« Le livre magistral de Maître Sédallian est le démenti le plus vif à la rumeur selon laquelle l'Internet aurait ouvert une brèche de non-droit qu'il conviendrait de combler.

L'auteur identifie de manière complète et traite avec minutie toutes les zones du droit, y compris les niches, touchées par l'Internet.

Ainsi, au fil d'une lecture agréable, les pièces d'un gigantesque puzzle juridique s'assemblent pour faire apparaître l'image de l'Internet.

L'ouvrage fourmille d'informations pratiques, de jurisprudences récentes…

Le juriste, averti ou profane, y puisera les réponses introuvables ailleurs.

Il y découvrira un droit horizontal, transversal, mobilisant un réseau de règles sur lesquelles on navigue avec bonheur.

Ce livre se lit comme un roman et c'est bien la force de cette œuvre : les questions juridiques, y compris les plus complexes, trouvent leurs solutions de manière simple – quasi naturelle – pour aboutir au constat que l'Internet est bien saisi par le droit. »

Alain Weber
Avocat, président de la Commission informatique et libertés
de la Ligue des droits de l'homme

Valérie Sédallian
avocat à la Cour d'appel de Paris

Droit de l'Internet

Réglementation

Responsabilités

Contrats

Collection AUI
Association des Utilisateurs d'Internet

Collection AUI
Association des Utilisateurs d'Internet

La collection AUI est née en 1996. Elle vise à promouvoir par le livre les objectifs poursuivis par l'Association des Utilisateurs d'Internet, qui oeuvre à la démocratisation et au développement d'Internet.

Sans pour autant représenter uniquement les vues de l'AUI, cette collection propose des ouvrages de qualité traitant de tous les aspects d'Internet, notamment techniques, sociologiques, et juridiques.

La formation et l'éducation des utilisateurs sont les préalables nécessaires au développement d'Internet dans les meilleures conditions. Internet prend de plus en plus de place dans notre quotidien, dans notre vie sociale ou professionnelle : le but de l'AUI et de cette collection est de contribuer à ce que son utilisation devienne un outil de citoyenneté à la portée de tous.

Avant-propos

Cet ouvrage inaugure la collection dirigée par l'AUI, et publiée par les éditions Net Press.

J'ai d'autant plus de plaisir à écrire ces lignes qu'elles constituent un avant-propos au texte de Valérie Sédallian, avocate au barreau de Paris. Valérie est membre de l'AUI depuis sa création, et aapporté une contribution essentielle aux actions menées par l'AUI jusqu'à ce jour.

Cet ouvrage met l'accent sur les questions nouvelles posées par Internet du point de vue de la législation. Il analyse avec rigueur et sans concession les problèmes posés, et permet d'y répondre en tout sérénité.

L'AUI a beaucoup oeuvré depuis le début de l'année 1996 afin de démystifier Internet, et de lutter contre le catastrophisme des tenants du « vide juridique » et autres billevesées. Valérie Sédallian fait ici le point de la situation, s'adressant aux professionnels, tout en s'exprimant de façon suffisamment pédagogique pour que chacun puisse trouver dans cet ouvrage réponse à ses questions et matière à réflexion.

Le 4 novembre 1996

Meryem Marzouki
présidente de l'AUI

Introduction
Présentation de l'Internet

Une bonne compréhension de ce qu'est l'Internet, de son fonctionnement, des services et des informations que l'on y trouve, de la manière dont on communique et diffuse de l'information est nécessaire pour appréhender les questions juridiques soulevées dans cet ouvrage[1].

Fonctionnement

L'infrastructure Internet ne peut être assimilée à d'autres infrastructures déjà existantes, et notamment au réseau Télétel : il ne s'agit pas en effet d'un réseau unique, mais de l'interconnexion d'une multitude de réseaux informatiques. Un réseau informatique est connecté à un deuxième réseau informatique, lui-même connecté à un troisième réseau informatique, lui-même connecté à un quatrième réseau, et ainsi de suite, d'une manière telle que chaque ordinateur d'un des réseaux peut communiquer avec n'importe quel ordinateur appartenant à un autre des réseaux.

Cet ensemble de réseaux constitue l'Internet. Cette interconnexion généralisée des réseaux est rendue possible par l'utilisation d'un protocole de communication commun dit TCP/IP.

Il est difficile d'évaluer avec exactitude la taille de l'Internet à un moment donné. On peut constater néanmoins son extraordinaire croissance en quelques années. En 1981, moins de 300 000 ordinateurs étaient reliés à l'Internet. En 1993, on en dénombrait plus de 1 million et plus de 12 millions en juillet 1996[2].

Début 1996, on évaluait à environ 40 millions le nombre de gens à travers le monde ayant un accès à l'Internet, répartis dans 170 pays, et plus de 200 millions de personnes devraient disposer d'un accès en l'an 2000.

---

[1] Cette présentation s'inspire du rapport élaboré par l'Association des utilisateurs d'Internet "Pour une intégration sereine et un développement harmonieux d'Internet dans la société française", disponible à : <http://www.aui.fr/Rapports/RAUI-070696.html>, 7 juin 1996, ainsi que du "Findings of facts" de la décision d'un tribunal américain sur la constitutionnalité du Communication Decency Act visant à réglementer la pornographie sur l'Internet : ACLU v. Reno, United States District Court for the Eastern District of Pensylvania, 11 juin 1996, 929 F. Supp. 824 (E.D. Pa. 1996), disponible à : <http://www.aclu.org/issues/cyber/trial.htm>.

[2] La société Network Wizard fournit des statistiques sur la croissance de l'Internet sous : <http://www.nw.com>.

Toutefois, les personnes bénéficiant d'un accès à l'Internet se trouvent principalement dans les pays riches. Ces derniers possèdent en effet les trois quarts des lignes téléphoniques nécessaires pour accéder à l'Internet. En 1995, plus de la moitié de la planète ne s'était jamais servi d'un téléphone, et dans 47 pays, il n'y avait même pas une ligne pour 100 habitants[3].

Né en 1969, d'un projet expérimental de l'armée et de la recherche américaine appelé ARPANET, le système a été conçu afin de permettre la communication des données, même si une partie du réseau informatique venait à être inutilisable. Cela est une spécificité fondamentale de l'Internet. Elle a pour corollaire qu'il s'agit d'une architecture distribuée et non hiérarchique, et que le maillage de l'Internet est tel qu'il n'est pas possible de déterminer *a priori* le chemin que suivront les données pour être acheminées d'un point à un autre.

La suppression d'un ordinateur du réseau, ou la fermeture de son accès n'a pas forcément d'influence sur les autres ordinateurs, ceux-ci pouvant toujours communiquer par « reroutage » des données qui emprunteront un chemin différent.

Comment accéder à l'Internet ?

On accède à l'Internet soit par un ordinateur relié de manière permanente à un réseau lui-même relié à l'Internet, soit en se connectant depuis son ordinateur personnel par le biais d'un modem auprès d'un réseau relié à l'Internet. Dans les deux cas, le réseau peut être relié directement ou indirectement à l'Internet.

La personne qui fournit cet accès direct ou indirect au réseau Internet à un utilisateur est un fournisseur d'accès Internet, ou Internet Access Provider en anglais.

Les fournisseurs d'accès ne constituent pas une catégorie homogène, mais ont des statuts très variables selon la nature du contrat qui les lie à l'utilisateur. Le fournisseur d'accès n'est en effet pas nécessairement une société qui commercialise des accès Internet.

On peut regrouper les fournisseurs d'accès en cinq catégories. Ces catégories ne sont elles-mêmes pas exhaustives de la manière dont on peut accéder à l'Internet, puisque des accès Internet sont également offerts par des cafés-restaurants, appelés cybercafés, ou par des bibliothèques, et peuvent être installés dans d'autres lieux ouverts au public.

Le fournisseur d'accès commercial

Un utilisateur, entreprise ou particulier, peut accéder à l'Internet en s'abonnant auprès d'un fournisseur d'accès dont l'activité est de fournir de telles connexions au public contre rémunération.

On peut ranger dans cette catégorie les fournisseurs de services en ligne comme Compuserve ou AOL (America On Line). Ces fournisseurs de services ont leur propre réseau privé sur lesquels ils fournissent du contenu à leurs abonnés. Compte tenu du succès de l'Internet, tous fournissent également à leurs clients un accès à l'Internet.

Les relations entre le fournisseur d'accès et l'utilisateur sont régies par un contrat de droit privé précisant les services fournis, leur coût, et les droits et obligations des parties.

---

[3] Dan Schiller, « Les marchands du cyberespace », *le Monde diplomatique,* mai 1996, pp.15 et 20.

Le fournisseur d'accès employeur

Il fournit des accès à ses employés à des fins professionnelles. Il peut avoir un abonnement auprès d'un fournisseur d'accès commercial ou disposer de sa propre infrastructure de connexion à l'Internet.

Les conditions d'utilisation des services Internet par les employés relèveront du contrat de travail, des conventions collectives, du règlement intérieur. L'accès à l'Internet est un outil de travail. L'employeur peut être une personne de droit privé ou public.

Le fournisseur d'accès école ou université

Les étudiants, lycéens, écoliers, enseignants et chercheurs des établissements d'enseignement peuvent disposer d'un accès à l'Internet par l'intermédiaire de leur université ou de leur école.

L'accès à l'Internet fait partie des moyens mis à la disposition des élèves, étudiants, enseignants et chercheurs pour l'enseignement et la recherche.

Le fournisseur d'accès associatif

Il fournit des accès à ses adhérents. La fourniture de l'accès peut être l'objet même de l'association, ou un service annexe fourni par l'association.

Le fournisseur d'accès individuel

Il n'a pas pour activité de fournir des accès au public mais, disposant lui-même d'un accès permanent, il peut à son tour fournir un accès à qui bon lui semble, dans la mesure de ses moyens et de l'infrastructure dont il dispose.

Le fournisseur d'accès, quelle que soit sa catégorie, fournit à l'utilisateur final un accès à l'infrastructure Internet, ainsi que les moyens matériels et techniques de bénéficier des services s'appuyant sur cette infrastructure.

L'utilisateur ne paie pas nécessairement son accès à l'Internet et ses connexions. Ce sera notamment le cas de l'utilisateur qui accède à l'Internet par son employeur ou par son université.

En plus de l'abonnement éventuellement versé à un fournisseur d'accès, le coût de la connexion à l'Internet dépend du mode d'accès utilisé. Si l'accès est permanent, ce coût est en principe forfaitaire, quelle que soit la durée de la connexion[4]. Si l'accès est fait par modem, le coût de la connexion est égal au coût de la connexion entre l'installation téléphonique de l'utilisateur et celle de son fournisseur d'accès (en principe le coût d'une communication téléphonique locale), quel que soit le service utilisé. Il coûte aussi cher d'envoyer un courrier électronique à un destinataire situé à 100 mètres ou à plusieurs milliers de kilomètres, que de se connecter à un site localisé à Los Angeles ou à Paris.

[4] Il existe cependant des exceptions à ce principe, car il s'agit d'un choix du fournisseur. Par exemple, EuNet facture au volume. Site Web : <http://www.eunet.fr>.

Services

L'Internet est constitué de différentes méthodes de communication. Ces méthodes sont en constante évolution. Par exemple, le World Wide Web, l'une des applications les plus populaires aujourd'hui n'est apparu qu'en 1992-93. Il ne fait pas de doutes que l'avenir verra de nouveaux services, peut-être encore insoupçonnés actuellement, conçus en fonction de la créativité des utilisateurs ainsi que de l'évolution des besoins et de la technologie.

Le terme service s'entend ici comme un « service automatique de transmission de l'information utilisant un protocole donné » et non pas comme un service de fourniture de contenu.

J'ai choisi de classer ces services en 4 catégories :

- les échanges personnels en temps différé ;
- les discussions publiques ;
- les services d'information ;
- les échanges en temps réel.

Ces catégories ne sont pas cloisonnées : les discussions publiques peuvent avoir lieu en temps réel ou en temps différé.

Les échanges personnels en temps différé

Il s'agit du courrier électronique ou e-mail. Le principe du courrier électronique est similaire à celui du courrier postal. Chaque usager dispose d'une boîte aux lettres électronique et d'une adresse qui l'individualise sur l'Internet. Un message qui n'a pas besoin d'être édité sur papier comme dans le cas de la télécopie est envoyé par son expéditeur à un ou à plusieurs destinataires identifiés par leur adresse électronique. Pour que le destinataire puisse lire le message, il suffit qu'il se connecte et relève sa boîte aux lettres.

Un courrier électronique met en général de quelques minutes à quelques secondes pour arriver à destination. L'échange s'effectue en temps différé et non en direct : le destinataire doit « relever son courrier », c'est-à-dire consulter sa boîte aux lettres pour prendre connaissance des messages reçus.

Les discussions publiques

Sur l'Internet, on peut communiquer de manière privée, par exemple grâce au courrier électronique, ou de manière publique : le nombre de personnes qui vont prendre connaissance d'un message particulier posté par une personne est indéterminé.

Les forums de discussion ou forums de nouvelles ou newsgroups ou Usenet

Usenet est un espace de discussion, une gigantesque base de données de messages organisée par centres d'intérêt. Les messages postés dans un forum particulier sont accessibles librement par toute personne choisissant de lire ledit message. Il existe quelques newsgroups

modérés, c'est-à-dire que tous les messages postés à destination d'un groupe transiteront par une même personne, qui vérifie que les messages sont bien en rapport avec le thème du forum. La grande majorité des newsgroups n'est pas modérée, et personne ne peut garantir que le contenu de l'article correspond à la thématique du groupe. Pour lire et écrire dans les newsgroups, l'usager doit se connecter à un serveur de news, en principe celui de son fournisseur d'accès, mais certains serveurs de news sont accessibles librement, en écriture et/ou en lecture[5].

Chaque administrateur d'un serveur de news choisit les forums qu'il décide de mettre à la disposition de ses utilisateurs, en lecture et en écriture, mais une fois qu'il a décidé d'accepter un forum particulier, le processus de diffusion et de transmission des messages postés dans les forums est automatique : chaque serveur distribue les contributions de ses utilisateurs à d'autres serveurs Usenet et reçoit en retour les articles postés par les utilisateurs des autres serveurs et ainsi de suite.

Les messages sont ainsi relayés mécaniquement de serveur en serveur, sans intervention humaine.

Le trafic généré par Usenet est très important : le nombre de serveurs Usenet est évalué à 200 000 à travers le monde, le nombre de messages à plusieurs centaines de milliers et le nombre de forums existant à 17 000.

A titre d'exemple, les forums en français (titres débutant par <.fr>) sont diffusés dans les pays francophones, mais également sur des serveurs américains et même sur le serveur de l'université de Tokyo.

La création d'un nouveau forum fait l'objet d'une procédure spécifique avec discussion sur l'opportunité de créer un nouveau groupe et vote des utilisateurs.

Font exception à cette règle les forums de la hiérarchie <alt.> (pour alternative). C'est dans cette hiérarchie que se trouvent d'ailleurs les newsgroups les plus controversés.

Enfin, les messages des newsgroups sont archivés sur certains sites, librement accessibles, comme Dejanews[6] ou Altavista[7].

Les listes de diffusion

Comme les newsgroups, les listes de diffusion ou mailing lists permettent à un groupe de personnes de discuter par thèmes d'affinité. A la différence des forums de discussion, il est nécessaire de s'abonner préalablement à la liste de diffusion, par courrier électronique. Chaque message posté est alors envoyé, soit automatiquement, par le serveur de liste, soit par l'intermédiaire d'un modérateur à tous les abonnés de la liste, qui reçoivent directement les messages dans leur boîte aux lettres.

La participation à un serveur de liste peut être ouverte (l'abonnement est ouvert à tous) ou fermée, l'accès étant réservé à certaines catégories de personnes. Par exemple, il existe une liste de discussion réservée aux magistrats francophones, Jugenet[8].

---

[5] Yves Eudes, « Un maillage complexe qui défie la censure », *le Monde,* supplément multimédia, 12 février 1996, p.27.
[6] Site Web : <http://www.dejanews.com>.
[7] Site Web : <http://www.altavista.digital.com/>.
[8] Site Web : <http://www.DROIT.UMontreal.CA/~laliberte/Justiciers/Juges/abonnement.html>.

Les services d'information

Les services d'information ont pour point commun de permettre la consultation et le chargement d'information se trouvant sur des ordinateurs situés à distance. Le terme « information » est ici pris au sens large, il recouvre tous types de données.

FTP ou File Transfert Protocol

FTP est le protocole qui permet le téléchargement de fichiers à distance. Il sert par exemple à transférer des logiciels. L'utilisateur se connecte sur un serveur FTP pour y retirer des fichiers ou en déposer. L'accès au site peut être réservé ou public (on parle alors de serveur FTP anonyme).

World Wide Web ou WWW ou Web ou la Toile

Il s'agit d'un des services les plus connus du grand public, qui est trop souvent confondu avec l'Internet lui-même. Le Web utilise un langage de description particulier, le HTML, qui permet de créer des applications multimédia reliées entre elles par des liens hypertextes. Ce langage permet de diffuser des documents contenant du texte, des images, mais également du son et de la vidéo. Des langages qui permettent de créer des images en trois dimensions font leur apparition. La lecture de documents audio ou vidéo n'est pas encore performante, mais devrait devenir de plus en plus courante au fur et à mesure de l'évolution des techniques (notamment de compression) et de la diminution du prix d'accès aux réseaux à haut débit.

La technique des liens hypertextes permet à l'utilisateur de passer d'un site Web à un autre de manière très conviviale. A la différence de ce qui se passe pour les newsgroups, chaque application est stockée, hébergée sur un ordinateur particulier et identifiable. L'information est mise à disposition sur une application à laquelle on accède en donnant son adresse Web ou URL ou en suivant un lien hypertexte.

Chaque application est elle-même composée de plusieurs fichiers ou « pages », reliées entre elles par des liens hypertextes. La consultation d'applications différentes amène l'usager à se connecter à des ordinateurs situés dans différentes parties du monde, sans que cela soit directement perceptible par l'utilisateur. L'information est mise à disposition et non diffusée, en ce sens que l'utilisateur, lorsqu'il consulte une application donnée, va se connecter à l'ordinateur sur lequel cette application tourne. Il rapatrie ensuite une copie du document qu'il veut consulter sur son ordinateur. Certaines applications sont situées sur des ordinateurs très puissants qui permettent à plusieurs milliers de personnes d'y accéder en même temps.

Le document rapatrié par l'utilisateur sur son ordinateur peut être conservé en mémoire, archivé, imprimé, modifié par celui-ci. En revanche, il n'est pas possible de modifier l'application elle-même sans y être autorisé.

Les échanges en temps réel

L'IRC ou Internet Relay Chat[9]

Un serveur IRC permet l'affichage de messages en temps réel et donc de dialoguer simultanément avec plusieurs utilisateurs reliés à d'autres serveurs du même type.

Des espaces de communication appelés channels permettent de regrouper les discussions par thèmes. De plus, il est possible de créer de nouveaux channels à tout moment. Chaque parti-

[9] Voir le dossier consacré à l'IRC, *Planète Internet* n° 5, mai 1996, pp. 38 et suivantes.

cipant est connu sous un pseudonyme. Le channel peut être rendu privé, de telle sorte que les messages ne puissent être lus que par des destinataires bien déterminés.

La téléphonie

Il existe aujourd'hui des logiciels qui permettent de téléphoner par l'Internet. Les deux interlocuteurs doivent disposer aujourd'hui du matériel et de logiciels adéquats et d'ordinateurs compatibles. Cette utilisation de l'Internet est aujourd'hui marginale et n'apporte pas un grand confort d'écoute mais elle pourrait être promise à un bel avenir.

La visiophonie

Sur l'Internet, la vidéo n'en est qu'à ses débuts. De nouveaux logiciels comme CU-Seeme (en français : « je te vois, tu me vois »), qui permettent de voir son interlocuteur et d'entendre sa voix en temps réel sont en cours de développement[10]. Déjà, en reliant une caméra à son ordinateur, on peut faire profiter le monde entier de la vue de son choix, réactualisée en permanence[11].

Les utilisations futures de ces applications restent à inventer, mais l'on peut penser qu'elles permettront à la fois de communiquer de manière privée par visioconférences entre deux ou plusieurs personnes déterminées, ou publiques, c'est-à-dire que les documents vidéos pourront être lus par n'importe quel utilisateur.

Les acteurs de la communication

Précisions terminologiques

Une fois que l'usager ou utilisateur final a accès aux services Internet par le biais de son fournisseur d'accès Internet, il peut consulter des données qui se présentent sous des formes variées. Pour mettre ces données à disposition des utilisateurs, différents ordinateurs sont nécessaires.

L'équipement informatique qui contient les informations mises à disposition selon un protocole particulier (Usenet, Web, etc.) est un *serveur*.

L'hébergement, c'est le fait pour un centre serveur de stocker les données d'un client afin de les mettre à disposition de l'utilisateur de l'Internet.

Par exemple, le serveur d'hébergement Web fournit la plate-forme informatique qui, raccordée à l'Internet, permet la consultation du *site Web* par l'usager.

Le *site* ou *service d'information* est un ensemble de données logiquement reliées et stockées sur un serveur.

L'information fournie par un service représente le contenu du service.

Le fournisseur de contenu ne doit pas être confondu avec le fournisseur d'accès. Le fournisseur d'accès fournit un accès à une infrastructure, à un ensemble de réseaux. Le fournisseur de contenu est un éditeur, un producteur d'information.

---

[10] Yves Eudes, « Conférences Planétaires », *le Monde,* supplément multimédia, 12 août 1966, p.24.
[11] Nicole Pénicaut, « Les yeux du Net », *Libération,* cahier multimédia, 8 mars 1996.

Qui fournit le contenu sur l'Internet ?

L'Internet n'est pas un moyen de communication exclusivement commercial.

Les entreprises mettent en place des sites Web pour présenter leurs activités, leurs produits et leurs services ou utilisent l'Internet pour faire de la télétransaction, du commerce électronique, de la publicité.

Elles fournissent également des informations d'intérêt général pour montrer leurs compétences dans un domaine particulier, pour des raisons de prestige, parce qu'elles se rémunèrent sur la publicité, comme complément de leurs activités hors réseaux, ou comme produit d'appel pour les services en accès sur abonnement.

De nombreux sites tels des universités, des administrations, des gouvernements mettent également à disposition des informations dans un but non commercial.

Les associations, les mouvements politiques et religieux utilisent aussi le Web comme moyen de présenter leurs idées et activités.

Enfin, le fournisseur d'information peut être l'utilisateur lui-même.

Les utilisateurs des réseaux sont aussi bien producteurs que consommateurs, émetteurs que récepteurs d'information. L'utilisateur peut être une entreprise, mais aussi un particulier agissant à titre personnel.

Cela est flagrant pour les catégories de services décrits ci-dessus, qui permettent les échanges et les discussions de manière interactive. Cela est également vrai pour les services d'information comme le Web.

De nombreux fournisseurs d'accès mettent à disposition de leurs utilisateurs des espaces de mémoire sur leur serveur de Web, et hébergent gratuitement le site réalisé par l'utilisateur lui-même. C'est ce que l'on appelle les sites ou pages personnels (homepage)[12].

L'Internet fournit ainsi un moyen de communication et de diffusion de masse peu onéreux.

Les sites réalisés par de petites associations côtoient ceux réalisés par de grandes multinationales.

Cette possibilité pour tout utilisateur de devenir fournisseur d'information est un trait original de l'Internet[13].

