion dans un système informatique à l'insu de son utilisateur. Quant au dommage, il faut savoir s'il y a eu une perte et/ou une altération des informations contenues dans le site ou si le pirate a communiqué les données personnelles s'y trouvant à des tiers. Enfin, le lien de causalité entre la faute et le dommage doit être clairement établi.

*Quid*, pourtant, si le pirate n'est pas de nationalité française ou s'il opère de l'étranger ? La question qui se pose, dans ce cas, est celle de la compétence judiciaire internationale et de la loi applicable.

En droit français, le tribunal compétent pour juger un litige international est, en principe, celui du domicile du défendeur, à moins que le demandeur, s'il est français, ne souhaite invoquer le privilège de juridiction des articles 14 et 15 du Code civil. Or, ce dernier privilège est interdit dans le cadre de la Communauté européenne par la Convention de Bruxelles de 1973, devenue en 2000 un règlement « concernant la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale ».

S'agissant d'un délit ou d'un quasi-délit, les articles 5§3 de la Convention de Bruxelles et du règlement 44/2001 précité, posent une règle de compétence spéciale en faveur du tribunal où le fait dommageable s'est produit ou risque de se produire. Ce lieu peut être aussi bien celui où le dommage est survenu qui celui de l'événement causal qui est à l'origine de ce dommage (CJCE, 30 novembre 1976, aff. C-21/76, *Mines de potasse d'Alsace* : Rec. CJCE, p. 1735).

Dans le cas où le dommage, causé par l'intrusion, serait survenu au sein du système informatique d'une société domiciliée en France, les juridictions françaises seraient sans doute compétentes pour juger le litige.

Quant à la loi applicable, le juge applique, de manière générale la *lex loci delicti*, c'est à dire la loi où le fait dommageable s'est produit. La Cour de Cassation a jugé que le lieu

où le fait dommageable s'est produit *s'entend aussi bien de celui du fait générateur du dommage que du lieu de réalisation de ce dernier* (Cass. 1re civ., 14 janvier 1997, D. 1997, p.177).

**c. La responsabilité civile contractuelle.**

Il est possible, en effet, d'engager la responsabilité civile contractuelle de l'héberger du site. Pour cela, il faudrait examiner les clauses contenues dans le contrat d'hébergement concernant notamment la sécurité du site et la mise en place de systèmes informatiques de protection contre toute forme d'intrusion. Il faudrait aussi qualifier cette obligation de l'héberger : s'agit-il d'une obligation de résultat ou de moyens ? Dans la plus part de cas, il ne pourra s'agir que d'une obligation de moyens qui aura pour effet de contraindre le prestataire d'apporter la preuve qu'il n'a pas manqué aux obligations normales qui lui incombaient, en cas d'intrusion informatique non autorisée.

**II. Les mesures préventives**

Certes, la possibilité d'intenter une action a posteriori contre le responsable de l'intrusion existe. Est-ce, pourtant, une solution efficace ?

Sur le plan juridique, la difficulté réside sur l'administration de la preuve, d'autant plus si l'intrusion a été effectuée à partir d'un réseau ouvert de type Internet. En effet, même si l'origine de cette intrusion peut être détectée, l'identification de la personne qui se cache derrière celle-ci peut s'avérer extrêmement difficile. Or, l'étendue les dommages susceptibles d'être causés tant aux systèmes d'information attaqués et, par voie de conséquence, à l'entreprise qui les gère qu'à la crédibilité de cette dernière sur le plan professionnel, impose que des mesures de précaution soient prises.

En premier lieu, il est important d'insérer dans tous les contrats techniques une clause concernant la sécurité du contenu du système en cause, sous le double angle de la sécurité physique et logique. Dans le premier cas, il s'agira de déterminer les conditions d'accès au serveur en tant que matériel informatique (contrôle des personnes ayant accès dans l'espace où sera localisé le serveur, conditions d'intervention en cas de panne etc). Dans l'hypothèse de la sécurité logique, le prestataire devra assurer la mise en place de systèmes informatiques de protection conformes aux technologies disponibles (sécurité logicielle, fire wall, anti-virus etc). A cet effet, une des solutions les plus efficaces consiste à isoler l'ordinateur connecté à l'Internet, afin d'empêcher les utilisateurs de s'en servir pour naviguer sur l'ensemble du système informatique. Les systèmes de signature électronique et de cryptologie permettent également d'assurer la sécurité des échanges.