Une autre de ses caractéristiques est la manière dont on accède à l'information. Compte tenu du nombre de sites disponibles, du nombre de messages échangés, on ne trouve pas de manière non intentionnelle l'information recherchée. L'accès à un site, la lecture d'un message posté sur un forum de discussion ou un channel de l'IRC résulte d'un acte volontaire de l'utilisateur. Il s'agit d'une différence fondamentale avec la télévision ou la radio avec lesquelles l'auditeur ou le téléspectateur sont passifs. Sur l'Internet, l'usager choisit spécifiquement ce qu'il veut consulter. Ainsi, lors des auditions de témoins dans le cadre du procès en inconstitutionnalité du Communication Decency Act américain, un témoin du gouvernement a reconnu que les chances étaient très faibles qu'un utilisateur tombe par accident sur un site contenant des informations de nature sexuelle[14].

Une dernière particularité essentielle de l'Internet est que les catégories définies ne sont pas étanches : l'utilisateur est également producteur d'information, un utilisateur peut à son tour devenir fournisseur d'accès pour des tiers. Le fournisseur d'accès n'est pas nécessairement fournisseur de contenu, le serveur pas nécessairement fournisseur d'accès. Une communication démarrée de façon publique peut devenir privée et inversement.

---

[12] Thierry Noisette, « Le Web, émois et moi », *le Monde,* supplément multimédia, 29 juillet 1996, p. 24.

[13] "The Internet is therefore a unique and wholly new medium of worldwide communication", ACLU v. Reno, préc., note 1, II-Findings of facts, point 81.

[14] ACLU v. Reno, préc., note 1, II-Findings of facts, point 88.

Son fonctionnement technique particulier, la variété des services offerts et de l'information disponible, le rôle actif joué par les utilisateurs, sa nature internationale et décentralisée ne vont pas toujours rendre aisée l'application à l'Internet des lois existantes, conçues pour des systèmes centralisés, hiérarchisés et des catégories strictement définies.

L’accès à l’Internet

Première partie

Les services de télécommunication

L'accès aux services Internet va dépendre de l'accès aux réseaux de télécommunication.

Le secteur des télécommunications fait l'objet depuis plusieurs années d'un important mouvement de libéralisation dans le monde. Son importance stratégique, le développement technologique et de besoins nouveaux, la globalisation du marché ont amené la Commission européenne à prendre diverses initiatives et à poursuivre depuis les années 80, une politique d'ouverture à la concurrence de ce secteur[15].

C'est dans ce contexte qu'est intervenue en France la réglementation des télécommunications du 29 décembre 1990[16] et que le statut de France Télécom est passé à celui d'établissement autonome distinct de l'Etat.

Puis la Commission européenne a fixé au 1er janvier 1998 l'échéance de la libéralisation totale de l'infrastructure et des services de télécommunication, y compris les services de téléphonie vocale[17].

C'est dans cette optique de l'ouverture totale à la concurrence qu'a été adoptée en France la loi du 26 juillet 1996[18] sur la réglementation des télécommunications. Une autre loi, du même jour[19], transforme à partir du 1er juillet 1997, France Télécom, l'opérateur national, en une société anonyme de droit privé dont l'Etat détient la majorité du capital social[20]. Je vais rappeler les grandes lignes du régime mis en place par la loi du 29 décembre 1990 avant d'examiner les modifications apportées par la réforme récente des télécommunications.

La loi du 29 décembre 1990 sur les réseaux et services de télécommunication

La loi crée une distinction entre les fonctions d'exploitation des réseaux et les services de télécommunication.

[15] Voir le Livre vert sur le développement des services et équipements de télécommunications, COM(87) 290 du 30 juin 1987 et les directives d'application, notamment directive n°88/301 du 16 mai 1988 relative à la concurrence dans les marchés de terminaux de télécommunication (JOCE L131 du 27 mai 1988), directive n°90/388 du 28 juin 1990 relative à la concurrence dans les marchés des services de télécommunication (JOCE n° L192 du 24 juillet 1990) et directive n° 90/387 du 28 juin 1990 relative à la mise en œuvre de la fourniture d'un réseau ouvert de télécommunications (Open Network Provision - ONP, JOCE L192 du 24 juillet 1990).

[16] Loi n°90-1170.

[17] Voir le Livre vert sur la libéralisation des infrastructures de télécommunication et des réseaux de télévision par câble, COM(94) 440 final et COM(94) 682.

[18] Loi n°96-659 , JO du 27 juillet 1996.

[19] Loi n° 96-660 relative à l'établissement national France Télécom, JO du 27 juillet 1996.

[20] Voir les rapports de MM. Gaillard, JOAN n°2891, et Larcher, JO Sénat, n°406

Les réseaux

Les réseaux sont rangés en deux catégories, les réseaux ouverts au public et les réseaux indépendants réservés à l'usage d'une personne ou d'un groupe fermé d'utilisateurs. Les réseaux ouverts au public, qui constituent l'infrastructure même des télécommunications, sont un monopole de France Télécom.

Des dérogations peuvent être accordées sur autorisation, subordonnée au respect d'un cahier des charges, du ministre chargé des Télécommunications pour établir et exploiter un réseau radioélectrique (article L33-1 I du Code des postes et télécommunications, CPT).

C'est grâce à cette dérogation qu'a été autorisée la mise en place des réseaux de téléphones portables concurrents de ceux de France Télécom.

Les services

Les services de télécommunications sont eux-mêmes rangés en deux catégories selon qu'ils sont fournis au public ou réservés à l'usage privé d'un groupe d'utilisateurs.

Parmi les services ouverts au public (articles L34 et suivants du CPT), on distingue :

- le service téléphonique qui relève du monopole de France Télécom, avec une dérogation pour le radiotéléphone ;
- les services supports, c'est-à-dire les services de transfert de données (services dont l'objet est de transmettre et d'acheminer des signaux entre les points de terminaison d'un réseau de télécommunication), comme les liaisons louées ou lignes spécialisées, les transmissions de données type Transpac, ou Numéris. France Télécom est autorisée de plein droit à les fournir. D'autres prestataires peuvent également les fournir sous réserve d'obtenir une autorisation du ministre des Télécommunications, avec respect d'un cahier des charges ;
- les services radioélectriques (fournis par voie hertzienne) et les services fournis sur le réseau câblé, qui nécessitent une autorisation préalable du ministre pouvant se cumuler avec les autorisations d'autres autorités comme le CSA (Conseil supérieur de l'audiovisuel) ;
- les autres services à valeur ajoutée (article L34-5 du CPT). La fourniture est libre pour les services directement exploités sur les infrastructures du ou des réseaux publics, notamment sur les lignes du réseau téléphonique commuté. Sinon, un régime de déclaration ou d'autorisation préalable est prévu, suivant la taille du réseau, pour les services fournis sur des liaisons louées.

Le fournisseur d'accès est fournisseur de services de télécommunications. Dans quelle catégorie se range-t-il ?

Le fournisseur d'accès utilise les réseaux de télécommunications, les liaisons spécialisées de France Télécom. Les fournisseurs d'accès ont besoin de ces lignes spécialisées pour se connecter au « backbone », à l'épine dorsale de l'Internet, ces artères à très haut débit qui relient les zones principales. Cependant, le fournisseur d'accès ne vend pas une connexion entre deux points comme les services supports, mais effectue une prestation à la fois beaucoup plus large et de nature différente. Il fournit la connexion à un réseau qui fait partie de l'infrastructure Internet, qui utilise le protocole TCP/IP.

Le fournisseur d'accès se range dans la dernière catégorie : il fournit des services à valeur ajoutée.

Les équipements de télécommunication

Les équipements (postes téléphoniques, modem) sont librement commercialisés sous réserve, pour les équipements destinés au réseau public, d'avoir fait l'objet d'un agrément préalable de la Direction générale des postes et télécommunications (articles L34-9 et suivants du

CPT). La mise sur le marché et la publicité en faveur d'un équipement non agréé est interdite sous peine d'amende[21].

L'agrément est exigé sous peine d'une amende de quatrième classe (5 000 francs)[22]. En application d'une directive européenne en date du 29 avril 1991[23] concernant le rapprochement des législations des Etats membres relatives aux équipements terminaux de télécommunication, l'agrément obtenu dans un autre Etat membre, s'il a été donné sur la base de normes techniques européennes, est reconnu en France.

La réforme de la loi du 26 juillet 1996

La loi crée une situation de pleine concurrence aussi bien en ce qui concerne l'établissement des infrastructures des réseaux qu'en ce qui concerne le marché des services de télécommunications.

On attend de l'ouverture à la concurrence des services de télécommunication et des infrastructures[24] :

- une offre de services plus abondante et diversifiée ;
- l'émergence de services nouveaux et de meilleure qualité ;
- que les diminutions de prix induites par la concurrence et l'évolution technologique soient répercutées sur les utilisateurs ;
- des effets favorables sur l'économie, l'emploi et l'aménagement du territoire.

Les réseaux

Les réseaux publics sont ouverts à la concurrence. Une autorisation du ministre des Télécommunications avec respect d'un cahier des charges est nécessaire pour établir et exploiter un réseau ouvert de télécommunication. Les motifs pouvant fonder un refus sont limités par la loi.

Les services

- service téléphonique entre points fixes

Il est également ouvert à la concurrence, sous réserve d'une autorisation du ministre chargé des Télécommunications.

- les autres services de télécommunications

Ils sont fournis librement (article L34-2 du CPT).

Cependant :

- si le service est fournit sur le réseau câblé, il est soumis à déclaration auprès de l'ART, l'Autorité de régulation des télécommunications (article L34-4 du CPT) ;
- la fourniture au public de services de télécommunication utilisant des fréquences hertziennes est libre (article L34-3 du CPT), sous réserve du respect des dispositions liées à l'établissement des réseaux quant à l'allocation des fréquences.

[21] Articles 8 à 10 de la loi n°89-1008 du 31décembre 1989.
[22] Articles R 20-26 à R20-30 du CPT.
[23] JOCE L128 du 23 mai 1991.
[24] Fiches techniques sur le projet de loi de réglementation des télécommunications du ministère des Télécommunications.

Les équipements terminaux

Ils sont fournis librement (article L34-9 du CPT) comme dans le régime antérieur. La loi ne parle plus d'agrément mais « d'évaluation de conformité », selon un mécanisme dont le détail est fixé par décret. Les organismes intervenant dans la procédure d'évaluation doivent être désignés de façon à offrir aux industriels concernés un choix préservant leur indépendance par rapport à des entreprises offrant des biens ou des services dans le domaine des télécommunications.

Les équipements ne peuvent être importés en vue de la mise à consommation de pays n'appartenant pas à l'espace économique européen, mis en vente, distribués, connectés à un réseau ouvert au public ou faire l'objet d'une publicité que s'ils ont fait l'objet d'une attestation de conformité.

Que risque l'étranger en déplacement en France qui emporte avec lui son modem en vue de se connecter ?

S'il réside dans un autre pays membre de l'Union européenne, et que son appareil est conforme aux normes européennes, il n'y a pas de problème.

Sinon, il est en infraction avec l'article L34-9 du CPT et risque les peines de contravention qui seront éventuellement prévues par le décret d'application.

Il peut également engager sa responsabilité envers l'exploitant du réseau pour toutes les conséquences financières liées à l'utilisation d'un matériel non conforme[25].

Interconnexion, portabilité, annuaire universel

La loi fixe les conditions d'interconnexion, c'est-à-dire les liaisons physiques et logiques entre les réseaux de différents opérateurs (article L34-8 du CPT), et pose le principe de portabilité des numéros (article L34-10 du CPT), c'est-à-dire que l'utilisateur pourra changer d'implantation géographique ou d'opérateur en gardant le même numéro.

La loi prévoit la mise en place d'un annuaire universel géré par une entité indépendante du ministère des Télécommunications, de France Télécom et des autres opérateurs du service de téléphonie publique (article L35-4 du CPT).

Le service universel

La loi fixe les contours du service universel (articles L35-1 à L35-4 du CPT), la notion européenne de service public. Le service universel est défini comme « la fourniture à tous d'un service téléphonique de qualité et à prix abordable, dans le respect des principes d'égalité, de continuité et d'adaptabilité, et ce indépendamment de la localisation géographique de l'utilisateur. Il comprend l'acheminement des communications téléphoniques entre les points d'abonnement, celui des appels d'urgence, la fourniture d'un service de renseignement et d'un annuaire d'abonnés, la desserte du territoire national en cabines téléphoniques ».

Les service universel ne comprend ni le téléphone mobile, ni l'accès au RNIS (Réseau numérique à intégration de services), aux réseaux à haut débit, aux offres de liaisons louées, de commutation par données de paquets, etc. [26]

La notion de service universel n'a pas été étendue à la fourniture de ces services au motif que cela mettrait en péril l'équilibre de son financement par France Télécom et que cela risquerait d'entraver sa compétitivité.

Toutefois, les services obligatoires que doit assurer France Télécom comprennent une offre sur l'ensemble du territoire d'accès au réseau numérique à intégration de services, de liaisons

[25] En ce sens : TI Paris 7 janvier 1993, Delaunay/France Télécom, Juris-PTT 1993/2 n°31.

[26] Voir amendement n°158 présenté par le groupe socialiste au Sénat et amendement n° 172 présenté par M. Trégouët, Compte-rendu analytique officiel du Sénat, séance du 6 juin 1996 p.39.

louées, de commutation de données par paquets, de services avancés de téléphonie vocale et de services télex (article L35-5 du CPT).

Le développement de l'Internet passe par le développement de l'offre de ces services à un prix abordable aussi bien pour les PME/PMI que pour les particuliers.

On attend de la concurrence qu'elle pousse le développement de ces services sur tout le territoire, à l'instar de ce qui se passe actuellement pour le téléphone mobile. Pour tenir compte de l'évolution des technologies et des services de télécommunication et des besoins de la société, de nouveaux services pourront être inclus dans le champ du service universel (article L35-7 du CPT).

La loi fixe enfin les modalités de financement du service universel, avec notamment la contribution des autres exploitants.

La nouvelle autorité de régulation

La loi met en place une nouvelle autorité de régulation, l'ART, l'Autorité de régulation des télécommunications à compter du 1er janvier 1997 (article L36 et suivants du CPT).

Cette autorité aura les pouvoirs suivants :

- pouvoir d'arbitrage en matière d'interconnexion ;
- pouvoir de sanction ;
- instruction des demandes de licence d'exploitation des services du réseaux ;
- allocations de fréquences ;
- édition de règles techniques applicables aux réseaux et terminaux.

Enfin, la loi crée une Agence nationale des fréquences radioélectriques (article L97-1 et suivants du CPT) à compter du 1er janvier 1997. Il s'agira d'un établissement public chargé de coordonner l'implantation sur le territoire national des stations radioélectriques, afin d'assurer une meilleure répartition des ressources disponibles.

La fourniture de services d'accès à l'Internet

Elle est *a priori* libre.

Néanmoins, dans un certain nombre de cas, une autorisation va se révéler nécessaire : fourniture d'accès sur le réseau câblé[27], fourniture d'accès par le réseau hertzien[28]. En outre, une fois qu'une personne est connectée à l'Internet, elle a accès à toutes sortes de services, dont les services de téléphonie vocale. Enfin, les données transportées peuvent transiter sur toutes les infrastructures existantes, qu'il s'agisse du fil, du câble, de la voie hertzienne ou des satellites.

Doit-on en déduire que tous les fournisseurs d'accès devraient notamment obtenir l'autorisation de fournir des services de téléphonie ? Une telle interprétation de l'article L34-1 du CPT serait excessive et sans aucun doute inapplicable, compte tenu de la variété et de la fluidité de la catégorie des fournisseurs d'accès. Lorsqu'une personne fournit un accès, elle ne sait pas à l'avance, elle ne peut pas contrôler quels services seront utilisés.

L'Internet est composé de réseaux informatiques et l'informatique a pour caractéristique de ne pouvoir traiter que des données sous forme numérique. Mais tous types de données peuvent être numérisées : texte, image, son, vidéo. Evidemment, la numérisation d'une bande vidéo nécessite plus de mémoire que la numérisation de texte. Une fois que l'information est numérisée, elle peut être traitée, stockée, modifiée, transmise, elle peut circuler à travers les réseaux.

---

[27] La société TV CABLE propose des accès à l'Internet par le câble. Site Web : <http://www.cybercable.tm.fr>.

[28] Une société lyonnaise, ASI, expérimente une technologie de transfert des données informatiques par voie hertzienne, site Web : <http://www.asi.fr>.

Plus l'espace occupé par un document numérisé est grand, plus la bande passante nécessaire pour faire passer ces données avec une définition acceptable croît. L'augmentation du débit des réseaux, l'amélioration des techniques de compression (c'est-à-dire les techniques qui permettent de faire passer la même information avec moins de données), l'évolution des techniques font que toutes ces données vont transiter sur les mêmes supports et pourront transiter sur les réseaux informatiques.

Dans ce contexte, toute réglementation qui tend à allier un type de données à un support particulier n'a plus de sens.

La réglementation concernant le service téléphonique en est une illustration : aujourd'hui, la voix passe par les réseaux filiaires, et par les réseaux radioélectriques (téléphone portable). Lorsque demain la voix passera aisément par les réseaux informatiques, la réglementation de la fourniture des services téléphoniques sera en pratique indifférente aux utilisateurs.

Pour être complet dans ce panorama des réformes législatives, il convient enfin de signaler la loi du 10 avril 1996 [29] relative aux expérimentations dans le domaine des technologies et services de l'information. Cette loi qui vise à « favoriser le développement des infrastructures et des services de télécommunications et de communication audiovisuelle », autorise des dérogations à la réglementation des télécommunications et de l'audiovisuel pour effectuer des expérimentations de projets spécifiques retenus par le Comité interministériel des autoroutes et services de l'information. Pour les télécommunications, il s'agit avant le 1er janvier 1998 de permettre des expérimentations incluant la fourniture de services de télécommunication entre ports fixes par l'intermédiaire de téléports, d'infrastructures alternatives, et de réseaux câblés.

En ce qui concerne l'audiovisuel, le CSA peut adapter les règles en vigueur, pour la diffusion des services de radiodiffusion sonore ou de télévision. Ceci concerne les services de télévision et radio mis simultanément à la disposition du public et multidiffusés (services audiovisuels à la demande). Les licences expérimentales sont délivrées pour une durée de trois ans.

Ces expérimentations ne concernent pas les réseaux informatiques et l'infrastructure Internet.

[29] Loi n° 96-299, JO du 11 avril 1996.

Deuxième partie

Les noms de domaine

Qu'est-ce qu'un nom de domaine ?

Chaque ordinateur relié à l'Internet doit pouvoir être identifié et localisé. Tout comme vous avez besoin de connaître l'adresse de votre correspondant pour lui envoyer un courrier, un ordinateur doit connaître « l'adresse Internet » de la machine à laquelle sont destinées les données qu'il transfère. Si vous souhaitez consulter des informations, que ce soit des informations présentes sur un site Web ou des fichiers à télécharger en FTP, vous devez là aussi être en mesure de fournir son adresse sur le réseau. Grâce à l'Internet Protocol(IP), chaque machine possède sur l'Internet une adresse unique (adresse IP) qui permet au réseau d'acheminer les paquets de données à bon port.

Les adresses Internet sont représentées par une suite de 4 chiffres séparés par des points. Par exemple, l'adresse de la machine hébergeant le site de l'Association des utilisateurs d'Internet (AUI) est : [194.2.1.73].

Si les chiffres conviennent parfaitement aux ordinateurs, il n'en va pas de même pour les humains. Un mécanisme a donc été mis en place pour faire correspondre à chaque adresse IP, une adresse symbolique afin de rendre leur mémorisation plus aisée : c'est le DNS (Domain Name System ou Système des noms de domaines).

Comme les adresses IP, les mots composant les noms de domaines sont séparés par des points. Par exemple, le nom de domaine de l'AUI est <aui.fr>.

Le DNS est organisé en zones ou espaces de nommages hiérarchiques et décentralisés, de manière à pouvoir attribuer à des personnes ou à des organisations différentes la responsabilité de la gestion des noms de domaines de chaque zone.

Il existe une zone par pays relié à l'Internet, ces zones nationales étant identifiées par un code à deux lettres : <.fr> pour la France, <.ca> pour le Canada, <.es> pour l'Espagne,etc. Chaque pays est responsable de la gestion de sa propre zone et peut à l'intérieur de son domaine créer librement des sous-domaines.

Par exemple, le sous-domaine <.gouv> a été créé pour les sites de l'administration française dans la zone <.fr>. Le nom de domaine du ministère des Télécommunications est ainsi : <telecom.gouv.fr>.

Il existe 3 zones à l'usage exclusif des américains : <.gov> (pour gouvernement), <.mil> (pour militaire), réservées au gouvernement américain et <.edu> pour les organismes d'enseignement supérieur, et 4 zones génériques à vocation internationale :

- <.com> pour les activités et sociétés commerciales ;
- <.net> pour les fournisseurs d'accès et les organismes participant au fonctionnement de l'Internet ;

- <.int> pour les organisations résultant de traités internationaux ;
- <.org> pour les organisations diverses ne rentrant dans aucune autre catégorie.

Ces zones sont appelées « Top-Level Domains », la hiérarchie des domaines se lisant de droite à gauche.

Exemples :

- dans le domaine <argia.fr>, <argia> appartient au domaine ou à la zone <.fr>, qui désigne la France ;
- le fournisseur d'accès Easynet a deux noms de domaine qui figurent sur ses publicités : <easynet.fr> ou <easynet.co.uk>. Le premier nom fait partie du domaine <.fr>, le deuxième du domaine <.uk> (pour Grande-Bretagne) et du sous-domaine <.co> (pour commercial) ;
- la société française Bull a déposé le nom de domaine <bull.com>, la société suisse Swissair le nom <swissair.com>, la société allemande Mercedes le nom <mercedes-benz.com> . Pour les zones internationales, il n'y a pas de notion de pays.

Chaque nom à l'intérieur d'un domaine doit être unique, mais un même nom peut être déposé dans plusieurs zones et plusieurs sous-domaines. Par exemple, <telecom.gouv.fr> pourrait coexister avec <telecom.tm.fr>.

Pour reprendre l'analogie avec les adresses postales, deux rues portant le même nom peuvent parfaitement exister dans deux villes différentes.

La gestion des zones <.com>, <.gov>, <.net>, <.edu> et <.org> est assurée depuis le 13 septembre 1995 jusqu'en 1998 par la société américaine Network Solutions Inc.

Chaque pays possède une antenne du NIC (Network Information Center) responsable de la gestion de la zone correspondante. En France, c'est l'INRIA (Institut national de recherche en information et automatique), établissement public à caractère scientifique et technologique sous la tutelle du ministère de l'Industrie, qui gère depuis 1987 le domaine <.fr>. Pour les zones internationales, c'est l'InterNIC qui assure cette responsabilité à travers Network Solutions Inc.

Noms de domaines et adresses Internet

Un nom de domaine, c'est une zone d'adressage, l'équivalent d'une rue dans une adresse postale. L'adresse complète d'un document sur l'Internet s'appelle URL pour Universal Resource Locator, que l'on pourrait traduire par Localisateur Universel de Ressource.

Une des composantes de l'URL est le nom de domaine. Ce nom de domaine est précédé du protocole de communication, qui, de manière simplifiée, sert à désigner le type d'application permettant d'accéder à une donnée.

Par exemple :

- <hhtp://www.argia.fr> est l'adresse sur le Web (les applications utilisent le protocole http) du serveur <argia> dans la zone <.fr>,
- <ftp://ftp.argia.fr> serait l'adresse ftp du serveur <argia> dans la zone <.fr>.

Après le nom de domaine est indiquée la situation exacte du document dans le serveur.

Par exemple :

- <http://www.argia.fr/doc1.html> permet d'accéder sur le serveur <argia>, à la page Web intitulée « doc1.html ».

Le nom de domaine est également une des composantes des adresses de courrier électronique.

Par exemple, mon adresse électronique est : sedallian@argia.fr.

L'importance du nom de domaine

Sa première fonction est de permettre d'atteindre quelqu'un ou un site particulier, de la même manière qu'un numéro de téléphone et une adresse fournissent des informations sur la manière de contacter une entreprise ou une personne.

L'adresse complète, ou URL, est également nécessaire pour localiser précisément une donnée sur l'Internet.

Dans ces conditions, une personne souhaitant monter un site Internet peut s'interroger sur l'utilité d'avoir son propre nom de domaine alors qu'elle pourrait tout aussi bien avoir une adresse sur le serveur du fournisseur de service hébergeant son site.

Par exemple : soit une société « lambda » souhaitant mettre à disposition un document « doc.html » sur un site logé chez un fournisseur « fournisseur », l'adresse la plus intéressante pour le document est-elle <http://www.fournisseur.fr/lambda/doc.html> ou bien <http://www.lambda.fr/doc.html> ?

La société pourrait être tentée de raisonner ainsi par mesure d'économie, l'enregistrement d'un nom de domaine étant une opération payante, et l'hébergement du site sous un nom de domaine propre étant facturé en général plus cher par le fournisseur de services.

Avoir son propre nom de domaine présente deux grands avantages.

En premier lieu, **les noms de domaines sont portables**, c'est-à-dire que le nom symbolique est indépendant de la localisation géographique de la machine supportant l'application. Pour une même adresse symbolique, on peut faire varier dans le temps l'adresse informatique correspondante de manière transparente pour l'utilisateur.

La machine à laquelle on accéderait à travers l'adresse <http://www.argia.fr> pourrait tout aussi bien se trouver à Seattle ou à Issy-les-Moulineaux, son nom de domaine resterait <argia.fr>. De même le service peut être transféré à tout moment chez un autre fournisseur sans que l'adresse symbolique ait besoin d'être modifiée.

Comment ce résultat est-il obtenu ? Ce que l'on appelle un serveur de nom fait la conversion entre l'adresse symbolique utilisée par les humains et les adresses informatiques.

Avoir son propre nom de domaine est donc un gage de stabilité comme le démontre l'affaire suivante.

L'association Relais et Châteaux, qui édite le guide du même nom, avait un site hébergé chez le fournisseur de services Calvacom à l'URL : <http://www.calvacom.fr/relais/accueil.html>.

L'association décide de changer de fournisseur et son adresse devient alors : <http://www.integra.fr/relaischateaux>.

Un conflit surgit lors de la rupture du contrat entre Relais et Châteaux et la société Calvacom, qui maintient en activité la première URL.

L'association s'aperçoit que près de deux mois après la rupture du contrat, la page d'accueil de Relais et Châteaux est toujours référencée dans les moteurs de recherche Internet sous l'ancienne URL, c'est-à-dire sous le nom de domaine de Calvacom[30].

Le temps que les moteurs de recherche Internet enregistrent la nouvelle URL, il peut s'écouler plusieurs mois en raison du nombre important de nouveaux sites créés chaque jour.

Si l'association Relais et Châteaux avait eu son propre nom de domaine, le changement de fournisseur n'aurait pas eu d'incidence sur l'URL de son site Web.

En second lieu, **un nom de domaine est une indication d'origine**.

[30] Communiqué de presse du 28 mai 1996 de Relais et Châteaux.

Les services de l'administration française sont ainsi dans l'obligation d'utiliser un nom de domaine composé de la racine <gouv.fr>, « afin que les usagers (français et étrangers) n'aient aucun doute sur le fait qu'il s'agit d'un service officiel de l'administration française, placé sous son contrôle ou agissant en son nom et pour son compte.[31] »

Pour une entreprise, il peut être important d'avoir un nom de domaine facilement reconnaissable et identifiable et correspondant à son nom commercial ou à sa raison sociale.

Les entreprises américaines ayant un service Web ont généralement adopté un nom de domaine composé de : <raison sociale.com>. L'utilisateur n'a aucun effort à faire pour se souvenir que l'adresse du site Web d'IBM est <http://www.ibm.com>, que celle de Microsoft est <http://www.microsoft.com>.

De même, les entreprises françaises adoptent souvent comme nom de domaine <raison sociale.fr>, comme <lemonde.fr> ou <airfrance.fr>.

Le journal *Libération,* hébergé un temps sous l'URL : <http://www.netfrance.com/Libe> a désormais son propre nom de domaine : <liberation.fr>. Ce nom est manifestement plus aisé à mémoriser que l'adresse précédente.

Aux Etats-Unis, les noms de domaine sont devenus un véritable enjeu.

Imagineriez-vous que votre concurrent principal prenne comme nom de domaine le nom de votre société ? C'est ce qui est arrivé à la société Kaplan, qui, lorsqu'elle a voulu monter un site Web s'est aperçue que <kaplan.com> avait déjà été enregistré par son concurrent direct, Princeton Review.

Vous vous attendez à trouver le site Web de la chaîne de fast food Mc Donald's à l'adresse <http://www.mcdonalds.com> ? C'est le cas aujourd'hui mais il n'en a pas toujours été ainsi, l'adresse ayant été initialement enregistrée par un journaliste du magazine américain Wired.

L'intérêt pour les noms de domaine se développe en même temps que s'accroît la proportion d'activités commerciales sur l'Internet.

Avoir un nom de domaine correspondant à une dénomination ou à une marque déposée et dont le consommateur puisse facilement se souvenir est devenu commercialement très important outre-atlantique. Toutes les sociétés veulent avoir leur nom de domaine dans la zone <.com>, et enregistrer leurs produits sous le nom de domaine approprié.

Ainsi la société Kraft General Foods a enregistré plus de 150 noms de domaine tel que <velveeta.com> et <parkay.com> et la société Procter et Gambler est allée encore plus loin, enregistrant non seulement ses marques habituelles, mais aussi des dizaines de noms comme <underarm.com> et <diarrhea.com>[32].

Les noms de domaine ont donc une double nature, à la fois indication d'une location, d'une adresse et indication d'une source.

En France, le NIC-France a élaboré des règles pour l'enregistrement des noms de domaine qui prennent en compte l'aspect « indication de source » du domaine. Aux Etats-Unis, où est gérée la zone <com>, la plus demandée, l'aspect <indication de source> des noms de domaine a en premier lieu été occulté : il suffisait pour déposer un nom de domaine que le nom n'ait pas été déjà enregistré. Après plusieurs affaires mettant en lumière des conflits entre noms de domaine et marques ou d'autres signes distinctifs comme les noms commerciaux, la société Network Solutions Inc (NSI) a été amenée, sans modifier la règle du « premier venu, premier servi », à adopter une charte de règlement des conflits (Dispute Resolution Policy).

Une personne désirant enregistrer un nom de domaine peut le faire dans la zone <.fr> ou dans les zones internationales, notamment en <.com>.

---

[31] Circulaire du Premier ministre du 15 mai 1996, relative à la communication, à l'information et à la documentation des services de l'Etat sur les nouveaux réseaux de télécommunication, JO du 19 mai 1996.

[32] Exemples cités par David G. Post, A domain by any Other Name, "Plugging In", American Lawyer, May 1996.

Seront examinées en premier lieu les procédures d'enregistrement en France et aux Etats-Unis.

Les règles, notamment américaines, d'attribution des noms de domaine sont des sources potentielles de conflits entre plusieurs personnes ou entités revendiquant le même nom de domaine.

Dans un second temps seront abordés les aspects juridiques de la question avec notamment le problème des conflits entre marques, signes distinctifs et noms de domaine.

Enregistrer un nom de domaine

Enregistrer un nom de domaine dans la zone <.fr>

Toute personne ou organisme désirant se faire attribuer un nom de domaine doit s'adresser au NIC-France[33].

Cet organisme a élaboré des règles pour l'attribution des noms de domaine, une « charte du nommage Internet en France », qui doit être respectée pour toute nouvelle création de nom de domaine dans la zone <.fr>.

Le nom choisi doit avoir un lien avec le demandeur et le NIC-France vérifie le bien-fondé de celui-ci à obtenir le nom souhaité, exerçant en fait un contrôle étroit sur l'attribution des noms de domaine en France.

Le nom choisi doit être soit le nom de l'organisme déposant, soit son sigle, soit une marque déposée par lui.

Les entreprises doivent fournir un extrait K-bis et le numéro SIRET, les associations une justification de la publication de leur constitution au Journal Officiel. Pour les marques, il faut fournir le certificat d'enregistrement à l'INPI (ou au moins le récépissé de dépôt).

Les marques sont, depuis mai 1996, enregistrées sous le domaine <tm.fr>. Selon le NIC, cela permettra de supporter simultanément des noms de marques et de sociétés identiques.

En effet, le NIC-France est particulièrement soucieux d'éviter les homonymies, ce qui l'amène insidieusement à prendre parfois la position du nommeur.

Par exemple, la société Eff-Management a voulu déposer le nom de domaine <eff.fr>. Il lui fut répondu par le NIC que ce nom de domaine ne pouvait pas être enregistré au motif que plusieurs sociétés possédaient « eff » dans leur raison sociale, le NIC proposant, d'après l'extrait K-bis du demandeur, d'enregistrer <eff-management.fr> ou <eff-mang.fr>.

Par ailleurs, un certain nombre d'entités sont obligées de choisir un nom de domaine en accord avec la convention de nommage élaborée par le NIC.

Par exemple, les ambassades doivent être enregistrées sous le format <amb-nom de ville ou pays.fr>, les chambres de commerce sous le domaine <cci.fr>, les universités sous le format <univ-nom de l'université.fr>.

De nouveaux sous-domaines sont régulièrement créés par le NIC, comme le domaine <gouv.fr> pour les ministères et le gouvernement français, <barreau.fr> pour les barreaux d'avocats, <asso.fr> pour les associations, <presse.fr> pour les périodiques, créés en mai et en juin 1996.

[33] NIC France. Domaine de Voluceau, BP 105, F78 153 Le Chesnay Cedex tél. : 01 39 63 56 16, fax : 01 39 63 55 34, site Web : <http://www.nic.fr>, courrier électronique : nic@nic.fr.

Un certain nombre de noms sont réservés et ne seront pas affectés : noms génériques, noms de protocoles, noms géographiques.

D'autres questions sont en cours de discussion dans les groupes de travail du NIC : nommage géographique[34], enregistrement de noms de domaine pour des particuliers notamment.

Les nouvelles règles qui seront élaborées par le NIC-France s'imposeront aux nouvelles demandes d'enregistrement de noms de domaine.

Une fois le nom demandé accepté par le NIC, la règle du <premier arrivé, premier servi> est appliquée.

En France, il est obligatoire de passer par un prestataire de services habilité par le NIC pour enregistrer un nom de domaine. Deux options sont proposées aux fournisseurs de services :

- avec une adhésion annuelle de 30 000 Francs HT par an, chaque nouveau domaine étant facturé 800 F HT ;
- sans adhésion annuelle, chaque nouveau domaine étant facturé 2 400 F HT (tarif 1996).

En outre, le NIC-France envisage de mettre en place une procédure de renouvellement périodique du nom de domaine qui pourrait être éventuellement facturée.

Les services NIC sont facturés au prestataire qui en répercute le coût sur ses propres clients.

Le domaine de mise en place d'un domaine dans la zone <.fr> est de 48 heures à compter de la réception du formulaire d'enregistrement correctement rempli qui doit obligatoirement être adressé par courrier postal.

Le nom de domaine ne peut pas être réservé, il doit correspondre à un serveur effectif fonctionnel et accessible en permanence de toutes les machines connectées à l'Internet.

Le nom attribué est la propriété de l'organisme demandeur, et non celle du fournisseur de services. En cas de changement de prestataire, le NIC précise que le fournisseur initial devra avoir reçu une demande de résiliation de la part de cet organisme.

Enregistrer un nom de domaine dans la zone <.com>

Pour enregistrer un domaine dans la hiérarchie <.com>, <.org> ou <.net>, il faut s'adresser à l'InterNIC, géré par le NSI aux Etats-Unis[35].

Contrairement à ce qui se passe pour la hiérarchie <.fr>, il n'est pas exigé que le nom du domaine choisi soit une marque ou un sigle ou le nom du requérant. On applique la règle du <premier arrivé, premier servi> : le NSI vérifie seulement que le nom demandé n'a pas déjà été attribué.

Le NSI demande au requérant de lui garantir qu'il a le droit d'utiliser le nom du domaine, que le nom du domaine choisi ne porte pas atteinte, à sa connaissance, aux droits d'autrui, qu'il a l'intention d'utiliser le domaine et que le nom sera utilisé dans un but légitime. Aucun contrôle n'est effectué par le NSI sur le nom choisi. Il est vrai qu'au mois de Janvier 1996, on recensait déjà 132 213 noms de domaine dans la zone <.com>, la plus demandée, alors qu'à titre de comparaison, on comptait sur la même période 2 439 demandes dans la zone <.fr>[36].

En Juillet 1996, les volumes avaient atteint 284 737 domaines en zone <.com> et 3 962 pour <.fr>.

---

[34] Le nom de domaine ferait référence au département du demandeur, une orientation qui semble paradoxale pour un réseau international.

[35] Network Solutions Inc. ATTN : InterNIC Registration Services, 505 Huntmar Park Drive, Herndon, VIRGINIA 22 070, tél. : 1 703 742 4777, fax : 1 703 742 8449, e-mail : hostmaster@internic.net, site Web : <http://rs.internic.net>.

[36] Statistiques fournies par Networks Wizards, site Web : <http://www.nw.com>.

On comprend aisément qu'avec un tel nombre de demandes à traiter, il soit difficilement possible au NSI d'effectuer un contrôle des noms de domaine qu'il enregistre cela ralentirait considérablement les délais d'enregistrement.

S'il n'est pas possible d'enregistrer les noms <paris.fr> ou <france.fr>, s'agissant de noms géographiques qui d'après les règles du NIC-France ne peuvent pas être attribués, en revanche vous auriez pu déposer <paris.com> ou <france.com> si ces noms n'avaient pas déjà été utilisés, <paris.com> par la société Paris Corp. de Virginie et <france.com> par une société californienne <France Online> détenue par des Français.

La règle du <premier arrivé, premier servi> a inévitablement entraîné des abus, et des conflits lorsque plusieurs entités ont revendiqué le même nom de domaine, cela a conduit le NSI à adopter une charte de résolution des conflits.

Autre différence avec le système français, il n'est pas obligatoire de passer par un fournisseur de services pour enregistrer un nom de domaine dans une des hiérarchies internationales. Il est néanmoins nécessaire d'indiquer l'adresse des serveurs de nom, ce qui suppose, si le déposant n'est pas directement relié à l'Internet, d'avoir un accord avec un fournisseur de services.

Toute la procédure d'enregistrement s'effectue directement à travers le réseau, sans recours aux moyens de communication traditionnels tels que la télécopie ou le courrier postal. Les renseignements suivants doivent être portés dans le formulaire d'enregistrement, disponible sur le site Web du NSI : adresse électronique, objectif poursuivi, nom de domaine, information sur le requérant, contact administratif, contact technique, adresse de facturation, information sur les serveurs de noms. Une fois rempli en ligne, le formulaire est validé. Pour la confirmation, un courrier électronique est adressé, auquel il devra être répondu par le même moyen pour valider l'opération. La facture est adressée au choix par courrier électronique ou par courrier postal. L'opération achevée, vous venez de conclure votre premier contrat entièrement électronique à travers l'Internet.

A court et moyen terme, déposer un nom de domaine en <.com> revient moins cher qu'en <.fr> : 100 dollars pour la création d'un domaine et après une période de deux ans, 50 dollars par année supplémentaire.

En revanche, la procédure d'enregistrement d'un nom de domaine en <.com> est un peu longue, mais des efforts sont en cours pour améliorer les délais.

En pratique, beaucoup de noms de domaine sont enregistrés sans être nécessairement utilisés. Des sociétés ont enregistré les marques de leur produit comme nom de domaine, soit à titre préventif, soit en vue d'une utilisation future, sans nécessairement mettre en place de site correspondant au nom de domaine enregistré.

Le nom enregistré est également la propriété de l'organisme requérant et non celle du fournisseur de services, considéré par le NSI, si c'est lui qui effectue la demande, comme un représentant du requérant. Il est précisé sur le formulaire d'inscription que le représentant prend la responsabilité de notifier au requérant les conditions d'enregistrement des noms de domaine. En cas de changement de fournisseur de services, un formulaire est à remplir, toujours en ligne, et toujours à confirmer par courrier électronique, pour mettre à jour les informations qui avaient été enregistrées.

Aspects juridiques

Avec la règle de l'InterNIC « du premier venu premier servi », des conflits n'ont pas tardé à apparaître aux Etats-Unis en ce qui concerne principalement les domaines de la zone <com>.

Notamment des noms de domaine correspondant à des marques déposées par autrui ont été enregistrés.

Juridiquement, il s'agit de savoir si l'utilisation de la marque déposée par un tiers comme nom de domaine constitue une contrefaçon.

Dans d'autres cas, un nom de domaine est enregistré en vue de porter atteinte aux droits d'un tiers.

Un certain nombre de conflits peuvent être résolus par application des principes généraux du droit de la propriété intellectuelle ou des principes généraux de la responsabilité civile.

En soi, un nom de domaine, ne confère aucun droit de propriété intellectuelle, il ne fait naître aucun droit privatif. Cette solution a été dégagée en droit français en ce qui concerne les codes d'accès Télétel : il a ainsi été jugé que l'usage du code télématique Domi ne pouvait pas être opposé comme antériorité faisant obstacle au dépôt d'une marque Domix[37]. Elle peut être étendue aux noms de domaine.

Un nom de domaine pourra être tenu comme contrefaisant s'il reprend exactement une marque existante ou s'il est similaire à cette marque. Ce principe valable en droit français en ce qui concerne les codes Télétel, a été également appliqué par un juge américain à un nom de domaine[38].

Dans certains cas, chaque partie revendiquant un nom de domaine similaire aura un droit sur le nom de domaine déposé : marques identiques dans des activités différentes, marque pour l'un, raison sociale pour l'autre.

Pour les zones internationales, le NSI va appliquer ses règles de conflit, il est donc important de les connaître, surtout si un dépôt dans la zone <com> est envisagé, ou si vous estimez qu'un dépôt dans cette zone a été effectué en violation de vos droits.

En France, *a priori,* le contrôle exercé sur les noms de domaine par le NIC diminue les risques de conflits potentiels, sans les supprimer, alors même que le rôle exercé par le NIC sur le nommage en France pourrait le placer dans une situation délicate en cas de litige.

Les conflits concernant les noms de domaine

Les conflits de la zone <.com>

Les conflits concernant les noms de domaine peuvent être classés en deux grandes catégories[39] :

> Le nom de domaine porte directement atteinte aux droits d'un tiers.

L'exemple de la société Princeton Review, qui a déposé comme nom de domaine <kaplan.com>, d'après le nom de son principal concurrent, Kaplan Education Center a déjà été cité. La société Princeton a dû abandonner le nom de domaine, mais l'affaire est allée jusqu'en arbitrage.

---

[37] TGI Paris 3ᵉ Ch. 7 Décembre 1994 PIBD 1995, n°584, III, p. 161.

[38] Voir infra affaire "Candyland".

[39] On trouvera de nombreuses informations et de nombreuses références sur les litiges survenus en matière de noms de domaine aux Etats-Unis avec notamment un petit résumé de chaque affaire connue, sur le site Web "What's in a name" : <http://www.law.georgetown.edu/lc/internic/domain1.html>.
Voir aussi le site Web du cabinet d'avocats Oppedahl & Larson : <http://www.patents.com> ou encore des articles de juristes américains sur le sujet :
Dan L. Burk, Trademarks Along the Infobahn : A first look at the Emerging law of Cybermarks, 1 RICH. J.L.&Tech. 1 (1995), disponible à : <http://www.urich.edu/~jolt/vlil/burk.html>.
David G. Post, A Domain by any Other Name, "Plugging In", American Lawyer, May 1996.

Une société Carnetta Wong Associates a déposé le nom <avon.com>. La société Avon a diligenté une procédure devant un tribunal new yorkais pour récupérer le nom.

KCRA, une station de télévision basée à Sacramento, Californie, a enregistré les noms <kvie.com>, <kpwb.com> et <ktxl.com>, les sigles de ses trois concurrents. Son fournisseur d'accès a demandé au NSI de supprimer les noms de domaine lorsqu'il s'est aperçu que les noms étaient source de conflit avec les autres stations de télévision.

Certains ont imaginé déposer comme noms de domaine les noms de personnalités connues, avec parfois l'objectif annoncé de les utiliser pour commercialiser des adresses électroniques telles : <dupont@depardieu.com>. On peut ainsi relever au cours d'une petite recherche effectuée dans les bases de données de l'InterNIC : <melgibson.com>, déposé par un certain McGrath Hill, Arizona ; <madonna.com>, déposé par Scott Seekinns, Mineapolis ; <liz-taylor.com> correspondant au déposant « Marry Me Please! What's More ? », avec une adresse en Floride[40].

Si les noms ont été déposés sans l'autorisation des stars concernées, on peut raisonnablement supposer que le droit américain leur offre un fondement juridique approprié pour faire annuler les noms de domaine.

En droit français, le nom patronymique est un droit de la personne. Le porteur légitime d'un nom peut agir en responsabilité contre l'utilisation abusive de ce nom.

Une société IEG rachète le nom de domaine <candyland.com> et monte un site Web pornographique. Candyland se trouve être une marque déposée de Hasbro, qui vend des jouets pour enfants.

Hasbro a obtenu en justice qu'il soit fait injonction à IEG de cesser d'utiliser le nom de domaine <candyland.com> et le nom candyland. Le juge a accordé à IEG le droit de faire un lien depuis la page d'accueil du site <candyland.com> vers son nouveau site <www.adultplayground.com> pendant 90 jours[41].

Dans une autre série d'hypothèses, le nom choisi peut laisser croire qu'il s'agit du site officiel d'une personne ou d'un organisme, alors qu'il n'en est rien, et engendrer ainsi une confusion.

Par exemple, le site <www.dole96.org> n'est pas l'adresse du site du candidat à la présidence américaine Robert Dole, dont le site officiel se trouve à : <http://www.dole96 .com>.

Le nom de domaine <micros0ft.com> a été déposé par une société informatique texanne Zero Micro Software, créant ainsi la confusion avec la célèbre entreprise Microsoft dont le nom de domaine est <microsoft.com>.

Signalons aussi <taiwan.com>, déposé par Xinhua, agence de presse officielle chinoise…

Le nom de domaine est revendiqué par deux entités qui ont toutes deux un droit sur le nom revendiqué

En 1994, Mark Newton a enregistré le nom de domaine <newton.com> pour un site qui offre du conseil en informatique. Newton est également une marque déposée de la société Apple.

La société RoadRunner Computer Systems utilise le nom de domaine <roadrunner.com>. RoadRunner est une marque déposée de Warner Brothers Inc, qui objecte à l'utilisation du nom de domaine <roadrunner.com> par la société RoadRunner.