Par ailleurs, on peut imaginer qu'une entreprise puisse souscrire une assurance contre le risque d'attaque informatique. Dans ce cas précis, le dédommagement dépendra du type d'assurance souscrite.

**B. L'aspiration de site**

La technique d'aspiration de site consiste, comme on l'a déjà précisé, à copier, partiellement ou entièrement le contenu d'un site, ainsi que des pages liées, sur le disque dur de l'ordinateur de l'utilisateur, afin de pouvoir y accéder hors connexion. Le site ainsi " aspiré " s'ouvre comme n'importe quel fichier sans attente ni risque de coupure de la connexion.

Il existe, en effet, des logiciels, tel que Mémoweb, qui permettent de récupérer les images, les sons, de préserver les liens entre les pages, et offrent de multiples capacités de traitement supplémentaires (mise à jour automatique des sites et des changements éventuels, comparaison périodique de pages…).

Il est vrai que l'aspiration des sites a suscité des multiples interrogations quant à sa légitimité face au droit d'auteur. D'autant plus que, comme on va le voir par la suite, les réponses données par l'application du droit de la propriété intellectuelle peuvent varier selon la catégorie à la quelle l'œuvre en cause s'attache.

**I. L'aspiration de site face aux droits de propriété intellectuelle**

a. La protection des droits d'auteur du créateur du site

L'auteur d'un œuvre bénéficie d'une protection élevée en France et en Europe en application des droits qui lui sont conférés par le CPI, ainsi que par la directive CE 2001/29 du 22 mai 2001 sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information.
La jurisprudence française considère, depuis un jugement du Tribunal de commerce de Paris du 9 février 1998, que le contenu des pages web est protégeable au titre des droits d'auteurs. Pour cela, il faut que les critères posés par le CPI – création originale, fixée sur un support- soient remplis. Ainsi, l'art. L.122-4 du CPI dispose que « *Toute représentation ou reproduction intégrale ou partielle faite sans le consentement de l'auteur ou de ses ayants droits au ayants cause est illicite* » et elle est donc punie à titre de contrefaçon.
Or, l'interdiction de la reproduction intégrale ou partielle de l'œuvre, faite sans le consentement de son auteur ne comprend pas, selon l'article 122-5 2° du CPI, « *les copies ou reproductions strictement réservées à l'usage privé du copiste et non destinées à une utilisation collective* ».
Ceci dit, l'aspiration d'un site peut parfaitement être considérée comme l'exercice par l'utilisateur de son droit de copie privée d'une œuvre déjà divulguée. En d'autres termes, la légitimité de la technique d'aspiration d'un site, face au droit d'auteur qu'on présume applicable, dépend, comme c'est le cas pour tous les œuvres de l'esprit bénéficiant de la protection par ce dernier, de l'utilisation qu'en est faite. Ainsi, la projection d'un site aspiré devant un publique serait, sans doute, considérée comme une utilisation collective de l'œuvre et serait, donc, interdite, à moins que le titulaire des droits n'ait pas donné préalablement son accord.