Le Women's Wire, une organisation voulant encourager les femmes à être plus actives sur le réseau, dépose le nom de domaine <wire.com>. Le magazine Wired, un des plus célèbres magazines consacré à l'Internet aux Etats-Unis, qui exploite le site <www.wired.com> pré-

[40] Recherche effectuée le 30 Mai 1996 sur la base Whois (http://rs.internic.net/cgi-bin/whois).

[41] Hasbro Inc. v. Internet Entertainment Group Ltd. N° C96-130WD (W.D. Wash. Feb 9, 1995) ; sur cette affaire voir : Jonathan Rosenoer, Famous Trademarks, Cyberlaw, February 1996, <http://www.cyberlaw.com>.

tend que le nom déposé par Women's Wire va entraîner une confusion avec son propre site et lui demande de modifier son nom, ce qui sera finalement fait.

Un fournisseur de services Internet irlandais, Genesis Project Ltd, dépose le nom de domaine <thegap.com> pour son service intitulé « the genesis access point ».

The Gap Inc, société américaine titulaire de la marque fédérale « the gap », proteste auprès du NSI. Les parties se seraient arrangées à l'amiable par la suite.

Fry's Electronic Inc, une chaîne californienne de vente d'électronique au détail, intente une action contre Frenchy Frys, une société basée à Seattle qui vend des friteuses, et qui a déposé avant elle le nom de domaine <frys.com>, qu'elle revendique également.

Digital Consulting, Massachusetts, détient la marque fédérale DCI qu'elle utilise depuis décembre 1986. La société Data Concept's, Tennessee, utilise le nom de domaine <dci.com> depuis août 1993. Il s'agit pour cette deuxième société d'une marque de common law (marque qui s'acquiert par l'usage), qu'elle utilise depuis 1981. Digital, s'appuyant sur sa marque fédérale revendique auprès du NSI le nom de domaine <dci.com>.

La société Regis McKenna a enregistré <regis.com> en 1993. Le même nom de domaine est aujourd'hui également revendiqué par la société Regis Corporation. Il y aurait une douzaine de sociétés comportant le terme « regis » dans leur dénomination aux Etats-Unis.

Clue Computing Inc., une petite société du Colorado, détient le nom de domaine <clue.com>. « Clue » est aussi une marque déposée de Hasbro, le fabricant de jouets.

Suite à l'augmentation du nombre de conflits concernant les noms de domaine, le NSI a élaboré une charte de règlement des litiges.

La Charte du NSI.

Cette charte a déjà été modifiée deux fois. J'examinerai la charte modifiée en vigueur au 9 septembre 1996[42].

Il est précisé dans le formulaire d'enregistrement des noms de domaine que la personne déposant un nom de domaine accepte d'être liée par la charte — Policy Statement[43] — élaborée par le NSI.

Cette charte peut toutefois être modifiée suivant la volonté du NSI, sous la seule condition d'un préavis de 30 jours, posté sur l'Internet à l'adresse suivante : <ftp://ftp.internic.net/policy/internic.domain.policy>.

Les nouvelles règles peuvent donc être appliquées rétroactivement, à des noms de domaine enregistrés avant l'entrée en vigueur des nouvelles dispositions.

La charte prévoit la possibilité pour le titulaire d'une marque fédérale américaine ou d'une marque étrangère de déposer une réclamation auprès du NSI, si sa marque a été enregistrée comme nom de domaine par un tiers postérieurement à l'enregistrement de sa marque.

Le NSI adresse alors une mise en demeure au déposant du nom de domaine de lui fournir sous 30 jours un justificatif au terme duquel il est bien titulaire d'une marque déposée.

Si le déposant peut justifier d'une marque fédérale américaine ou étrangère antérieure à la date de la réclamation, le nom de domaine lui reste attribué.

Si le titulaire du nom de domaine ne possède pas de marque fédérale ou étrangère correspondant à son nom de domaine, le NSI lui demandera d'abandonner ce nom.

S'il accepte, un délai de 90 jours est prévu pour organiser la transition entre le nouveau nom qui lui sera attribué et l'ancien.

[42] Disponible à : <http://rs.internic.net/domain-info/internic-domain-6.html>.
[43] Disponible à : <ftp://rs.internic.net/policy/internic/internic-domain-1.txt>.

S'il refuse, après un délai de 30 jours, le nom de domaine en litige est placé en attente (on hold), c'est-à-dire qu'il n'est utilisable par aucune des parties, jusqu'au jugement d'un tribunal américain ou jusqu'à ce qu'un accord entre les parties intervienne et précise la partie ayant le droit sur le nom de domaine. Cependant, si le réclamant ou le déposant intentent une procédure relative à l'utilisation et à l'enregistrement du nom de domaine en litige, le NSI place le contrôle du nom de domaine sous la garde du tribunal. Il s'agit d'une modification de la procédure résultant de la dernière version de la charte. Auparavant, le NSI plaçait systématiquement le nom de domaine en attente, ce qui obligeait les titulaires de noms de domaine à obtenir très rapidement une injonction du tribunal à l'encontre du NSI de maintenir le nom de domaine actif.

Cette règle de la suspension du nom de domaine en litige a été appliquée dans l'affaire Newton et dans l'affaire « the gap ». Dans l'affaire Fry's, le NSI a refusé d'intervenir car Fry's Electronic n'était pas titulaire d'une marque fédérale.

Dans l'affaire RoadRunner, la société titulaire du nom de domaine s'est empressée de déposer une marque en Tunisie, pays où l'enregistrement était le plus rapide (la charte du NSI a été modifiée sur ce point et prévoit maintenant que la marque doit avoir été déposée avant la réclamation), et a démarré une procédure contre le NSI le 26 mars 1996 afin de demander, entre autres que le NSI élabore de nouvelles règles assurant un traitement équitable des propriétaires de noms de domaine, lorsque surviennent des conflits en matière de marques et surtout que NSI cesse d'agir de manière arbitraire et capricieuse lorsqu'il interprète les règles relatives à l'enregistrement des noms de domaine et publie ses critères d'interprétation. Trois mois après le début de cette procédure, l'affaire a été classée à la demande du NSI, la société RoadRunner Computer Systems conservant son nom de domaine intact[44].

Dans l'affaire DCI, la société Data a immédiatement saisi le juge d'une action en contrefaçon contre la société Digital (la lettre du NSI lui demandant d'abandonner le nom de domaine date du 17 Avril 1996, et la procédure en contrefaçon a été initiée le 8 Mai 1996) et d'une demande d'injonction contre le NSI. Le NSI a finalement accepté le 24 Mai 1996 de ne pas suspendre le nom de domaine dans l'attente du résultat de la procédure en contrefaçon[45].

Dans l'affaire « Clue », la société Clue Computing a obtenu une injonction du tribunal ordonnant au NSI de laisser son nom de domaine actif[46].

Une entreprise française n'est pas à l'abri d'une telle mésaventure, si une personne est titulaire aux Etats-Unis d'une marque fédérale identique au nom de domaine qu'elle avait choisi.

En principe, une entreprise française titulaire d'une marque déposée en France peut faire une réclamation auprès du NSI contre une entreprise américaine, française ou étrangère qui aurait enregistré dans la zone <com> un nom de domaine similaire à la marque française sans être titulaire d'une marque fédérale américaine ou étrangère. Si une procédure en contrefaçon s'avère nécessaire, le processus peut être lourd : il faudra soit diligenter une procédure aux Etats-Unis, soit obtenir une reconnaissance de la décision étrangère devant les tribunaux américains.

Si le litige concerne des parties et des marques françaises, il va être plus pratique et plus efficace de saisir les tribunaux français. La société de services télématiques Atlantel, détentrice du nom de domaine <atlantel.fr> a ainsi demandé en référé au Tribunal de grande instance de Bordeaux de condamner une société Icare à retirer le nom de domaine <atlantel.com>[47].

---

[44] Sur cette affaire voir : <http://www.patents.com/nsi.sht>.

[45] Sur cette affaire voir : InfoLawAlert : <http://infolawalert.com/source/src061496_dc_intro.html>, ainsi que Oppedahl & Larson Patent Law Web Server : <http://ww.patents.com/nsi.sht>.

[46] Voir : <http://www.clue.com/legal/index.html>.

[47] « Micmac bordelais dans les noms de domaine », *Planète Internet* n° 11, septembre 1996, p.6.

La charte du NSI est très critiquée.

Elle ne prend pas en compte les marques de « common law », qui s'acquièrent par l'usage en droit américain, ou les marques enregistrées dans les Etats fédérés, ainsi que les autres signes distinctifs. Elle ne prend pas en compte le fait que plusieurs personnes peuvent utiliser le même nom.

En outre, le titulaire d'une marque fédérale peut forcer le NSI à suspendre un nom de domaine, sans avoir à démontrer qu'il y a risque de confusion, sans avoir à prouver que le maintien du nom de domaine lui cause un dommage irréparable (irreparable harm) ou des chances raisonnables de succès (likelihood of success), des conditions exigées en droit américain pour obtenir une injonction d'un tribunal.

En droit français, un signe portant atteinte à un nom commercial ou à une enseigne connue sur l'ensemble du territoire national ne peut pas être adopté comme marque s'il existe un risque de confusion dans l'esprit du public.

Une marque ne peut pas porter atteinte à une dénomination sociale antérieure s'il existe un risque de confusion[48].

De même en droit américain, il n'y a pas de contrefaçon si la dénomination sociale est antérieure à la marque et qu'il n'y a pas risque de confusion.

La marque ne prime donc pas systématiquement sur la dénomination sociale.

Les règles élaborées par le NSI, qui donnent à une personne la possibilité de faire suspendre un nom de domaine sans autre condition que la preuve qu'il détient une marque fédérale ou nationale dûment enregistrée, ne sont pas conformes aux principes généraux régissant le droit des marques qui prend également en compte les antériorités des dénominations sociales et le risque de confusion.

De plus le droit des marques ne va pas pouvoir résoudre tous les litiges concernant les noms de domaine.

En droit des marques, on applique le principe de la spécialité : la marque n'est appropriée que pour les produits et services désignés à l'acte de dépôt. Seul le dépôt d'une marque pour des produits et services identiques ou présentant une certaine similitude est prohibé.

En droit américain, c'est le critère de l'absence de confusion[49].

Par exemple, coexistent sans problème les stylos Mont Blanc et la crème Mont Blanc, mais un seul <montblanc> pourra être déposé dans la même zone (<.com> ou <.fr>).

Le même problème peut d'ailleurs se poser avec les dénominations sociales.

Faites une recherche dans l'annuaire sur le nom Lefebvre, par exemple dans les Hauts-de-Seine. Parmi les professionnels, vous trouverez les Editions Francis Lefebvre, la Maison Lefebvre (fleurs), une infirmière, un médecin, une entreprise de bâtiment…

Un autre principe est celui de la territorialité. En France, les seules antériorités opposables sont celles des marques et autres signes qui sont protégés sur le territoire français. La marque déposée en France peut coexister avec une marque identique déposée à l'étranger.

Un principe qui, appliqué aux noms de domaines, atteint ses limites, puisque n'importe quelle entité, sans condition de nationalité, peut enregistrer des noms dans la zone <com>.

Certes les marques notoires voient leur protection étendue au-delà de leur activité : « l'emploi d'une marque jouissant d'une renommée pour des produits ou services non similaires à ceux désignés dans l'enregistrement engage la responsabilité civile de son auteur s'il

[48] Article L711-4 du Code de la propriété intellectuelle.
[49] Mark E., Trademark Wars in Cyberspace, Dr.Dobb's Sourcebook, November-December 1995.

est de nature à porter préjudice au propriétaire de la marque ou si cet emploi constitue une exploitation injustifiée de cette dernière »[50].

En droit américain, le Federal Trademark Dilution Act de 1995 permet désormais au titulaire d'une marque connue d'invoquer que l'utilisation d'un signe par un tiers « dilue », porte atteinte au caractère distinctif de sa propre marque, même si l'utilisation du signe par le tiers n'est pas susceptible de créer une confusion dans l'esprit du public.

C'est le principe posé par cette loi qui a été invoqué avec succès par Hasbro dans l'affaire Candyland.

Mais comment ce principe va-t-il être appliqué dans le cas d'un conflit entre une marque américaine connue nationalement et une marque similaire étrangère ?

N'y a-t-il pas un risque qu'il soit fait interdiction à une société non américaine d'utilisesr un nom de domaine similaire à une marque américaine ? Certaines décisions américaines ont fait une application extra-territoriale du droit des marques si le commerce de la société étrangère a un effet sur le commerce américain[51]. Les noms de domaine de la zone <.com> étant gérés aux Etats-Unis, ils se trouvent *de facto* soumis au droit américain.

Les conflits de la zone <.fr>

Pour les noms de domaine de la zone <.fr>, le contrôle effectué par le NIC élimine les cas de fraude manifeste. Par exemple, il ne vous sera pas possible d'enregistrer comme nom de domaine la dénomination sociale de votre concurrent.

Cependant, ces règles n'éliminent pas tous les conflits potentiels car il n'existe pas de principe de spécialité pour les noms de domaine.

Des conflits pour revendiquer le même nom de domaine entre marques similaires désignant des produits différents peuvent tout à fait survenir.

On peut imaginer également qu'une partie enregistre une marque pour obtenir le nom de domaine correspondant, mais que ce dépôt porte atteinte à une marque existante.

Le NIC-France n'est, en effet, pas juge de la validité et de la disponibilité de la marque correspondant au nom de domaine choisi.

D'un autre côté, les règles du NIC, qui ne reconnaissent pas la possibilité de déposer comme nom de domaine un nom commercial ou une enseigne, vont obliger dans un certain nombre de cas le requérant à déposer une marque.

Le précédent des codes Télétel montre que des litiges peuvent survenir et qu'il ne s'agit pas d'hypothèse d'école.

Par exemple, des marques déposées afin de désigner des codes d'accès pour des services Minitel en rapport avec le tourisme on pu être jugées contrefaisantes avec des marques existantes, désignant également une activité de tourisme[52].

Le fait d'utiliser le sous-domaine <tm> pour les marques déposées n'est pas un fait exonérateur de contrefaçon, si la marque utilisée s'avère similaire à une dénomination sociale existante et est susceptible de créer une confusion dans l'esprit du public.

---

[50] Article L713-5 du Code de la propriété intellectuelle.
[51] Nancy Dix and Allyn Taylor, Cyberpsace Names receive limited protection in US, IP Worldwide, July, August 1996, p.21.
[52] Paris, 4e Ch. 29 Mars 1993, PIBD, n°548, III-459.

Les précautions à prendre dans le choix d'un nom de domaine

L'examen des affaires américaines montre qu'il peut être prudent de déposer la marque correspondant au nom de domaine choisi, surtout pour les zones internationales où s'applique la règle du « premier venu, premier servi », et même si le nom est celui de la dénomination sociale du déposant.

Compte tenu du rôle joué par le droit des marques dans la résolution des conflits, il apparaît important de consolider le nom de domaine par un dépôt de marque. Une marque enregistrée sera plus facilement prise en compte par le NSI ou par un juge américain en cas de litige qu'un simple nom commercial.

En France, si le nom choisi n'est pas la dénomination du déposant, un dépôt de marque est imposé par les règles du NIC. Cette fois le dépôt ne sert pas à consolider un nom, il est la condition nécessaire de la création du domaine.

Quelques principes de base doivent être respectés dans le choix d'une marque.

Une marque pour pouvoir être déposée doit être disponible, c'est-à-dire ne pas porter atteinte à une marque déjà existante, ou à un droit antérieur. Elle ne devra pas constituer l'imitation du nom commercial d'un tiers susceptible de constituer un acte de concurrence déloyale.

La disponibilité s'apprécie au regard du principe de spécialité, sous réserve du cas des marques notoires.

Pour vérifier cette disponibilité, il est conseillé d'effectuer une recherche d'antériorité auprès de l'INPI (Institut national de la propriété intellectuelle)[53].

La marque ne doit pas être déceptive, c'est-à-dire de nature à tromper le public sur les qualités du produit qu'elle désigne.

La marque doit également être distinctive, c'est-à-dire ne pas être constituée par des termes usuels servant à désigner le produit sur lequel elle porte ou sur ces caractéristiques. Par exemple « informatique » ne peut pas être déposé pour des ordinateurs.

L'enregistrement de la marque suppose le dépôt d'un formulaire de demande d'enregistrement auprès de l'INPI[54], avec indication de la liste des produits et services pour lesquels la protection est sollicitée et des classes correspondantes.

La classification des produits et services est une classification internationale.

Cependant cette classification n'a qu'un but pratique, la protection de la marque est déterminée par l'énumération des produits et services et non par référence à la classe administrative[55].

Il est donc important de soigner la désignation des produits et services.

Un dépôt doit évidemment être effectué dans la classe correspondant aux produits auxquels est consacré le site envisagé. Par exemple, pour un site Web fournissant des informations commerciales, il faudrait un dépôt en classe 35 (publicité, affaires).

La tendance est d'enregistrer systématiquement les marques qui vont servir à désigner un code Télétel dans la classe 38, télécommunications.

---

[53] Pour les recherches d'antériorité, s'adresser à : INPI, Division des marques, 32 rue des Trois Fontanots, 92016 Nanterre, tél. : 01 46 92 58 00, fax : 01 46 92 58 94; recherche par Minitel ICI Marques : 36 29 36 30.
Sur le droit des marques en général, voir : Azéma J. Les marques de fabrique, de commerce et de service, Lamy droit commercial 1996 n° 1994 et suivants, Chavannes A. et Burst J.J., Droit de la propriété intellectuelle, Précis Dalloz 4e édition 1994.

[54] Direction Générale : 26 bis, rue de Saint Petersbourg, 75008 Paris, tél. : 01 42 94 52 52, fax : 01 42 93 59 30, Minitel : 3615 INPI.

[55] Lamy droit commercial 1996, n° 2061.

Cependant, le dépôt dans la classe 38 pour obtenir un nom de domaine ne doit pas porter atteinte à des marques déjà déposées pour désigner des produits et services spécifiques dans d'autres classes, même si lesdites marques n'ont pas été déposées dans la classe 38. Par exemple, la marque Joker déposée en classe 38 et le code 3615 Joker pour des jeux télématiques ont été jugés contrefaisants de la marque Joker déposée antérieurement pour des jeux dans la classe 28[56].

A titre comparatif, on peut noter que pour le Bureau des marques (Trademark Office) américain, les services de la classe 38 désignent seulement le procédé technique de communication. Un service qui offre des informations incidemment fournies par un moyen de télécommunication n'a pas à être enregistré dans la classe 38. Ainsi, même des fournisseurs de services en ligne comme Compuserve ou Prodigy ont vu leur marque enregistrée dans la classe 42 avec comme activité : fourniture d'accès multiples à un réseau informatique global[57].

On peut aussi envisager un dépôt dans la classe 42 qui couvre « la programmation pour ordinateurs ».

Compte tenu du caractère global de l'Internet, on peut également vouloir effectuer un dépôt international.

Depuis le 1er Janvier 1996, il est possible de déposer une marque communautaire, qui permet d'obtenir une protection dans l'ensemble des pays de la Communauté. Les demandes doivent être déposées auprès de l'Office d'harmonisation dans le marché intérieur des marques, dessins et modèles[58].

L'arrangement de Madrid du 14 Avril 1891 a permis la mise en place d'un système de protection d'enregistrement international des marques afin de faciliter leur protection dans plusieurs pays.

Une fois titulaire d'une marque française, il vous est possible d'adresser une demande d'extension à l'INPI qui transmet à l'OMPI (Organisation mondiale de la propriété Industrielle). L'enregistrement international produit les mêmes effets qu'un dépôt national dans tous les pays adhérents désignés. Les autorités compétentes de chaque pays dans lesquels la protection est demandée examinent la régularité du dépôt au regard de leurs lois nationales.

Cependant les pays anglo-saxons, dont les Etats-Unis, ne figurent pas parmi les pays adhérents à cette convention.

Si un dépôt aux Etats-Unis, où siège l'organisme responsable de l'attribution des noms de domaine de la zone <com>, est envisagé, il n'est donc pas possible de recourir à la procédure d'arrangement de Madrid. Un dépôt devra directement y être effectué.

La Convention de l'union de Paris du 20 Mars 1883, dont sont adhérents cette fois les Etats-Unis, a institué un mécanisme de priorité qui consiste à ouvrir au déposant d'une première demande d'enregistrement dans un pays de l'Union un délai de 6 mois pour procéder à des dépôts dans d'autres pays membres de l'Union. Les effets des dépôts étrangers rétroagissent à la date du dépôt initial.

Perspectives

L'utilisation de la marque d'autrui comme nom de domaine peut constituer une contrefaçon. On considère ainsi que les noms de domaine peuvent créer une atteinte sur la nature du pro-

[56] Paris 4e Ch.16 février 1995, PIBDn°587, III-248.
[57] "Registration of domain names in the trademark office", disponible à : <http://www.uspto.goc/web/uspto/info/domain.html>.
[58] OHMI, avenida de Aguilera, 20, E-3090 Alicante Espagne, fax : 34-6 513 9173.

duit, l'identité de la personne ou l'organisation trouvée à l'adresse correspondante. Or, à l'origine, un nom de domaine est la traduction alphanumérique d'un numéro de machine, il a une fonction d'adressage.

Les ingénieurs qui ont mis en place le système n'avaient l'intention ni de faire en sorte que les noms de domaine puissent servir à l'identification des produits et services, ni d'en faire un outil de recherche.

En outre, à la différence des marques et autres signes distinctifs, un nom de domaine ne permet pas les nuances géographiques ou par activité. Le système actuel ne va pas pouvoir satisfaire tous les titulaires de marques sans compter les dénominations sociales et autres signes distinctifs. Les noms de domaine sont uniques internationalement, alors que les signes distinctifs ne sont pas nécessairement uniques et qu'il n'existe pas de marque internationale.

Des services de surveillance, comme Markwatch[59], ont vu le jour, qui permettent à leurs clients de surveiller le contenu des sites Web, newsgroups et bases de données des noms de domaines afin de s'assurer que leurs marques ne sont pas contrefaites sur l'Internet, une possibilité qui ne devrait pas tarder à déclencher les premiers litiges internationaux de marques.

La croissance exponentielle des noms de domaine va nécessiter à plus ou moins long terme la création de sous-domaines dans la zone <com> ou de nouvelles zones. Il est actuellement envisagé de créer des nouveaux domaines internationaux dont la gestion serait confiée à des sociétés privées afin d'éviter la constitution de monopoles[60].

Des solutions vont devoir être trouvées pour concilier tous les intérêts en présence. Il n'est pas impossible que dans le futur on soit obligé de changer les caractéristiques ou les attributs des noms de domaine pour répondre aux besoins de connectivité et d'adressage du futur Internet.

S'il est important de déposer un nom de domaine pour des raisons de stabilité, et s'il peut être envisagé dans certains cas de compléter ce dépôt par un dépôt de marques, il ne faut pas non plus se focaliser si le nom que vous envisagiez de prendre a déjà été enregistré, hormis les cas où il y un préjudice certain (confusion, marque notoire, concurrence déloyale).

Le seul fait d'utiliser comme nom de domaine le nom d'une autre société ne crée pas nécessairement de confusion, si les produits et services concernés sont différents.

La complexité croissante du nommage de la zone <.fr> peut également amener à envisager le dépôt d'un nom comme sous-domaine d'un autre.

Pour les organisations à but non lucratif, il est ainsi possible de déposer, sous certaines conditions, des sous-domaines gratuits de <eu.org>[61] pour la France ou <ml.org>[62] pour les

---

[59] Site Web : <http://www.markwatch.com>.

[60] Jon Postel, New Registries and the Delegation of International Top Level Domains, Internet-Draft, disponible à : <ftp://ds.internic.net/internet-drafts/draft-postel-iana-itld-admin-01.txt>, juin 1996.
Voir aussi : Robert Shaw, Les Noms de Domaine : De qui est-ce le domaine ?, présenté lors du débat OCDE/EC DG XIII/COMTEC sur "Access and Pricing for Information Infrastructures Services : Communication Tariffication, Regulation and the Internet", Trinity College, Dublin, Irlande, 20-21 juin 1996, traduction française de Laurent Chemla, disponible à : <http://www.aui.fr/Groupes/GT-DRE/dns-shaw.html>.

[61] Site Web : <http://www.eu.org>.

[62] Site Web :<http://www.ml.org>.

Etats-Unis. Enregistrer le domaine <nom.asso.fr> est-il vraiment plus important que d'avoir le domaine <nom.eu.org> ?

La réglementation des services Internet

Les services qui véhiculent des messages destinés à une ou plusieurs personnes déterminées et individualisées relèvent du régime de la correspondance privée. Les autres services dits publics relèvent du régime de l'audiovisuel.

Concernant les services de communication Internet, la frontière entre ces deux régimes ne va pas toujours être aisée à tracer.

En effet, un service Internet peut se définir comme « un service automatique de transmission de l'information, utilisant un protocole informatique donné ». Un même protocole peut à la fois servir à véhiculer des informations de nature privée ou de nature publique, selon les circonstances.

Par exemple, le courrier électronique est aussi bien utilisé pour véhiculer les correspondances privées que pour effectuer des communications publiques au sens de la loi.

Quelles que soient les difficultés que cette distinction entre communication publique et privée puisse susciter quant à son application aux services Internet, elle implique deux régimes juridiques bien distincts.

Première partie

La réglementation des services de communication privée

Le régime de la correspondance privée

Le principe du secret des correspondances émises par la voie des télécommunications

Divers principes protègent le secret des correspondances : principe de protection de la vie privée, lois relatives au secret professionnel notamment. L'article 8 de la Convention européenne des droits de l'homme rappelle que « toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance »[63].

La loi du 10 juillet 1991[64] a consacré le secret des correspondances émises par la voie des télécommunications :

« Le secret des correspondances émises par la voie des télécommunications est garanti par la loi. Il ne peut être porté atteinte à ce secret que par l'autorité publique, dans les seuls cas de nécessité d'intérêt public prévus par la loi et dans les limites fixées par celle-ci. »

Une télécommunication est elle-même définie comme « toute transmission, émission ou réception de signes, signaux, d'écrits, d'images, de sons ou de renseignements de toute nature par fil, optique, radioélectricité ou autres systèmes électromagnétiques »[65].

Le champ d'application de la loi du 10 juillet est large : il n'est pas limité aux seules correspondances téléphoniques, mais englobe toutes les correspondances transitant par les réseaux de télécommunications, y compris les réseaux informatiques. Le terme de correspondance vise toutes les formes de communication, et pas seulement les messages écrits. La loi du 10 juillet 1990 a donc vocation à s'appliquer aux échanges sur l'Internet[66].

Les correspondances concernées

Sont protégées toutes les correspondances émises par la voie des télécommunications. Cependant, bien que cela ne soit pas précisé par le texte, il faut également que la correspondance ait un caractère privé. En effet, les données mises à disposition du « public »

[63] Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales du 4 novembre 1950.
[64] Loi n° 91-646 du 10 juillet 1996 relative au secret des correspondances émises par la voie des télécommunications.
[65] Article 32 du CPT.
[66] Alain Bensoussan (sous la direction de),Internet aspects juridiques, Hermès 1996, p.85.

ou d'une « catégorie de public » ne sont évidemment pas protégées par le secret des correspondances mais relèvent de la loi sur l'audiovisuel.

Pour qu'une communication soit considérée comme privée, il faut qu'elle soit personnelle et individualisée.

Il a ainsi été jugé, en matière de messageries roses sur Minitel, qu'étaient publics les messages accessibles à un nombre indéterminé de personnes[67].

Une circulaire du 17 février 1988[68] précise qu'il y a correspondance privée lorsque le « message est exclusivement destiné à une (ou plusieurs) personne, physique ou morale, déterminée ou individualisée ».

La difficulté en ce qui concerne les services Internet est de définir ce qui relève de la correspondance privée.

Les messages échangés par courrier électronique doivent être considérés comme des correspondances privées puisque le courrier transmis ne doit être lu que par le titulaire du compte correspondant à l'adresse électronique du destinataire.

Les logiciels de courrier électronique permettent également d'adresser le même message à plusieurs personnes en même temps.

Les listes de diffusion ouvertes sont une sorte de variante des groupes de discussions publiques, mais qui permettent de recevoir directement les nouveaux messages dans sa boîte aux lettres électronique. Les messages de certaines listes sont au surplus archivés sur des sites publics. Dans cette hypothèse, il y a communication audiovisuelle au sens de la loi : les messages peuvent être lus par un nombre indéterminé de personnes.

Entre la messagerie électronique, entre deux correspondants déterminés et la liste de diffusion dont l'accès est ouvert à toute personne s'y abonnant, il y a des situations intermédiaires : messages envoyés à plusieurs personnes en utilisant la fonction copie du courrier électronique, listes de diffusion fermées, dont l'accès est réservé à certaines personnes.

Par exemple, il existe une liste de diffusion dédiée aux magistrats francophones[69]. L'idée est de permettre à des magistrats, tenus par le devoir de réserve, de pouvoir communiquer librement entre eux. Une telle liste relève-t-elle de la correspondance privée ou du service audiovisuel ?

Les newsgroups peuvent être lus librement par toute personne ayant accès à Usenet. Les messages postés dans ces forums ne relèvent donc manifestement pas du régime de la correspondance privée.

L'IRC permet de correspondre simultanément avec plusieurs personnes en temps réel. Savoir si la communication relève de la correspondance privée ou de l'audiovisuel va dépendre de la question de savoir si les messages peuvent être lus par un nombre déterminé ou indéterminé de personnes.

En pratique, la frontière entre les deux catégories va s'avérer dans bien des cas floue et incertaine.

Un serveur Web est le type même de l'application multimédia à laquelle la définition de la communication audiovisuelle semble parfaitement s'adapter. Mais si le service Web est utilisé pour des services de téléachat, la transaction constitue une communication privée : l'utilisateur du service entre dans une relation « personnelle » avec l'entreprise qui fournit le service.

---

[67] Crim. 17 novembre 1992, Petites Affiches 1993, n°44, p.4.
[68] JO du 9 mars 1988.
[69] Jugenet, Site Web : <http://www.DROIT.UMontreal.CA/~laliberte/Justiciers/Juges/abonnement.html>.

Quant aux communications téléphoniques via l'Internet, elles sont comme les communications téléphoniques traditionnelles, couvertes par le secret des télécommunications.

On voit à travers ces exemples que la distinction entre communication audiovisuelle et correspondance privée n'est pas toujours aisée. Il est néanmoins un principe important : les correspondances échangées entre personnes déterminées par courrier électronique sont couvertes par le secret des télécommunications.

Les personnes soumises à l'obligation au secret

Le secret des correspondances doit être respecté par l'exploitant public lui-même, France Télécom, par les opérateurs de réseaux publics ainsi que par tout fournisseur d'un service de télécommunications (article L32-3 du CPT).

Les fournisseurs d'accès relèvent de la catégorie des fournisseurs de services de télécommunications[70].

Le secret des correspondances doit également être respecté par les salariés ou agents des exploitants des réseaux et fournisseurs de service de télécommunications, c'est-à-dire par toute personne relevant de l'autorité desdits exploitants, quel que soit son statut (article L32-3 et L41 du CPT).

Ces trois catégories (France Télécom, les opérateurs de réseaux et les fournisseurs de services de télécommunications) ainsi que les personnes dépositaires de l'autorité publique, lorsque « agissant dans l'exercice de leurs fonctions, ordonnent, commettent ou facilitent, hors des cas prévus par la loi, l'interception ou le détournement des correspondances émises, transmises ou reçues par la voie des télécommunications, l'utilisation ou la divulgation de leur contenu », sont passibles d'une peine de 3 ans d'emprisonnement et de 300 000 francs d'amende[71].

Un autre texte du Code pénal, d'application générale et qui n'est pas limité à certaines catégories d'exploitants ou aux fournisseurs de services de télécommunications prévoit que « le fait commis de mauvaise foi d'intercepter, de détourner, d'utiliser ou de divulguer des correspondances émises, transmises ou reçues par la voie des télécommunications ou de procéder à l'installation d'appareils conçus pour réaliser de telles interceptions » est puni d'un an d'emprisonnement et de 300 000 francs d'amende[72].

Toute personne concourant à la transmission des données à travers les réseaux informatiques (opérateurs, fournisseurs d'accès, administrateurs systèmes…) est donc soumise directement ou indirectement à l'obligation de respect du secret des correspondances.

Les faits visés sont larges puisque sont condamnés aussi bien les actes d'interception, de détournement, ou de divulgation du contenu des correspondances. Le problème qui se pose pour les fournisseurs d'accès est que dans le cadre de l'exercice de leurs fonctions, de la surveillance du système de communication, ils peuvent être amenés à prendre connaissance des correspondances transitant par leurs serveurs. Cela est très fréquent en pratique.

Sont réprimées les intrusions volontaires dans une correspondance privée. Mais si l'intrusion est justifiée par une nécessité technique, il n'y aurait pas d'infraction de violation du secret des correspondances [73].

Cette distinction proposée par un auteur est inspirée des droits américains et canadiens dont les législations concernant la confidentialité des communications fournissent aux opérateurs de systèmes de fréquentes exceptions à la prohibition d'interception de communications

[70] Voir supra
[71] Article 432-9 du Code pénal.
[72] Article 226-15 du Code pénal.
[73] O. Hance, Business et Droit d'Internet, Best Of Editions 1996, p. 110.

privées, notamment lorsque la surveillance est nécessaire à la bonne administration du système informatique[74].

En droit français, cette distinction pourrait être fondée sur un principe du droit pénal qui veut qu'il n'y ait point de crime ou de délit sans intention de le commettre, sans volonté délibérée[75].

Le régime des interceptions

Une fois posé le principe du secret des correspondances par la voie des télécommunications, la loi du 10 juillet 1991 définit les cas et conditions dans lesquelles il peut être porté atteinte à ce secret.

En premier lieu un juge d'instruction, si la peine encourue pour les faits que le juge instruit est supérieure à 2 ans d'emprisonnement, peut « lorsque les nécessités de l'information l'exigent, prescrire l'interception, l'enregistrement et la transcription de correspondances émises par la voie des télécommunications ».

En second lieu, la loi organise les modalités des interceptions de sécurité dites écoutes administratives. Ces interceptions peuvent être réalisées sur autorisation du Premier ministre lorsqu'elles ont pour objet de rechercher des renseignements intéressant la sécurité nationale, la sauvegarde des éléments essentiels du potentiel scientifique et économique de la France, la prévention du terrorisme ou de la criminalité organisée. La CNCIS, Commission nationale de contrôle des interceptions de sécurité, a été instituée pour veiller au respect de la légalité des interceptions de sécurité.

Ce régime légal des interceptions est-il applicable aux échanges réalisées sur l'Internet ?

La réponse devrait être affirmative chaque fois que la communication, l'échange relève du régime de la correspondance privée.

Pourtant la secrétaire générale de la CNCIS, interviewée par le journal *Planète Internet*[76] indique que « ce qui passe par l'Internet, comme sur le réseau hertzien, ne nous concerne pas ».

Il est exact que les dispositions de la loi concernant les interceptions ne sont pas applicables à la surveillance et au contrôle des transmissions empruntant la voie hertzienne effectuées par les pouvoirs publics pour la défense des intérêts nationaux[77].

Mais les communications transitant par l'Internet n'empruntent pas nécessairement la voie hertzienne, elles utilisent toutes les ressources des réseaux : fils, câbles, satellites…

En réalité, si la loi du 10 juillet 1991, qui pose le principe du secret des correspondances émises par la voie des télécommunications, est applicable aux correspondances échangées sur l'Internet, il est bien évident que les dispositions de cette loi relatives aux interceptions s'appliquent également.

La CNCIS pourrait se reconnaître compétente pour vérifier les interceptions de sécurité relatives à des échanges sur l'Internet[78].

[74] Idem, p. 115.
[75] Article 121-3 du Code pénal.
[76] Septembre-octobre 1995, n° 3, p.9.
[77] Article 20 de la loi du 10 juillet 1991.
[78] Alain Bensoussan (sous la direction de), Internet aspects juridiques, Hermès 1996, p.90.

La surveillance électronique des salariés

Les nouvelles technologies sont de plus en plus couramment utilisées à des fins de contrôle du travail des salariés dans les entreprises. Pour cela, l'entreprise dispose de moyens de plus en plus sophistiqués.

L'écoute téléphonique des salariés est courante sur certains lieux de travail, dans les salles de marché et de vente, dans les systèmes de réservation, dans les sociétés de vente par correspondance, écoutes justifiées par la conservation de la preuve que les prestations ont été correctement exécutées. On assiste également à l'apparition de caméras de vidéosurveillance sur les lieux de travail, dans les entreprise privées[79].

La CNIL, Commission nationale informatique et libertés, dénonce les risques de surveillance des salariés, tant dans leur présence, dans leur productivité que dans leur personnalité : abandon de la frontière entre vie privée et vie professionnelle avec le téléphone portable qui autorise les appels en tous lieux et à toute heure, enregistrement des données sur la destination et la durée des appels téléphoniques passés par les salariés, comptage automatique du temps passé par tâche…[80]

De nombreuses personnes ont accès à l'Internet dans le cadre de leurs activités professionnelles. L'Internet n'échappera pas à ces pratiques de surveillance, comme en témoigne ce qui se passe déjà aux Etats-Unis.

Des logiciels permettent aux employeurs de surveiller ce que font leurs salariés pendant qu'ils sont connectés : les sites Web visités, le temps passé, le type de fichiers téléchargés. Parmi les procédés qui font l'objet d'une surveillance, le courrier électronique occupe une place de choix. Selon une enquête conduite en décembre 1995 par the « Society for Human Resource Management », 36 % des organisations qui fournissent des services de courrier électronique regardent les courriers de leurs salariés pour des motifs liés à la conservation de la preuve ou des raisons de sécurité, 75 % estiment que les employés ont le droit de lire les courriers électroniques fournis par la société[81].

Il faut dire que les systèmes informatiques rendent particulièrement aisée la surveillance des courriers électroniques : certains systèmes sont programmés afin de conserver automatiquement une copie de tous les messages reçus ou envoyés, d'autres conservent la copie des courriers dans leurs disques durs, même si l'utilisateur croit les avoir effacés. Avec une procédure dite de « back-up », il est possible de récupérer les courriers se trouvant stockés sur le disque dur. Ainsi des courriers électroniques échangés entre Olivier North et John Poindexter qui communiquaient à travers le système de messagerie du National Security Council et que ces derniers pensaient avoir effacés, avaient été préservés par un tel procédé et ont été utilisés dans l'affaire Iran-Contra[82].

Lorsqu' un salarié bénéficie d'un accès à l'Internet, il peut être amené à utiliser les moyens de communication privée offerts et notamment le courrier électronique à des fins personnelles, de la même manière que le téléphone n'est généralement pas exclusivement consacré aux conversations d'ordre professionnel.

Certes le salarié qui reçoit des lettres à caractère professionnel ne peut pas opposer le secret des correspondances à son employeur[83], mais le seul fait qu'une correspondance de nature privée soit adressée à un salarié sur son lieu de travail n'autorise pas l'employeur à la soustraire ou à la retenir de façon indue[84].

---

[79] Voix, image et protection des données personnelles, Rapport de la CNIL, Documentation française 1996, p.41.
[80] Présentation à la presse du 16ème rapport de la CNIL par M. J. Fauvet, Président, le 8 juillet 1996.
[81] Suzan Stellin, Who's watching you on line, C/Net, <http://www.cnet.com/Content/Features/Dlife/Privacy>, 1996.
[82] Cité par Robert L. Jones, Client Confidentiality : A Lawyer's Duties with regard to Internet e-mail, <http://www.kuesterlaw.com/netethics/bjones.htm>, 16 août 1995, note n°4.
[83] Crim. 16 janvier 1992, Dr. Pénal 1992, n°170.
[84] Crim. 18 juillet 1973, Bull. Crim., n°336.

Tôt ou tard, la question de la légalité du contrôle de l'utilisation des services de communication Internet par le salarié va se poser.

J'examinerai plus particulièrement la question du contrôle du courrier électronique, le moyen le plus utilisé pour échanger des correspondances sur l'Internet.

L'employeur peut-il surveiller les courriers électroniques de ses salariés ? L'usage abusif du courrier électronique par un salarié peut-il servir de fondement à un licenciement ? Les courriers électroniques peuvent-ils être utilisés comme preuve dans le cadre d'une procédure de licenciement ?

Ces types de problèmes ont déjà été soumis à des juges américains.

Une société qui avait mis à disposition de ses salariés une messagerie électronique leur assure que toutes les communications par courrier électronique seront confidentielles (confidential and privileged) et qu'elles ne seront pas interceptées et utilisées à l'encontre des salariés comme motif de licenciement et d'avertissement.

Contrairement à ces promesses, les courriers électroniques d'un salarié sont interceptés et il est licencié pour avoir tenu des propos désobligeants sur la société dans lesdits courriers électroniques.

Le salarié licencié a invoqué l'atteinte à sa vie privée devant le tribunal. Par une décision du 18 janvier 1996, il est débouté de sa demande[85]. Pour le juge, on ne peut s'attendre à ce que les communications par courrier électronique volontairement adressées par un salarié à son supérieur sur la messagerie de la société aient un caractère privé malgré l'assurance que de telles communications ne seraient pas interceptées par la direction. Le tribunal ne trouve pas qu'une personne raisonnable doive considérer l'interception des communications par l'employeur comme une atteinte substantielle et manifeste à son intimité. Enfin, le juge estime que l'intérêt de la société à prévenir critiques et dénigrement à son égard et même des activités illégales sur le système de messagerie l'emporte sur les intérêts privés de ses employés.

Dans une autre affaire, une salariée a assigné sa société qui conservait une copie de tous les messages émis et reçus, pour atteinte à sa vie privée[86]. Le tribunal californien saisi a considéré que le courrier électronique n'était pas couvert par la loi relative aux écoutes téléphoniques, et que le droit à la vie privée garanti par la Constitution de l'Etat de Californie couvre les informations de nature personnelle mais non professionnelle.

Il faut également citer le cas d'Eugène Wang, ancien vice-président de la société Borland International qui fut accusé en 1993 d'avoir divulgué des informations confidentielles par courrier électronique à la société concurrente CEO Gordon Eubanks peu de temps avant son départ pour cette société.

Les décisions évoquées seraient-elles envisageables en droit français ?

Il n'existe pas encore de décisions de jurisprudence ou de textes concernant le contrôle du courrier électronique dans l'entreprise. Il existe en revanche des règles qui s'imposent à l'employeur qui veut mettre en place des procédés de contrôle de ses salariés comme la vidéosurveillance, les autocommutateurs, les écoutes téléphoniques. Ces règles peuvent servir de lignes directrices sur l'attitude à adopter et les précautions à prendre en matière de contrôle des courriers électroniques.

[85] Michael A. Smyth v.The Pillsbury Company, C.A. N.O. 95-5712, US dictrict Court for the eastern district of Pennsylvania, disponible à :<http://www.epic.org/privacy/internet/smyth_v_pillsbury.html>.

[86] Flanagan et al.vs.Epson America Inc., cité par Suzan Stellin, Who's watching you, C/Net, <http://www.cnet.com/Content/Features/Dlife/Privacy>, 1996.

La légalité des moyens de contrôle de l'activité des salariés

Deux principes s'opposent et doivent être mis en balance : d'un côté l'employeur est en droit de contrôler la bonne exécution de leur travail par ses salariés. D'un autre côté, le salarié a droit au respect de sa vie privée même dans le cadre de son contrat de travail. Le contrôle de l'employeur doit s'opérer sans porter atteinte à la vie privée de ses salariés.

Une obligation constante se dégage de la jurisprudence : l'information préalable des salariés.

L'installation d'un système de contrôle doit être porté à la connaissance du personnel de telle sorte qu'il ne puisse pas ignorer les contrôles dont il peut faire l'objet[87].

Si un enregistrement a été réalisé à l'insu du salarié, il ne peut pas être utilisé contre lui. Ainsi, un arrêt de la Chambre sociale de la Cour de cassation a refusé d'admettre comme mode de preuve l'enregistrement effectué par une caméra dissimulée à proximité de la caisse d'une vendeuse de magasin révélant que la salariée avait dérobé de l'argent[88].

Dans un arrêt en date du 22 mai 1996, la Cour de cassation a adopté la position de principe suivante :

« (…) si l'employeur a le droit de contrôler et surveiller l'activité de son personnel durant le temps de travail, il ne peut mettre en œuvre un dispositif de contrôle qui n'a pas été porté préalablement à la connaissance des salariés »[89].

Les autres obligations de l'employeur

Si les informations collectées sont nominatives et font l'objet d'un traitement informatique, les dispositions de la loi « informatique et libertés » s'appliquent et le traitement devra faire l'objet d'une déclaration auprès de la CNIL[90].

Selon l'article 432-2-1 du Code du travail, le comité d'entreprise doit être informé et consulté, préalablement à la décision de mise en œuvre dans l'entreprise sur les moyens et techniques permettant un contrôle de l'activité des salariés. Enfin, l'employeur doit veiller à ce que les moyens de contrôle n'entravent pas l'exercice des fonctions du délégué du personnel ou syndical.

Concernant l'usage du téléphone, l'écoute et l'enregistrement des conversations téléphoniques des salariés constitue une atteinte à la vie privée, une infraction passible d'un an d'emprisonnement et de 300 000 francs d'amende, prévue par l'article 226-1 du Code pénal qui réprime :

« Le fait, au moyen d'un procédé quelconque, volontairement de porter atteinte à l'intimité de la vie privée d'autrui :

1° en captant, enregistrant ou transmettant sans le consentement de leur auteur, des paroles prononcées à titre privé ou confidentiel;

2° en fixant enregistrant ou transmettant sans le consentement de celle-ci, l'image d'une personne se trouvant dans un lieu privé. »

Il a par exemple été jugé que commet le délit d'atteinte à la vie privé la personne qui enregistre des communications téléphoniques d'ordre personnel, données du bureau d'une entreprise, dès lors qu'elle n'ignore pas que lesdites communications ont par nature un caractère intime[91].

---

[87] Sur la question du contrôle de l'activité des salariés, voir Lamy droit social 1996, n°836 et s.
[88] Soc. 20 novembre 1991, n°8-43.120, cité par Lamy droit social 1996, n°837.
[89] Soc. 22 mai 1995, Bull. Civ. V, n°164.
[90] Voir infra
[91] Crim 8 décembre 1983, Bull. Crim., n°333.

Cela même si le salarié est avisé à l'avance que ses communications téléphoniques sont susceptibles d'être écoutées. Certains mettent à part le cas où la ligne téléphonique surveillée est réservée à un usage professionnel exclusif[92].

Le salarié doit donner son consentement ne serait-ce que de façon tacite. Le consentement est présumé lorsque l'enregistrement est accompli « au vu et au su des intéressés sans qu'ils s'y soient opposés, alors qu'ils étaient en mesure de le faire »[93].

En revanche, l'usage abusif du téléphone de l'entreprise de façon continuelle et journalière à des fins privées peut justifier un licenciement.