**b. La protection des bases de données**

Selon l'article L.341-1 du CPI « *Le producteur d'une base de données, entendu comme la personne qui prend l'initiative et assure le risque des investissements correspondants, bénéficie d'une protection du contenu de la base lorsque la constitution, la vérification ou la présentation de celui-ci atteste d'un investissement financier, matériel ou humain, substantiel. Cette protection est indépendante et s'exerce sans préjudice de cesses résultant du droit d'auteur ou d'un autre droit sur la base de données ou un de ses éléments constitutifs* ».
Le producteur d'une base de données a le droit d'interdire l'extraction, par transfert permanent ou temporaire, de la totalité ou d'une partie qualitativement ou quantitativement substantielle du contenu d'une base de données sur un autre support, ainsi que la réutilisation, par la mise à la disposition du public de ceci (art. L. 342-1 CPI).
L'article 122-4 du CPI exclue le droit de copie privée pour les « *copies et reproductions d'une base de données électronique* ».
Il reste à savoir ce qu'on l'en entend comme base de données. A cet égard, l'article L. 112-3 du CPI dispose qu' « *on entend par base de données un recueil d'œuvres, de données ou d'autres éléments indépendants, disposés de manière systématique ou méthodique, et individuellement accessibles par des moyens électroniques ou par tout moyen* ».
Or, si certains sites web peuvent être considérés comme des bases de données, la majorité d'entre eux ne le sont pas. La raison est qu'ils ne répondent pas à la définition de « recueil d'œuvres, de données ou d'autres éléments indépendants, disposés de manière systématique ou méthodique ».
En effet, si un site de compilation de données (un annuaire en ligne par exemple ou un site portail) constitue certainement une base de données, un site classique (site commercial) ne semble pas pour autant pouvoir revêtir cette qualification ; dans le cas de ce dernier, l'assemblage d'images, de sons et de textes n'a rien ni d'une disposition systématique, ni d'un recueil de données.

Qu'en est-il, pourtant, des sites commerciaux qui constituent et mettent à jour en permanence des bases des données sur leurs clients ou des sites qui proposent des modes de recherche, nécessitant le passage par une ou plusieurs bases de données ? Dans ces cas très fréquents, il faut considérer que l'objet de la protection c'est non pas le site entier, qui ne présente, par ailleurs, aucune structure systématique et méthodique, mais seulement la base elle-même. Cette dernière, d'ailleurs, n'est pas visible pas les internautes et par conséquent elle ne peut pas être aspirée. L'accès à une telle base constituerait l'infraction, décrite ci-dessus, d'accès et maintien dans un système de traitement automatisé de données.

## II. L'aspiration d'un site peut-elle être considérée comme une intrusion dans un système informatique ?

Pour que l'aspiration d'un site puisse être sanctionnée au titre de l'article 323-1 du Code pénal, il faut, avant tout, qu'il y ait eu intrusion dans un système informatique au sens de ce même article. Or, il n'y a intrusion que si la pénétration dans le système informatique en cause a été **effectuée de manière irrégulière par une personne non-autorisée**. Comme le montre la décision récente de la Cour d'appel de Paris précitée (4), il ne suffit pas que la personne acteur de l'intrusion n'avait pas le droit d'accès dans le système, mais encore faut-il qu'il en ait forcé l'accès, en utilisant une méthode particulière et non pas un simple navigateur.
L'aspiration d'un site s'effectue bien sur avec des logiciels spéciaux. En plus, dans la plus part de cas, l'utilisateur ne demande pas l'autorisation préalable du créateur du site. Or, l'accès à ce dernier n'est nullement forcé!

Enfin, si des dégâts au contenu ou au système du site ont été causés, le préjudice pourra être réparé sur le fondement de la responsabilité civile délictuelle, à la condition, toutefois, de rapporter la preuve du lien de causalité entre l'aspiration et le dommage.

L'aspiration d'un site n'est rien d'autre qu'un téléchargement simultané de tous les éléments d'une page ou d'un site web. Mis à part l'hypothèse où le site puisse être considéré en lui-même comme une base de données et supposant que l'accès à celui-ci est libre, rien a priori ne semble s'opposer à son aspiration pour des fins privés.

**Auteur :** : **Me. Murielle-Isabelle Cahen** **| Source :** **www.murielle-cahen.com** **|**

**NOTES**

(1) CA Paris, 5 avril 1994, D. 1994, IR, p. 130.
(2) Affaire Tati c/ Kiketoa, décision disponible sur le site www.juriscom.net
(3) Décision disponible sur le site www.juriscom.net .
(4) Voy. supra page 2

**LIENS**
http://www.murielle-cahen.com
http://www.juriscom.net