L'usage de la vidéosurveillance sur le lieu et pendant le temps de travail est admis, à condition que le recours au système soit justifié par un intérêt légitime, comme prévenir la fraude ou assurer la sécurité des salariés. Mais la vidéosurveillance ne peut pas avoir pour seul but de contrôler l'activité professionnelle des salariés[94].

L'idée générale est que l'employeur est fondé à prendre des mesures nécessaires au fonctionnement de l'entreprise, mais sans porter atteinte à la vie privée de ses salariés.

Ce principe est consacré par l'article 120-2 du Code du travail :

« Nul ne peut apporter aux droits des personnes et aux libertés individuelles et collectives des restrictions qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché. »

Quels enseignements en tirer quant au contrôle des courriers électroniques des salariés ?

Le juge français, placé devant le cas d'une société qui annonce à ses salariés que leurs courriers seraient confidentiels et qu'elle ne les intercepterait pas, devrait logiquement décider que l'interception des courriers électroniques ayant servi de fondement au licenciement s'est effectuée à l'insu du salarié.

Si l'employeur annonce que les courriers électroniques des employés sont confidentiels, ce qui les place dans la sphère de la vie privée du salarié, il est malvenu ensuite de violer ses engagements et l'intimité qu'il avait assurée à ses salariés. Au delà des spécificités du droit américain, la décision décrite ci-dessus semble surprenante sur ce point.

En l'absence de précisions par l'employeur quant au contrôle des courriers électroniques émis et reçus par les salariés, peut-il enregistrer systématiquement lesdits courriers, les utiliser comme preuve d'une faute ?

La lecture des courriers électroniques soulève des questions différentes de celles de leur enregistrement systématique.

Le contrôle des courriers électroniques des salariés

Lecture

La loi du 10 juillet 1991 pose le principe du secret des correspondances émises par la voie des télécommunications et ce principe s'applique au courrier électronique[95]. Le contrôle réalisé par l'employeur constituerait donc le délit d'atteinte au secret des correspondances[96].

D'un autre côté, si la boîte aux lettres électronique est fournie par l'entreprise, on peut considérer le courrier électronique comme une correspondance professionnelle, au même titre que

[92] Lamy droit social 1996, n°841.
[93] Article 226-1alinéa 4 du Code pénal.
[94] Phillippe Hélis, La vidéosurveillance sur le lieu de travail, Petites Affiches, 26 avril 1996, n°51.
[95] Voir supra
[96] Article 226-15 du Code pénal.

la télécopie et le courrier courant reçu dans l'entreprise par le salarié et donc librement utilisable à ce titre.

Le courrier électronique permet d'effectuer des échanges personnels comme avec le téléphone. Mais l'infraction d'atteinte à la vie privée[97] ne vise que les paroles, c'est-à-dire les conversations téléphoniques. Ce texte ne peut pas concerner en l'état le courrier électronique.

Afin d'éviter les contestations sur la nature privée ou professionnelle des courriers électroniques, il paraît prudent de respecter le principe d'information préalable des salariés et donc de les avertir que les courriers électroniques sont réservés à un usage professionnel exclusif, que le respect de cet usage pourra être contrôlé et que les courriers électroniques pourront être utilisés comme moyen de preuve dans une procédure disciplinaire ou de licenciement.

Le salarié dûment averti pourrait plus difficilement invoquer une atteinte à son intimité, ou au secret de ses correspondances personnelles.

Enregistrement systématique

Il est possible de programmer le serveur de la messagerie afin de conserver une copie de tous les messages émis et reçus. Les techniques informatiques permettent d'archiver un grand nombre d'informations, et de faire des recherches par mot-clé, date ou nom.

Même dans l'hypothèse où l'employeur a annoncé que le courrier électronique était réservé au seul usage professionnel, la mise en place d'un tel système serait-elle licite ?

Outre le fait qu'un tel système devrait faire l'objet d'une déclaration à la CNIL, d'une information des salariés et du comité d'entreprise le cas échéant, sa mise en place devrait être justifiée par un intérêt légitime et non dans le seul but de contrôler l'activité professionnelle des salariés.

Notamment, l'enregistrement et le stockage peuvent être justifiés pour des raisons de preuve[98]. L'activité de l'entreprise peut également justifier un contrôle plus étroit. Il est possible de transférer des documents textes, des programmes, des images par la messagerie électronique. Un salarié malveillant pourrait être tenté de divulguer des secrets d'entreprise par ce procédé. Des motifs de sécurité peuvent donc également justifier un contrôle plus étroit.

Lorsque les enregistrement sont conservés à titre de preuve, deux principes vont se heurter : pour les besoins de la preuve, les informations devront être conservées parfois pendant plusieurs années. Pour la protection du salarié, la CNIL recommande que les informations nominatives enregistrées ne soient pas conservées trop longtemps. Or, un courrier électronique va mentionner des informations qui vont permettre d'identifier le salarié qui a émis ou reçu un courrier.

Un autre problème est qu'un tel système enregistre également le courrier que le salarié émet ou reçoit sur sa boîte aux lettres personnelle dès lors qu'il utilise un ordinateur de l'entreprise pour se connecter.

A l'heure où l'usage du courrier électronique dans l'entreprise n'est pas encore une pratique courante, il est difficile de dégager des solutions qui dépendent à la fois du développement de cet usage, de la perception qu'en auront les utilisateurs et des moyens de contrôle qui seront imaginés par les employeurs. Les salariés ne devront pas oublier qu'à la différence des conversations téléphoniques, le courrier électronique laisse des traces dans la mémoire des ordinateurs.

---

[97] Article 226-1 du Code pénal.
[98] Voir infra

Le manque de fiabilité du courrier électronique

Le courrier électronique présente de nombreux avantages qui devraient rendre son usage aussi courant, voire plus populaire que celui de la télécopie d'ici quelques temps :

- il est rapide puisque, en quelques minutes, vous pouvez transmettre un message à l'autre bout de la planète. Par opposition au courrier électronique, les Anglo-saxons qualifient le courrier postal de « snail mail », courrier escargot ;
- il est peu coûteux puisque du fait de l'infrastructure de l'Internet, cela ne coûte pas plus cher à l'expéditeur d'envoyer un message à Paris, à New York ou à Tokyo ;
- il permet de transporter facilement des informations variées car, à un courrier électronique, il est possible de joindre un fichier, sous forme de texte, mais aussi d'image et de son et demain de vidéo, ainsi que des programmes informatiques ;
- les fonctions du logiciel de courrier électronique permettent d'envoyer le même message à plusieurs correspondants en même temps, de faire suivre les messages, de les classer, de les archiver, de répondre à un message, le tout de manière très conviviale.

Par rapport au courrier électronique, la télécopie est lente, chère et fournit des documents difficiles à traiter puisqu'ils devront être ressaisis et retravaillés.

Cependant, le courrier électronique n'est pas totalement fiable, car il présente les inconvénients suivants :

- il n'existe aucune garantie que les messages envoyés au correspondant ne seront pas lus, interceptés, détournés, modifiés volontairement par un tiers auquel le courrier n'était pas destiné, ceci sans que l'expéditeur puisse le déceler ;
- du fait de l'architecture même de l'Internet, un message avant d'arriver à destination passe par plusieurs ordinateurs. Un message peut donc être intercepté pendant son transit lors de son passage sur l'un de ces ordinateurs.

Il existe des logiciels spécialement conçus pour faire systématiquement une copie de tous les messages à destination ou originaire d'une personne déterminée.

Où sont-ils placés ? Sur les routeurs, les grands nœuds de communication du trafic. La NSA (National Security Agency) américaine surveillerait ainsi de près ce qui se passe sur le réseau. La quantité de données qui transitent nécessite néanmoins de disposer de machines capables de traiter et de stocker l'information recueillie. Qui espionne ainsi ? L'Etat, les puissances étrangères, les espions industriels[99].

D'une manière générale, on compare le courrier électronique à une carte postale, que chacun peut lire n'importe où sur le réseau entre le moment de l'expédition et celui de la réception. Outre le gouvernement et les espions, le courrier peut être lu par les employeurs[100] et les fournisseurs d'accès.

En effet, ces derniers, pour les besoins de l'administration de leur système de messagerie, peuvent par exemple être amenés à faire des copies des messages qui transitent par leurs serveurs, à lire un message mal délivré à cause d'une erreur d'aiguillage.

On peut imaginer aussi l'hypothèse où l'employé d'un fournisseur d'accès se rend complice d'un espion extérieur.

Outre ces problèmes d'interception, on n'est jamais sûr que le message a bien été reçu par son destinataire.

---

[99] Voir Jean Guisnel, Guerres dans le cyberespace, services secrets et Internet. Editions La Découverte, 1995.
[100] Voir supra

Une personne relatait par exemple qu'elle avait reçu à plusieurs reprises des résultats de tests médicaux sur sa messagerie, en raison d'une similitude entre son adresse et celle d'un laboratoire[101].

Outre les erreurs d'envoi, des failles techniques peuvent se produire chez le fournisseur d'accès. Rien ne permet non plus de certifier l'identité de l'expéditeur. Un message peut être envoyé par un imposteur, qui usurpe l'identité d'une personne, en utilisant son adresse électronique.

Dans 99 % des cas, aucun problème de la sorte ne se pose, le message arrive à son destinataire, ou l'expéditeur est prévenu en cas de problème dans la délivrance d'un message par un courrier d'avertissement, et il faut être un peu paranoïaque pour imaginer que tout le monde vous espionne.

Néanmoins ces inconvénients du courrier électronique doivent être gardés à l'esprit avant d'envoyer par ce biais des informations de nature confidentielle, sensible ou intime. Les professions soumises à un secret professionnel strict comme les médecins ou les avocats doivent également rester vigilantes.

Il existe des outils informatiques qui permettent d'assurer la confidentialité des messages transmis, d'authentifier l'émetteur, de s'assurer de l'intégrité et de la bonne réception du message transmis, qui utilisent des techniques de cryptographie. Mais ces outils ne peuvent pas être librement utilisés en France, en raison de la réglementation particulière s'appliquant aux procédés et moyens cryptographiques[102].

[101] Mark Lemley,<MLEMLEY@mail.law.utexas.edu>, Re : Confidentiality and Expectations of Privilege, In Law and Policy of Computer Communications, Cyberia-l<cyberia-l@listserv.aol.com>, 30 juillet 1996.

[102] Voir infra

Deuxième partie

La réglementation des services de communication publique

La réglementation applicable

La réglementation à titre de service audiovisuel

Notre droit comporte une définition très large de la communication audiovisuelle :

« On entend par communication audiovisuelle toute mise à disposition du public ou de catégories de public, par un procédé de télécommunication, de signes, signaux, d'écrits, d'images, de sons ou de messages de toute nature qui n'ont pas le caractère d'une correspondance privée »[103].

On considère que cette définition inclut les services télématiques. Compte tenu de la généralité des termes employés, elle inclut les services Internet comme les services Web ou les newsgroups.

Toutefois, l'ensemble des services de communication Internet ne relève pas nécessairement de la législation sur l'audiovisuel.

Ce qui caractérise l'audiovisuel aux termes de la loi, c'est le fait que soit visé un « public » ou une « catégorie de public », un ensemble d'individus indifférenciés.

Le régime des services audiovisuels varie selon le support ou le mode de transmission.

Les services utilisant la voie hertzienne, les services de radiodiffusion sonore et de télévision distribuée par câble et les services publics de télévision sont soumis à un régime d'autorisation préalable par le CSA. Tous les autres services sont soumis à un régime de déclaration préalable à leur mise en œuvre, par l'article 43 de la loi du 30 septembre 1986.

Les modalités de la déclaration ont été précisées par un décret du 17 avril 1987[104].

La déclaration est effectuée auprès du procureur de la République du tribunal de grande instance du lieu du domicile ou du siège social du déclarant. Si ce dernier est à l'étranger, la déclaration est faite auprès du tribunal de grande instance de Paris.

La déclaration indique :

[103] Loi n° 86-1067 du 30 septembre 1986, article 2 alinéa 2.
[104] Décret n° 87-277.

- les noms et prénoms de la personne physique propriétaire du service, ou, s'il s'agit d'une société, sa dénomination, son siège social, le nom de son représentant légal et de ses trois principaux associés ;
- le nom du directeur de la publication ou celui du responsable de la rédaction ;
- la liste des publications éditées par l'entreprise et la liste des autres services de communication audiovisuelle qu'elle assure ;
- la dénomination et l'objet du service ;
- le nom et l'adresse du centre serveur auquel il est éventuellement fait appel.

En cas de changement dans l'un des éléments soumis à déclaration et en cas de cessation du service, une déclaration doit également être effectuée dans les 8 jours.

Le décret a prévu que l'omission de la déclaration ou une déclaration incomplète ou inexacte est passible de la peine d'amende prévue pour les contraventions de la 5e classe, soit une amende de 10 000 francs.

Si dans le cadre de l'exploitation du service est mise en œuvre un traitement automatisé d'informations nominatives, la loi « informatique et libertés » s'applique, et il faut déclarer le fichier à la CNIL[105]. Le décret du 17 avril 1987 prévoit que le récépissé de déclaration auprès de la CNIL est joint à la déclaration du service audiovisuel auprès du tribunal de grande instance.

Cette déclaration est systématiquement effectuée en ce qui concerne les services télématiques : lors du dépôt du dossier dit « contrat Télétel » pour obtenir un code d'accès auprès de France Télécom, l'éditeur du service doit joindre le récépissé de la déclaration auprès du tribunal de grande instance.

Voici à titre d'exemple, un modèle de déclaration de service télématique utilisé (TGI de Paris) :

```
_____________________________________________
TRIBUNAL DE GRANDE INSTANCE DE PARIS
*****
PARQUET DU PROCUREUR DE LA REPUBLIQUE
*****
Titre du service audiovisuel :
Objet :
Directeur de la Publication :
Demeurant :
Date de naissance :
Lieu de naissance :
Propriétaire :
 OU/
Dénomination :
Siège social :
Représentant légal :
Principaux associés :
1)
2)
3)
Responsable de la rédaction :
Liste des publications:
Centre serveur :
Nom :
```

[105] Voir infra

Adresse :
_____

Pour cette déclaration de service télématique, chaque tribunal a ses propres procédures. Par exemple, à Nanterre[106], il faut adresser le formulaire en deux exemplaires à la section économique, avec une copie de la carte d'identité du directeur de la publication, alors qu'à Paris, un seul exemplaire du formulaire doit être adressé au service concerné[107].

Une déclaration similaire devrait logiquement, à la lecture des textes applicables, être effectuée en ce qui concerne les services Web, y compris dans l'hypothèse d'une simple page personnelle.

Le régime de cette déclaration préalable est inspiré du régime de la presse écrite.

Information de l'utilisateur

Les informations suivantes doivent être mises en permanence à la disposition du public[108] .

- Si la personne propriétaire du service est une personne morale : sa dénomination ou sa raison sociale, son siège social, le nom de son représentant légal et de ses trois principaux associés ;
- si la personne propriétaire du service est une personne physique : ses nom et prénom ;
- dans tous les cas : le nom du directeur de la publication et celui du responsable de la rédaction ;
- la liste des publications éditées par l'entreprise et la liste des autres services de communication audiovisuelle qu'elle assure.

Le régime des entreprises de presse

La loi du 1er août 1986[109], portant réforme du régime juridique de la presse, donne de la presse la définition suivante:

« Au sens de la présente loi, l'expression "publication de presse" désigne tout service utilisant un mode écrit de diffusion de la pensée mis à la disposition du public en général ou de catégories de publics et paraissant à intervalles réguliers. »

Cette loi ne fixe pas un régime juridique de la presse, mais un statut des entreprises de presse.

Les entreprises de presse se voient accorder un certain nombre d'aides fiscales (taux réduit de TVA, régime spécial des provisions pour investissement). En contrepartie, elles sont soumises à des obligations particulières (transparence, pluralisme, indépendance, limitation des concentrations, limitation des participations étrangères pour les publications de langue française). La notion de presse désigne en principe la presse écrite, « les journaux, revues ou écrits périodiques ».

Est-ce qu'un service de communication sur l'Internet pourrait prétendre bénéficier du régime des entreprises de presse ?

Un service de communication sur l'Internet n'utilise pas nécessairement de manière exclusive un mode écrit de diffusion de la pensée, mais un mode multimédia.

La notion de parution à intervalles réguliers ne semble pas être applicable aux services Internet : une mise à jour en temps réel ne correspond pas par exemple à cette notion[110].

---

[106] Tribunal de grance instance 181, avenue Jolliot Curie, 92 020 Nanterre Cédex, tél. : 01 40 97 10 10.
[107] 4e section du parquet de Paris, 14 quai des Orfèvres, 75059 Paris.
[108] Article 37 de la loi du 30 septembre 1986.
[109] Loi n°86-897.

Ainsi, les aides à la presse prévue par la loi n'ont pas été étendues aux services télématiques, même exploités par des entreprises de presse[111].

Il n'existe donc pas de régime spécifique de la presse électronique qui relève du droit commun des autres services de communication audiovisuelle soumis à déclaration. Une circulaire du 17 février 1988[112] fait toutefois obligation aux services de presse électronique (services télématiques des publications de presse électronique paraissant à intervalles réguliers) de faire apparaître le nom du directeur de la publication et du responsable de la rédaction lors de chaque consultation du service sur la première page écran indiquant la dénomination du service.

Le dépôt légal

Les journaux périodiques, les livres et revues sont soumis depuis longtemps[113] à une obligation de dépôt légal, dans un but de conservation et de diffusion du patrimoine culturel.

Une loi du 20 juin 1992[114] est venue étendre ce dépôt légal aux œuvres audiovisuelles et multimédia.

On considère que les bases de données auxquelles on accède en ligne sont exclues de cette obligation de dépôt légal, le texte faisant référence à un support matériel, et que par conséquent, le dépôt légal ne s'applique pas à la télématique[115]. Cependant, les services d'information Internet ne permettent pas seulement de mettre en ligne des bases de données, ils permettent la diffusion de documents multimédia, qui eux doivent faire l'objet d'un dépôt « quels que soient leurs supports et procédés techniques de production, d'édition ou de diffusion », dès lors qu'ils sont mis à disposition du public[116].

Il reste qu'organiser un dépôt légal pour des services d'information en ligne semble assez difficile à mettre en œuvre. Par exemple, les pages des services Web peuvent être mises à jour fréquemment.

En pratique, ni les éditeurs de services télématiques, ni les éditeurs de services d'information sur l'Internet n'effectuent de dépôt légal.

Les limites de l'application du régime de l'audiovisuel

Les difficultés soulevées par la déclaration à titre de service audiovisuel

Une déclaration à titre de service audiovisuel devrait être effectuée en application de l'article 43 de la loi du 30 septembre 1986 dès lors que la notion de service de communication audiovisuelle est entendue très largement.

---

[110] Le statut d'entreprise de presse n'a ainsi pas été attribué à l'AFP, qui assure la retransmission immédiate et continue des informations qu'elle reçoit de ses journalistes, Paris 18 mai 1988, D 1990.35.

[111] Pierre Huet, Problèmes juridiques relatifs aux autoroutes de l'information et au multimédia, Droit de l'Informatique et des Télécoms, 1995/2, p.5, n°15.

[112] JO du 9 mars 1988.

[113] L'institution du dépôt légal remonte à François 1er en 1537.

[114] JO du 23 juin 1992.

[115] Lamy informatique 1996, n°1863.

[116] Articles 21 et 22 du décret n° 93-1429 du 31 décembre 1993 relatif au dépôt légal, JO du 1er janvier 1994.

Cependant, la déclaration envisagée par les textes suppose que chaque service soit doté d'un directeur de la publication ou d'un responsable de la rédaction, elle assimile les services de communication audiovisuelle à des entreprises de presse.

Or, sur l'Internet, il n'y a pas nécessairement d'intermédiaire entre l'auteur, le producteur d'une information et le serveur qui fournit les moyens matériels et logiciels. La même personne peut être propriétaire du service, et responsable de sa rédaction. En outre, tout usager peut devenir fournisseur d'information. Toutes les pages Web personnelles doivent-elles faire l'objet d'une déclaration ?

La lecture des textes entraîne une réponse affirmative.

Concernant les forums de discussion, le même régime est théoriquement applicable. La personne qui poste un message dans un forum met « à disposition du public par un procédé de télécommunication, des signes, signaux, écrits »[117] et parfois même des images et du son. Certains auteurs indiquent au sujet de ces forums qu'il faut mettre en œuvre un régime de déclaration préalable à l'instar de celui de la presse écrite : « Il faudrait par suite appliquer aux forums de discussion pareil système qui exigerait simplement *ab initio* une déclaration préalable au CSA »[118].

Peut-être, mais celui qui dans cette hypothèse fournit l'information, c'est l'auteur du message. Le fournisseur d'accès fournit l'accès au serveur de news, mais pas le contenu du service qui résulte de l'ensemble des messages postés par les utilisateurs eux-mêmes. Le fournisseur d'accès ne peut d'ailleurs pas être propriétaire d'un service qui n'appartient à personne.

Chaque usager de l'Internet étant potentiellement en mesure de communiquer de manière publique sur les forums de discussion, doit-il faire une déclaration auprès du procureur de la République ?

Ce serait une interprétation déraisonnable de l'article 43 de la loi de 1986, sauf si la France adoptait en matière d'Internet, une politique identique à celle de la Chine populaire, où chaque utilisateur doit se faire enregistrer auprès des services de police.

Si cette déclaration préalable doit pouvoir être effectuée pour des services réalisés par des sociétés commerciales, ou d'autres groupements comme des associations déclarées, elle est inapplicable pour les services de discussions publiques et peu pratique pour les services d'information réalisés par les particuliers eux-mêmes.

En pratique aujourd'hui, peu de personnes ou de sociétés ayant réalisé un service Web ont pris la peine d'effectuer de telles déclarations. Début 1996, ni les services de Paris, ni ceux de Nanterre n'avaient apparemment enregistré de déclaration de service Web, une des greffières, contactée au téléphone m'ayant même demandé : « C'est quoi l'Internet ? ». Editeur d'un site Web sur le droit des nouvelles technologies, j'ai voulu effectuer une déclaration qui m'a été renvoyée : on me demandait de préciser le code d'accès télétel (3614 ou 3615). J'ai arrêté là l'expérience.

On voit néanmoins apparaître dans les contrats d'hébergement les références à cette déclaration. Par exemple, une société a inclus dans ses conditions générales d'hébergement la clause suivante : « Le Service devra être déclaré par l'éditeur avant sa mise en service, auprès du procureur de la République. »

[117] Article 2 de la loi du 30 septembre 1986 sur l'audiovisuel.

[118] Yves Benhamou, Quelle régulation pour les futures autoroutes de l'information, Contribution au droit des nouvelles technologies, Gaz. Pal. 21 mai 1996, p.7.

La différence entre les médias de masse et les services de communication Internet

La fourniture de services multimédia sur un réseau câblé est subordonnée à la conclusion d'un accord avec le CSA si leur objet est directement associé à la fourniture d'un service de radiodiffusion sonore ou de télévision[119]. De même, la diffusion de services multimédia par un réseau hertzien ou par satellite est subordonnée à un accord du CSA, lorsque les services utilisent des fréquences dont l'attribution lui a été confiée. Ces règles sont justifiées pour des raisons techniques tenant à la rareté des fréquences hertziennes, ou tenant aux contraintes d'utilisation des réseaux câblés qui nécessitent de puissants investissements. On veut éviter dans ce dernier cas la concentration et la constitution de monopoles[120].

Avec l'Internet, cette distinction pourrait se révéler délicate, dans la mesure où les mêmes services peuvent emprunter différents réseaux. Par exemple, on voit apparaître des radios sur l'Internet, TV CABLE propose des accès par câble et une société lyonnaise envisage de fournir des accès par voie hertzienne[121]. La mise en œuvre d'une radio sur l'Internet va-t-elle relever d'un régime distinct selon le support à partir duquel elle est diffusée ?

Dès lors que la capacité des réseaux et les techniques de compression permettront la diffusion d'œuvres numérisées sur tous les réseaux de télécommunication, la distinction entre régulation de l'audiovisuel et celle des télécommunications deviendra de plus en plus artificielle[122].

C'est en réalité la nature du service plutôt que celle des supports qui devrait déterminer dans le futur le régime applicable[123].

Par ailleurs, les services de communication autorisés par le CSA sont soumis à un ensemble de règles contraignantes concernant la programmation, le pluralisme de l'information, le régime et la durée de la publicité, la production et la diffusion des œuvres audiovisuelles[124]. Les règles fixées par les textes sont complétées par les conventions passées avec le CSA et assorties de pénalités contractuelles.

La raison de ce régime dérogatoire au principe de la liberté de communication tient à la nature et à l'impact des services en cause, qui sont des moyens de communication de masse.

Ces services sont fondés sur la notion de programme, qui est étrangère au principe de l'interactivité par laquelle l'utilisateur choisit les données qu'il veut consulter[125] et caractéristique de la manière dont l'information est appréhendée par l'usager sur l'Internet.

En outre, sur l'Internet, tout utilisateur peut être amené à devenir producteur d'informations. Les personnes physiques ou morales fournissant de l'information sur l'Internet sont aussi variées que la nature et l'activité humaine, puisqu'il peut s'agir aussi bien de sociétés commerciales, d'associations, d'administrations, d'universités, de mouvements religieux, politiques, et même de simples particuliers, qui peuvent eux-mêmes avoir des opinions et des centres d'intérêt très différents. Cette diversité n'existait pas pour les services télématiques. Bien que la qualité du contenu puisse varier, un particulier a autant d'audience potentielle que les organisations les plus larges.

Ces différences fondamentales entre les médias de masse et les services de communication sur l'Internet posent la question de la légitimité d'une institution de contrôle des services Internet.

---

[119] Article 34-2 de la loi du 30 septembre 1986.

[120] E. Derieux, Droit de la communication, LGDJ, 2e édition, p.202.

[121] Voir supra

[122] Nathalie Mallet- Poujol, Autoroutes de l'information : les grandes manœuvres juridiques, Petites Affiches, 2 février 1996, p. 4.

[123] Pierre Huet, Problèmes juridiques relatifs aux autoroutes de l'information et au multimédia, Droit de l'Informatique et des Télécoms, 1995/2, p.5, n°20.

[124] Articles 27 et 33 de la loi du 30 septembre 1986.

[125] Pierre Huet, Problèmes juridiques relatifs aux autoroutes de l'information et au multimédia, Droit de l'Informatique et des Télécoms, 1995/2, p.5, n°18.

La légitimité de l'instauration d'une institution de contrôle des services de communication Internet

Le régime d'autorisation actuellement en vigueur pour la télévision et la radiodiffusion n'a évidemment pas lieu d'être pour l'Internet.

Le rapport de synthèse de la mission interministérielle sur l'Internet présidée par Mme Falque-Pierrotin[126] précise ainsi que :

« L'Internet semble difficilement s'inscrire dans un schéma de contrôle administré de type contrôle *a priori* (…). On voit mal dans ces conditions, une réglementation contraignante d'autorisations et d'obligations de contenus se mettre en place comme il en existe, au nom de la rareté des fréquences, pour la télévision. »

Sous la pression de l'actualité, le gouvernement a tenté de mettre en place un régime de contrôle administré par le CST (Conseil supérieur de la télématique) placé sous la tutelle du CSA, en faisant adopter par le Sénat un amendement (dit amendement Fillon) à la loi sur les télécommunications[127], ajoutant à la loi du 30 septembre 1986 sur l'audiovisuel des articles 43-1 à 43-3.

L'amendement Fillon à la loi sur les télécommunications et la décision du Conseil constitutionnel

Le fournisseur d'accès est défini comme « toute personne dont l'activité est de fournir un service de connexion à un ou plusieurs services de communication audiovisuelle mentionné au 1° de l'article 43 de la loi du 30 septembre 1986 (services audiovisuels soumis à déclaration) ».

Il est tenu de proposer à ses clients un moyen technique leur permettant de bloquer l'accès à certains services et de les sélectionner.[128]

Le CST, est placé auprès du CSA. Le CSA est chargé d'adopter sur proposition du CST des recommandations propres à assurer le respect par les services de communication audiovisuelle relevant du régime de la déclaration préalable des règles déontologiques adaptées à la nature des services proposés. Ces recommandations sont publiées au Journal officiel.

Le CST comporte en son sein une instance chargée d'émettre, à la demande de tout utilisateur, de tout opérateur, de tout fournisseur de services, ou de toute organisation professionnelle ou association d'usagers, des avis sur la conformité de tout service de communication audiovisuelle aux recommandations émises. L'avis est notifié aux intéressés. Lorsque le CST estime que le service ne respecte pas ces recommandations, son avis est publié au Journal officiel.

Le président du CSA, lorsqu'il a connaissance de faits de nature à motiver des poursuites pénales, est tenu d'informer sans délai le procureur de la République.

Lorsque le fournisseur d'accès a fourni à ses clients des logiciels de filtrage et a bloqué l'accès à un service ayant fait l'objet d'un avis défavorable publié au Journal officiel, il n'est pas pénalement responsable des infractions résultant du contenu des messages diffusés par un service de communication audiovisuelle, sauf s'il a en connaissance de cause personnellement commis ou participé à la commission de l'infraction.

L'objectif du ministère des Télécommunications à l'origine de ce texte était de clarifier le statut des fournisseurs d'accès.

Le Conseil constitutionnel, saisi d'une demande d'examen de conformité à la constitution de la loi sur la réglementation des télécommunications par un groupe de sénateurs, a censuré les

---

[126] 16 mars 1996 - 16 juin 1996, disponible à < http://www.telecom.gouv.fr/francais/activ/techno/missionint.htm >.

[127] Voir supra

[128] Sur les questions soulevées par les logiciels de filtrage, voir infra

deux dispositions relatives à l'attribution de pouvoirs de recommandations et d'avis au CSA et au CST en matière de contrôle de la communication audiovisuelle (services télématiques et Internet)[129].

En effet, en vertu de l'article 34 de la Constitution :

« La loi est votée par le Parlement.

La loi fixe les règles concernant :

- les droits civiques et les garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques. »

Parmi ces libertés publiques, figure la liberté d'expression telle que consacrée par l'article 11 de la Déclaration des droits de l'homme et qui a valeur constitutionnelle :

« La libre communication des pensées et des opinions est un des droits les plus précieux de l'homme : tout citoyen peut donc parler, écrire, imprimer librement, sauf à répondre à l'abus de cette liberté dans les cas déterminés par la loi. »

Après avoir rappelé que :

« Aux termes de l'article 34 de la Constitution, la loi fixe les règles concernant les droits civiques et les garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques ; qu'il appartient au législateur d'assurer la sauvegarde des droits et des libertés constitutionnellement garantis ; que s'il peut déléguer la mise en œuvre de cette sauvegarde au pouvoir réglementaire, il doit toutefois déterminer lui-même la nature des garanties nécessaires ; que s'agissant de la liberté de communication, il lui revient de concilier, en l'état actuel des techniques et de leur maîtrise, l'exercice de cette liberté telle qu'elle résulte de l'article 11 de la Déclaration des droits de l'homme et du citoyen, avec, d'une part, les contraintes techniques inhérentes aux moyens de communication concernés et, d'autre part, les objectifs de valeur constitutionnelle que sont la sauvegarde de l'ordre public, le respect de la liberté d'autrui et la préservation du caractère pluraliste des courants d'expression socioculturels. »

le Conseil constitutionnel a déclaré les articles 43-2 et 43-3 du projet de loi contraires à la Constitution pour les motifs suivants :

« Considérant que la loi a confié au CST le soin d'élaborer et de proposer à l'adoption du CSA, auprès duquel il est placé, des recommandations propres à assurer le respect par certains services de communication de règles déontologiques, sans fixer à la détermination de ces recommandations, au regard desquelles des avis susceptibles d'avoir des incidences pénales pourront être émis, d'autres limites que celles, de caractère très général, résultant de l'article 1er de la loi susvisée du 30 septembre 1986 ; qu'ainsi le législateur a méconnu la compétence qu'il tient de l'article 34 de la Constitution ».

Il est donc reproché par le Conseil constitutionnel au législateur de ne pas avoir défini les principes à respecter pour l'élaboration de ces recommandations et des avis qui y font suite.

Le gouvernement a annoncé son intention de faire d'autres propositions dans le même sens, conformes à l'avis du Conseil constitutionnel.

Cependant, est-il possible de mettre en place sur l'Internet un contrôle d'une autorité administrative sans porter atteinte à la liberté d'expression constitutionnellement garantie compte tenu de la spécificité des services Internet ?

[129] Décision n° 96-378 DC du 23 juillet 1996, JO du 27 juillet 1996.

Services de communication Internet et liberté d'expression

La mise en place d'une autorité administrative risque de porter atteinte à la liberté d'expression

Se trouveraient placés dans la sphère de contrôle de l'autorité administrative de tutelle des services de communication, qui, s'ils étaient fournis hors réseau, bénéficieraient du régime de liberté sans contrôle d'une autorité de tutelle. On pense notamment aux journaux de la presse écrite, aux associations, aux partis politiques.

Par ailleurs, le droit commun, en matière pénale, civile et commerciale s'applique au contenu des services de communication[130], et les textes encadrant la liberté d'expression sont déjà nombreux et variés.

La liberté de communication est en principe la règle, dans les limites appréciées par le juge pénal, par référence à des infractions définies par la loi. La télévision et la radiodiffusion ont pu être soumises à un régime d'autorisation administrative, afin de concilier l'exercice de la liberté de communication « avec, d'une part, les contraintes techniques inhérentes aux moyens de la communication audiovisuelle et, d'autre part, les objectifs de valeur constitutionnelle que sont la sauvegarde de l'ordre public, le respect de la liberté d'autrui et la préservation du caractère pluraliste des courants d'expression **auxquels ces modes de communication, par leur influence considérable, sont susceptibles de porter atteinte**[131] ». On relèvera que cette précision « auxquels ces modes de communication (…) sont susceptibles de porter atteinte. ». ne figure pas dans la décision du Conseil constitutionnel relative à l'amendement Fillon.

Cette différence entre les services de communication audiovisuelle de masse et les services d'information type Internet a donc été relevée par le Conseil constitutionnel.

Quel que soit l'angle sous lequel la question est envisagée, il va se révéler délicat de mettre en place une autorité de contrôle sans porter atteinte à la liberté d'expression.

L'autorité est conduite à expliciter, à interpréter les interdictions du Code pénal limitant la liberté d'expression.

Ceci l'amènerait à se substituer à l'autorité judiciaire, dont la mission est précisément de juger ces questions.

Or, remplacer la procédure judiciaire d'interprétation des textes pénaux, entourée de garanties, par l'avis d'une autorité administrative est contraire à l'esprit de l'article 66 de la Constitution aux termes de laquelle l'autorité judiciaire est gardienne des libertés publiques.

Il existe effectivement des cas où une autorité administrative possède des pouvoirs de sanction. C'est notamment le cas du CSA. Le Conseil constitutionnel a estimé que le législateur pouvait charger une autorité administrative indépendante de veiller au respect de la liberté de communication audiovisuelle et la doter de pouvoirs de sanctions dans la limite nécessaire à l'accomplissement de sa mission.

Mais pour le CSA, il s'agit de sanctionner des manquements à des obligations attachées à une autorisation administrative[132].

Dans notre hypothèse, l'autorité risquerait d'être amenée à sanctionner des manquements à la loi pénale.

---

[130] Voir infra

[131] Décision n°88-248 DC du 17 janvier 1989 sur la loi modifiant la loi n°86-1067 du 30 septembre 1986 relative à la liberté de communication.

[132] Pour un exemple de sanction ayant donné lieu à la suspension de la radio Skyrock pour atteinte à la dignité humaine, TGI Paris 5 février 1992, MP c/ Bellanger, Légipresse, mai 1996, III, p.49.

Les services Internet sont supposés bénéficier du régime de liberté avec contrôle *a posteriori,* comme la presse, dont on soulignera qu'elle n'est soumise à aucune autorité ou conseil de ce type.

> L'autorité est amenée à appliquer de nouvelles interdictions qui seraient prévues par le législateur.

Dans ce cas, la communication sur l'Internet bénéficierait d'une liberté d'expression réduite par rapport à d'autres moyens d'expression, notamment la presse écrite, ce qui là encore pose un problème au regard des libertés publiques.

C'est d'ailleurs à un problème de ce type que s'est heurté le législateur américain.

La loi américaine contient déjà diverses dispositions réprimant la diffusion de matériel obscène ou pédophile. Le législateur américain a adopté dans le cadre de la loi sur les télécommunications du 8 février 1996, un Communication Decency Act, dit CDA, visant à lutter contre la pornographie sur l'Internet. La loi incrimine la diffusion de messages « indécents » ou « manifestement choquants selon les normes de la société contemporaine », des termes vagues, créant une incertitude sur le champ d'application exact de la loi, pour ses détracteurs.

Un tribunal américain a été saisi d'un recours en inconstitutionnalité du CDA.

En matière de discours indécent, la Cour suprême américaine considère que bien que les adultes aient le droit, garanti par le 1er amendement de la Constitution sur la liberté d'expression, de tenir des propos indécents, le gouvernement peut, sans violer la Constitution, réglementer l'indécence à la radio et à la télévision, compte tenu de la nature de ce média[133].

Analysant longuement les spécificités de la communication sur l'Internet, les juges américains qui ont examiné le CDA ont considéré dans une décision en date du 11 juin 1996 que les termes « indécents » et « manifestement choquants » étaient inconstitutionnellement vagues[134].

Pour le juge Dalzell :

« L'intrusion du CDA sur l'Internet va nécessairement affecter la participation des adultes dans le média [...]. Dès lors que la plupart des communications sur l'Internet sont de nature interactive, c'est-à-dire une forme de dialogue, une diminution du nombre des interlocuteurs, des forums de discussion et des sujets autorisés va restreindre le dialogue mondial qui constitue la force et la réussite du média.

(...)

En réalité, l'affirmation du gouvernement de l'"échec" de l'Internet repose sur le constat implicite que le volume d'expression qui circule et l'accessibilité de cette expression est trop élevé. C'est toutefois exactement le bénéfice de la communication sur l'Internet. Le gouvernement demande implicitement à ce tribunal de limiter à la fois le volume d'expression qui circule sur l'Internet, mais aussi de limiter son accessibilité. Cet argument est profondément dédaigneux du premier amendement.[...]

L'Internet peut être considéré comme une conversation mondiale sans fin. Le gouvernement ne peut pas, avec le CDA, interrompre cette conversation. En tant que forme d'expression de masse la plus interactive développée à ce jour, l'Internet mérite le degré de protection le plus haut contre l'intrusion gouvernementale.[135] »

---

[133] FCC v. Pacifica Foudation, 438 US 726 (1976).

[134] ACLU et al. V. Janet Reno, Attorney General of the United States, 11 juin 1996, 929 F. Supp. 824 (E.D. Pa. 1996), disponible à : < http://www.aclu.org/issues/cyber/trial.htm>.

[135] "The Internet may fairly be regarded as a never-ending worldwide conversation. The government may not, through the CDA, interrupt that conversation. As the most participatory form of mass speech yet developed, the Internet deserves the highest protection from governmental intrusion".

Le législateur français va être confronté à la même problématique.

Par exemple, pourquoi le journaliste qui s'exprimerait sur l'Internet ne bénéficierait-il pas de la même liberté d'expression que son confrère qui s'exprime par écrit ?

La situation de la télématique est différente de celle de l'Internet

On objectera qu'un organisme de contrôle existe déjà pour la télématique.

Cependant la situation de la télématique et celle de l'Internet sont différentes à plusieurs titres.

Le CST a été créé par un décret[136], de telle sorte que la conformité du dispositif prévu n'a pas été examinée par la Conseil constitutionnel. Le CST émet des « recommandations de nature déontologique visant notamment à la protection de la jeunesse, applicables aux services offerts par les accès télématiques anonymes écrits ou vocaux ». Il peut émettre des avis sur les projets de France Télécom. Un autre comité consultatif, le CTA (Comité de la télématique anonyme) veille à l'application des recommandations du CST dans les contrats.
Le dispositif permet bien d'élaborer, sans base législative, une réglementation assortie de sanctions.

Seulement, tout fournisseur de services télématiques est tenu de passer un contrat avec France Télécom, qui insère dans ses « contrats kiosque » les recommandations de nature déontologique, leur donnant ainsi une base contractuelle.

L'article 10 du contrat Télétel précise ainsi que :

« En cas de manquement par le fournisseur de services ou le(s) centre(s) serveur(s), à l'une des obligations souscrites au titre du présent contrat, France Télécom pourra résilier ou suspendre le présent contrat, après une mise en demeure restée sans effet, sous réserve de respecter les dispositions légales et réglementaires rappelées en annexe 3. »

Ainsi le fournisseur de services télématiques en cas de manquement à ses obligations déontologiques peut à tout moment perdre le droit de fournir son service. La technique juridique du recours au contrat a été validée en jurisprudence.

Dans une affaire où il était reproché à un fournisseur de services d'avoir diffusé des messages à caractère pornographique préenregistrés, la Cour d'appel de Paris a considéré que :

« Enfin, si France Télécom n'a pas à se substituer au ministère public pour poursuivre les infractions à l'ordre public et aux bonnes mœurs, elle conserve la faculté de veiller au respect des obligations souscrites par les fournisseurs de services sur les kiosques téléphoniques et, en cas de violation, de procéder à la résiliation des conventions suivant la procédure contractuellement prévue [137]. »

Un auteur a pu déclarer à propos de ce système :

« Il faut bien voir que ce système fait, dans une certaine mesure, de l'opérateur un régulateur –ce qui n'est guère conforme au livre vert de la Commission européenne – et un juge de l'application de la loi, voire de la loi pénale, car le droit de résilier la convention kiosque est un droit de vie ou de mort sur les services qui en sont tributaires.

C'est là une dérogation au droit commun – c'est-à-dire la liberté de communication dont le limites sont fixées par la loi – et qui rapproche le régime de la télématique (régime de déclaration) d'un régime d'autorisation précaire et révocable par l'administration[138]. »

[136] Décret n°93-274 du 25 février 1993.
[137] Paris, 1re Ch. 13 octobre 1992, SA Midratel c. France Télécom, D 1993, I.R. 32.
[138] Pierre Huet, Cadre juridique de l'Audiotex en France et dans le monde, Droit de l'Informatique et des Télécoms, 1994/3, p.59.

Le dispositif mis en place pour la télématique, critiquable au regard des principes européens et constitutionnels, ne semble en tout état de cause pas transposable à l'Internet, en raison de l'absence d'opérateur unique et de la multiplicité des intervenants.

A côté des fournisseurs d'accès dont le statut varie fortement, il faut également compter les serveurs, qui peuvent héberger des services sans être nécessairement fournisseurs d'accès grand public. Ce système ne serait pas non plus justifié en raison des différences entre services télématiques et services Internet : le contenu des services Internet est beaucoup plus varié que le contenu des services télématiques, les services télématiques sont toujours des services payants, ce qui n'est pas nécessairement le cas des services Internet, une messagerie télématique suppose nécessairement qu'un fournisseur ait mis en place cette messagerie, ce qui n'est aucunement le cas des forums de discussion.

> Quelle autorité administrative pourrait disposer d'une légitimité suffisante pour prétendre exercer un contrôle sur le contenu des services Internet ?

Pour certains, il faut « pour assurer une régulation efficace des futures autoroutes de l'information conférer des prérogatives plus affirmées[139] au CSA ».

Et c'est en ce sens qu'a tranché le législateur en plaçant le CST auprès du CSA.

Le CSA a pour mission essentielle d'assurer l'égalité de traitement, de garantir l'indépendance et l'impartialité du secteur public de la radiodiffusion sonore et de la télévision, de veiller à favoriser la libre concurrence, de veiller à la qualité et à la diversité des programmes, au développement de la production et de la création audiovisuelle nationales ainsi qu'à la défense de la langue et de la culture françaises[140].

« Pourquoi avoir donné au CSA une telle responsabilité concernant un domaine nouveau et prometteur de communication, qui a si peu à voir avec la mission traditionnelle du CSA ? »[141].

La réglementation des médias de masse est de nature différente de celle des services en ligne, et ces domaines devraient rester séparés[142].

Le rapport de la mission interministérielle sur l'Internet[143] préconise la mise en place d'un organisme de veille. Cet organisme serait chargé de conseiller le gouvernement sur les services en ligne et de faire toute recommandation d'ordre déontologique, de recevoir des plaintes des utilisateurs et pourrait à leur demande ou à celle du gouvernement, donner des avis sur des sites litigieux, avis pouvant être versés dans une procédure pénale.

On voit que la frontière entre « organisme de veille » et l'instauration d'un organisme administratif de régulation émettant des avis susceptibles d'avoir des effets juridiques (les avis pourraient être versés dans une procédure pénale) est difficile à tracer.

Le rapport ajoute d'ailleurs qu'« il (l'organisme de veille) devra, enfin, articuler son action avec les organismes de régulation existants : le CST auquel il se substitue, le CSA, pour qu'une approche déontologique commune soit adoptée quel que soit le support de la communication[144] ». Pourtant le rapport avait exclu une régulation de nature administrative du réseau.

---

[139] Yves Benhamou, Quelle régulation pour les futures autoroutes de l'information, Contribution au droit des nouvelles technologies, Gaz. Pal. 21 mai 1996, p.7.

[140] Article 1er alinéa 4 de la loi du 30 septembre 1986.

[141] Daniel Kahn, Le contrôle d'Internet, vite fait -bien fait ? Les Annonces de la Seine, 24 juin 1996, n°45.

[142] AFTEL, Le droit du multimédia, rapport réalisé sous la direction de P. Huet avec le concours de H. Maisl, J. Huet et A.Lucas 1996, p.171.

[143] Mission présidée par Mme Falque-Pierrotin, 16 mars 1996- 16 juin 1996, disponible à : < http://www.telecom.gouv.fr/francais/activ/techno/missionint.htm>.

[144] Recommandation n°5 de la synthèse du rapport.

L'Association des Utilisateurs d'Internet s'interroge en ces termes au sujet de la mise en place d'un observatoire[145] :

« D'autres propositions, plus sérieuses et plus respectueuses de nos valeurs, suggèrent la mise en place d'un "observatoire" qui serait une instance de référence, à laquelle un citoyen pourrait s'adresser lorsqu'il constate une information délictueuse sur Internet. Le rôle de cet organisme, qui serait en quelque sorte un médiateur, consisterait en la collecte des plaintes ou avertissements, aurait en charge la vérification de leur bien-fondé, et le cas échéant signalerait la chose aux fournisseurs d'accès.

Les questions soulevées par ce type de proposition sont de deux ordres : d'abord, où serait l'intérêt de mettre en place un tel organisme, dont on peut supposer qu'il fonctionnerait aux frais de l'Etat et donc de la collectivité, qui ne serait qu'un niveau intermédiaire supplémentaire et inutile ? Que pourrait apporter de plus un tel organisme par rapport à la situation où le citoyen alerte directement le fournisseur d'accès ? Ensuite, et c'est le plus important, de qui dépendrait cet organisme ? Comment pourrait-on assurer l'indépendance de ses avis ? Comment pourrait-on garantir l'exercice de la démocratie et éviter toute dérive future d'un tel organisme ?

On pourra objecter que le CSA existe. Mais le CSA n'agit que sur la diffusion de l'audiovisuel (radio et télévision) français. Le CSA ne peut rien dans le cas de la réception par satellite. De plus, le champ d'action du CSA est limité (et n'a aucune raison de s'étendre) à la diffusion de son et d'image sous la responsabilité éditoriale des chaînes concernées. Internet, encore une fois, est fondamentalement différent : c'est le citoyen qui s'exprime au moyen de cette infrastructure, et non plus seulement des groupes — privés ou publics — puissants, organisés et limités en nombre.

On peut rappeler que la justification de l'existence de l'organisme nommé aujourd'hui CSA était à l'origine la rareté des fréquences hertziennes, ce qui impliquait la nécessité de les attribuer. Les pouvoirs du CSA ont été très étendus depuis, alors qu'il n'existe pas d'équivalent de cet organisme dans le domaine de la presse écrite, par exemple (où la responsabilité éditoriale est autant assurée que pour les médias audiovisuels) : qu'est-ce qui justifierait donc l'existence et l'autorité d'un tel organisme dans le cas d'Internet ?

Si un tel dispositif chargé de collecter les plaintes et d'en informer les fournisseurs d'accès commerciaux (ou autres) se justifiait, ce serait uniquement en tant que mise en commun de moyens par les fournisseurs d'accès pour limiter les coûts d'une telle opération. Un tel dispositif ne saurait donc avoir une autorité quelconque vis-à-vis de la société dans son ensemble. Le législateur n'a pas à intervenir dans sa constitution, et n'a pas à lui conférer ni à lui reconnaître une autorité supérieure, en tous cas certainement pas d'ordre déontologique, ni éthique, à celle qu'aurait un cabinet juridique attaché au service d'un fournisseur d'accès commercial.

Ce dispositif permettrait uniquement de répartir les coûts de l'expertise juridique entre plusieurs fournisseurs d'accès commerciaux. Sa mise en place relèverait de la volonté de fournisseurs d'accès commerciaux de s'associer pour ce faire ».

Sur l'Internet comme ailleurs, des transgressions aux limites tracées à la liberté d'expression sont inévitables.

Cependant ces transgressions présentent-elles un caractère tellement massif de la part des utilisateurs français qu'elles justifieraient la mise en place d'un régime dérogatoire au principe de la liberté de communication ?

Quelques affaires surmédiatisées, traitées sans recul ni sérénité, ne doivent pas occulter la richesse et la variété des communications publiques, des informations que l'on trouve sur l'Internet.

---

[145] Pour une intégration sereine et un développement harmonieux d' Internet dans la société franaçaise, rapport élaboré pour une consultation organisée dans le cadre de la mission interministérielle sur le développement des réseaux ouverts au public, de type Internet, 7 juin 1996, disponible à : <http://www.aui.fr/Rapports/RAUI-070696.html>.

Certes le législateur français entend réagir contre la diffusion de messages à caractère raciste, révisionniste, pédophile que l'on peut malheureusement aussi trouver sur l'Internet.

De tels messages sont déjà interdits en France.

Ces messages émanent généralement de personnes situées hors d'atteinte de notre système judiciaire.

En voulant réglementer l'impossible, c'est-à-dire des messages émis hors de France, c'est toute la communication des usagers français, qui sont déjà responsables devant le juge français, qui se trouve affectée.

Le caractère international de l'Internet pose certaines difficultés dès lors que certaines informations sont licites dans le pays d'émission, mais illicites dans le pays de réception.

Certains pays peuvent juger choquants et inacceptables des discours et images que nous considérons comme normaux. On peut citer à titre d'exemple la fatwa contre l'écrivain Salman Rushdie.

Si le problème posé par l'Internet est dans cette confrontation des cultures, la solution d'organismes de contrôle semble peu adaptée dès lors que leurs avis et recommandations n'auront aucun effet sur les auteurs protégés par leur réglementation nationale, compte tenu de la nature territoriale du droit pénal. Il ne nous semble pas que les différences culturelles entre pays souverains qui se trouvent directement exposées sur l'Internet puissent fonder des limitations à nos propres libertés publiques, à notre conception de la démocratie.

La poursuite des auteurs des infractions peut également être rendue plus complexe en raison de la nature transnationale des réseaux informatiques. Mais la mise en place d'un organisme de contrôle sera impuissante à régler ce type de problèmes, qui semble surtout relever d'une amélioration de la coopération internationale entre polices.

Troisième partie

La réglementation des contenus

Si la liberté d'expression est un des fondements des sociétés démocratiques, consacrée en France par la Constitution, et au niveau européen par la Convention européenne des droits de l'homme[146], elle n'est pas sans limites.

Elle s'exerce conformément à l'article 11 de la Déclaration des droits de l'homme dans « la limite du respect des droits d'autrui ». Les limites ou interdictions formulées dans un souci d'ordre public ou de protection des personnes doivent être fixées par la loi de manière précise, et ne peuvent donner lieu à répression qu'*a posteriori,* au terme d'une procédure judiciaire.

Ces limitations sont applicables à l'information diffusée sur l'Internet.

Ces règles peuvent être divisées en deux grandes catégories : les règles générales applicables à tous les services et les règles particulières en raison du produit ou du service offert. La question des droits d'auteur mérite un examen particulier.

Enfin, les services d'information Web, en raison des possibilités offertes de créer des liens hypertextes, posent des problèmes originaux qui seront également examinés.

Les règles générales applicables à tous les services

Il n'est pas question de faire ici un inventaire exhaustif de tous les textes encadrant la liberté d'information. Si à l'origine, les interdictions étaient peu nombreuses, l'évolution a élargi le champ des délits qui résultent de textes variés et sont de nature diverse. Certaines interdictions sont visées comme délits de presse[147], d'autres se rapportent au droit commun. En pratique, certaines dispositions font l'objet de larges tolérances et pour beaucoup d'entre elles, les poursuites sont rares, voire inexistantes[148]. J'ai choisi de présenter les principales règles à prendre en compte en les divisant en quatre catégories.

Ces textes sont-ils applicables à l'information diffusée sur l'Internet ? Hormis les hypothèses où la disposition concernée vise un moyen précis de communication, un support particulier, la réponse de principe est positive.

La réglementation relative aux délits de presse s'applique, que l'information en cause soit diffusée par voie de presse écrite ou par un autre moyen de communication comme l'audiovisuel. D'autres textes peuvent viser la diffusion par quelque moyen ou procédé que ce soit, ce qui inclut les services de communication audiovisuelle.

---

[146] Article 10.2.

[147] Délits énumérés au chapitre 4 de la loi de 1881 sur la liberté de la presse.

[148] Abrégé du droit de la presse, éditions du Centre de formation et de perfectionnement des journalistes, 4e édition p.69-70.

La protection de l'ordre public

Les textes rentrant dans cette catégorie sont relatifs soit à la protection de l'intégrité et de la dignité humaine, soit à la protection de la nation, soit à la justice.

La protection de l'intégrité et de la dignité humaine

La provocation aux crimes et délits

L'article 23 de la loi de 1881 prévoit que :

« Seront punis comme complices d'une action qualifiée crime ou délit ceux qui, soit par des discours, cris ou menaces proférées dans des lieux ou réunions publics, soit par des écrits, imprimés, dessins, gravures, peintures, emblèmes, images ou tout autre support de l'écrit, de la parole ou de l'image vendus ou distribués, mis en vente ou exposés dans des lieux ou réunions publics, soit par des placards ou des affiches exposés au regard du public, soit par tout moyen de communication audiovisuelle, auront directement provoqué l'auteur ou les auteurs à commettre ladite action, si la provocation a été suivie d'effet. »

Même dans le cas où la provocation n'aurait pas été suivie d'effet, sont punis de 5 ans d'emprisonnement la provocation à commettre les délits suivants (article 24 de la loi du 29 juillet 1881) :

- les atteintes à la vie, à l'intégrité de la personne et les agressions sexuelles ;
- les vols, extorsions, destructions, dégradations volontaires dangereuses pour les personnes ;
- les crimes et délits portant atteinte aux intérêts fondamentaux de la nation ;
- les actes de terrorisme.

L'apologie de certains crimes

Sont punis des mêmes peines l'apologie des crimes de guerre, crimes contre l'humanité, crimes ou délits de collaboration avec l'ennemi (article 24, alinéa 3 de la loi du 29 juillet 1881).

La provocation au suicide d'autrui est munie de 3 ans d'emprisonnement lorsque la provocation a été suivie du suicide ou d'une tentative. Les peines sont aggravées lorsque la victime a moins de quinze ans (article 223-13 du Code pénal).

Provocation à la haine raciale et négationnisme

La provocation à la discrimination, à la haine ou à la violence à l'égard d'une personne ou d'un groupe de personnes à raison de leur origine ou de leur appartenance ou de leur non-appartenance à une ethnie, une nation, une race ou une religion déterminée est punie d'un emprisonnement d'un an et/ou d'une amende de 300 000 francs (article 24, alinéa 6 de la loi du 29 juillet 1881).

L'article 24 bis de la loi du 29 juillet 1881 punit des mêmes peines ceux qui auront contesté « l'existence d'un ou plusieurs crimes contre l'humanité tels qu'ils sont définis par l'article 6 du statut du tribunal militaire international annexé à l'accord de Londres du 8 août 1945 et qui ont été commis soit par les membres d'une organisation déclarée criminelle en application de l'article 9 dudit statut, soit par une personne reconnue coupable de tels crimes par une juridiction française ou internationale ».

La protection de la nation

L'offense au président de la République et aux chefs de gouvernements étrangers est punie d'un an d'emprisonnement et d'une amende de 300 000 francs (articles 26 et 36 de la loi du 29 juillet 1881).

Les délits de fausses nouvelles et fausses informations :

- la publication, la diffusion ou la reproduction de nouvelles fausses, de pièces fabriquées, falsifiées ou mensongèrement attribuées à des tiers sont passibles d'un emprisonnement de 3 ans et d'une amende de 300 000 francs si elles ont été « faites de mauvaise foi » et si elles ont troublé « la paix publique » (article 27 de la loi du 29 juillet 1881) ;
- le fait, en communiquant une fausse information, de compromettre sciemment la sécurité d'un aéronef en vol ou d'un navire est puni de 5 ans d'emprisonnement et de 500 000 francs d'amende (article 224-8 du Code pénal) ;
- le fait de communiquer ou de divulguer une fausse information dans le but de faire croire qu'une destruction, une dégradation ou une détérioration dangereuses pour les personnes va ou a été commise est puni de 2 ans d'emprisonnement et de 200 000 francs d'amende (article 322-14 du Code pénal).

Informations à caractère militaire

Il est interdit de publier des informations concernant des renseignements, procédés, objets, documents, données informatisées ou fichiers ayant le caractère d'un secret de la Défense nationale, sous peine de 5 ans d'emprisonnement et de 500 000 francs d'amende (article 413-11 du Code pénal).

Les informations relatives à la justice

« Le fait de chercher à jeter le discrédit, publiquement ou par actes, paroles, écrits ou images de toute nature, sur un acte ou une décision juridictionnelle, dans des conditions de nature à porter atteinte à l'autorité de la justice ou à son indépendance est puni de 6 mois d'emprisonnement et de 50 000 francs d'amende. » Sont autorisés toutefois les « commentaires techniques, actes, paroles, écrits ou images de toute nature tendant à la réformation, la cassation ou la révision d'une décision »(article 434-25 du Code pénal).

Il est interdit de publier des images ou photographies montrant tout ou partie des circonstances d'un crime de sang, d'un crime ou d'un délit contre les mœsurs, des délits de coups et blessures volontaires, des menaces et délits d'homicide involontaires, sauf sur demande écrite du juge d'instruction, sous peine d'une amende de 25 000 francs (article 38 de la loi du 29 juillet 1881).

Le fait de publier des informations couvertes par le secret de l'instruction peut constituer le délit de recel de violation du secret de l'instruction (article 11 du Code de procédure pénale).

La protection des mineurs

Les publications destinées à la jeunesse

La loi du 16 juillet 1949 fixe un régime particulier pour les publications destinées à la jeunesse. Les entreprises éditrices de ces publications ne doivent pas appartenir à une seule personne mais à une société commerciale ou à une association sans but lucratif dûment déclarée. Elles sont tenues d'avoir à leur tête un comité de direction d'au moins 3 membres et devant respecter certaines conditions et dont les noms doivent figurer sur chaque exemplaire de la publication. Ces publications sont également assujetties à une déclaration et à des obli-

gations de dépôt particulières auprès du ministère de la Justice. Une commission spéciale contrôle ces périodiques.

Ce régime spécial pourrait-il être appliqué à des services d'information en ligne destinés aux enfants et aux adolescents ?

L'article 1er de la loi sur les publications destinées à la jeunesse précise que « sont assujetties aux prescriptions de la présente loi toutes les publications périodiques ou non qui, par leur caractère, leur présentation ou leur objet apparaissent comme principalement destinées aux enfants et aux adolescents ».

Traditionnellement, une publication, c'est un écrit publié, un livre ou une revue. L'article 6 de cette loi fait d'ailleurs clairement référence à des documents imprimés : « Le directeur ou l'éditeur de toute publication visée à l'article 1er est tenu de déposer gratuitement au ministère de la Justice 5 exemplaires de chaque livraison ou volume de publication. »

Etendre à l'Internet les dispositions de cette loi particulière, dérogatoire du droit commun, élaborée à une date où bien évidemment les services Internet n'existaient pas, n'apparaîtrait pas judicieux.

En matière de télévision et de radiodiffusion, des décrets en Conseil d'Etat définissent pour chaque catégorie de services soumis à agrément les obligations concernant la protection des mineurs.

En matière de services télématiques, les recommandations déontologiques du CST attirent plus particulièrement l'attention des fournisseurs de services sur la protection des mineurs :

« Les services destinés à la jeunesse doivent tout particulièrement ne comporter aucune rubrique, aucun message présentant sous un jour favorable le banditisme, le mensonge, le vol, la paresse, la lâcheté, la haine, la débauche ou tous actes qualifiés crimes ou délits ou de nature à démoraliser l'enfance ou la jeunesse, ou à inspirer ou entretenir des préjugés ethniques »[149]. Ces dispositions sont directement inspirées de l'article 2 de la loi du 16 juillet 1949. Toutes ces dispositions ne sont pas applicables aux services Internet qui ne sont pas *a priori* tenus à des obligations plus sévères que celles résultant du droit commun.

Parmi les infractions du droit commun concernant plus particulièrement les mineurs, il convient de citer les articles 227-18 et suivants du Code pénal qui répriment et sanctionnent de peines d'emprisonnement pouvant aller jusqu'à 7 ans :

- le fait de provoquer directement un mineur à faire un usage illicite de stupéfiants ;
- le fait de provoquer directement un mineur à la consommation habituelle et excessive de boissons alcooliques ;
- le fait de provoquer directement un mineur à la mendicité ;
- le fait de provoquer directement un mineur à commettre habituellement des crimes ou des délits ;
- le fait de favoriser ou de tenter de favoriser la corruption d'un mineur.

Les personnes qui mettent en place des services destinés à la jeunesse devraient néanmoins faire preuve de prudence quant au contenu des services. Toute excès ou dérive qui serait constaté appellerait très certainement une intervention du législateur, qui ne peut être que particulièrement sensible à tout ce qui touche la protection des mineurs.

[149] Recommandations du 28 mars 1994, article 3 b).

Les dispositions visant à protéger l'anonymat de mineurs impliqués dans une procédure judiciaire :

- interdiction de la publication, par quelque moyen que ce soit, de tout texte ou de toute illustration concernant l'identité des mineurs qui ont quitté leur parents, leur tuteur ou la personne chargée de leur garde, sauf sur demande écrite de ces personnes ou autorisation écrite des autorités judiciaires ou administratives[150] sous peine d'amende et d'un emprisonnement d'un an en cas de récidive ;
- interdiction de publier tout texte ou toute illustration concernant le suicide de mineurs sauf sur la demande écrite ou avec l'autorisation du procureur[151] ;
- la publication de compte rendus des procès concernant les mineurs et de tout texte ou illustration concernant l'identité et la personnalité des mineurs délinquants est interdite[152] sous une peine de 40 000 francs d'amende et de 2 ans d'emprisonnement en cas de récidive.

Si un jugement concernant un mineur est diffusé, publié, le nom et même les initiales ne devront pas être indiqués, sous peine d'une amende de 25 000 francs[153].

Les interdictions visant à la protection de la jeunesse en général

La diffusion de messages à caractère violent ou pornographique

L'article 227-24 du Code pénal prévoit que :

« Le fait, soit de fabriquer, de transporter, de diffuser par quelque moyen que ce soit et quel qu'en soit le support un message à caractère violent ou pornographique ou de nature à porter gravement atteinte à la dignité humaine, soit de faire commerce d'un tel message, est puni de 3 ans d'emprisonnement et de 500 000 francs d'amende lorsque ce message est susceptible d'être vu ou perçu par un mineur. »

La description des actes incriminés est large. Si la protection des mineurs est la finalité, il suffit pour que l'infraction soit constituée que le message violent ou intolérable soit susceptible d'être vu ou perçu par un mineur : dès lors qu'un service est accessible librement, ce qui est le cas des services Internet, le texte est applicable.

Parmi les messages visés figurent les messages « de nature à porter gravement atteinte à la dignité humaine », ce qui laisse une place à l'interprétation.

La pornographie, c'est l'obscénité, la référence à des représentations d'ordre sexuel, l'incitation à la débauche. Ce n'est pas la simple indécence, ce qui est contraire à la pudeur. La notion de pornographie, qui fait appel aux concepts de bonnes mœurs et de moralité, est néanmoins perçue différemment selon les époques, les individus et les pays.

La portée du texte n'est pas restreinte à ce qui est écrit : la notion de message peut s'appliquer à tout type d'information ou de communication.

L'infraction supposant que le texte puisse être vu par un mineur, la question est de savoir quelles mesures doivent prendre les éditeurs de services pornographiques pour dégager leur responsabilité.

Un simple message d'avertissement sur la page d'accueil du service « Interdit aux moins de 18 ans » ne semble pas suffisante[154]. En outre, sur le Web, l'utilisateur ne passe pas nécessai-

[150] Article 39 bis de la loi du 29 juillet 1881.
[151] Article 39 ter de la loi du 29 juillet 1881.
[152] Article 14 de l'ordonnance n° 45-174 du 2 février 1945.
[153] Idem.
[154] Lamy informatique 1996, n°1918.

rement par la page d'accueil du service, mais peut accéder directement à n'importe quelle page du site.

A la différence de la diffusion de films pornographiques, de la vente de cassettes, de l'accès à des sex-shops, il n'est pas possible de se rendre compte *de visu* de l'âge de la personne ou de lui demander un justificatif de son âge.

Le seul moyen semblerait de mettre en place des services payants, les moyens de paiement utilisés étant censés être réservés aux adultes, ou sur abonnement préalable.

La protection de l'intégrité de la personne des mineurs

L'article 227-24 du Code pénal prévoit que : « le fait, en vue de sa diffusion, de fixer, d'enregistrer ou de transmettre l'image d'un mineur lorsque cette image présente un caractère pornographique est puni d'un an d'emprisonnement et de 300 000 francs d'amende. Le fait de diffuser une telle image, par quelque moyen que ce soit, est puni des mêmes peines. Les peines sont portées à 3 ans d'emprisonnement et à 500 000 francs d'amende lorsqu'il s'agit d'un mineur de moins de 15 ans ».

La protection des intérêts privés

Les atteintes à l'honneur

Diffamation et injure[155]

La diffamation est définie comme « toute 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 ». Le corps signifie les groupes sociaux.

L'injure est « toute expression outrageante, termes de mépris ou invective qui ne renferme l'imputation d'aucun fait ».

La différence entre les deux tient à ce que la diffamation porte sur un fait déterminé, qui peut faire l'objet d'une preuve et d'un débat contradictoire. Sinon, il y a injure. La diffamation doit avoir été rendue publique. Cette condition sera nécessairement remplie pour tous les services d'information en libre accès et les services de discussions publiques. La diffamation et l'injure non publiques sont des contraventions.

Il peut y avoir diffamation même si les faits sont exacts.

La preuve de la vérité des faits diffamatoires ne peut pas être rapportée lorsque l'imputation concerne la vie privée, des faits qui remontent à plus de 10 ans, un fait constituant une infraction amnistiée ou prescrite ou qui a donné lieu à une condamnation effacée par la réhabilitation ou la révision[156]. Les imputations diffamatoires sont présumées faites de mauvaise foi et il appartient à leur auteur de rapporter la preuve contraire[157].

La diffamation est punie d'une peine de 6 mois d'emprisonnement et de 80 000 francs d'amende[158], les peines étant plus élevées si elle a lieu envers certains corps, institutions ou personnes (tribunaux, armée, fonctionnaires, dépositaires de l'autorité publique etc.).

Le respect de la présomption d'innocence

L'article 9-1 du Code civil rappelle que : « Chacun a droit au respect de la présomption d'innocence.

---

[155] Articles 29 et suivants de la loi du 29 juillet 1881.
[156] Article 35 de la loi du 29 juillet 1881, *exceptio veritatis*.
[157] Article 35 bis de la loi du 29 juillet 1881.
[158] Article 32 de la loi du 29 juillet 1881.

Lorsqu'une personne placée en garde à vue, mise en examen ou faisant l'objet d'une citation à comparaître en justice, d'un réquisitoire du procureur de la République ou d'une plainte avec constitution de partie civile, est, avant toute condamnation, présentée publiquement comme étant coupable de faits faisant l'objet de l'enquête ou de l'instruction judiciaire, le juge peut, même en référé, ordonner l'insertion dans la publication concernée d'un communiqué aux fins de faire cesser l'atteinte à la présomption d'innocence, sans préjudice d'une action en réparation des dommages subis ».

Le respect de la vie privée et du droit à l'image

L'article 9 du Code civil consacre le droit au respect de la vie privée. Il s'agit d'un principe important en droit français.

Les faits relatifs à la vie sentimentale, à la maternité, à l'état de santé, à la religion, à l'adresse personnelle ne peuvent pas être divulgués sans le consentement des personnes concernées.

La jurisprudence a également consacré un droit à l'image : toute personne, fut-elle artiste de spectacle, peut, sur le fondement du droit au respect de la vie privée, s'opposer à la diffusion sans son autorisation expresse, de son image, considérée comme un attribut de sa personnalité[159].

Concernant les photographies prises dans un lieu public, la publication de la photographie doit être justifiée par la relation d'un événement d'actualité[160].

La réalisation et la publication de photographies de biens, propriétés privées, exposées au public est en principe libre, sinon il y aurait atteinte à la liberté de communication et d'expression. Il ne faut pas cependant que cette publication porte atteinte à la vie privée ou dénature la personne du propriétaire du bien[161].

Par exemple, une atteinte à la vie privée a été retenue dans le cas d'un journal ayant publié la photographie de la résidence privée parisienne de la famille de Monaco avec l'adresse de cet immeuble[162].

L'utilisation à des fins publiques sans autorisation du propriétaire de l'image d'un immeuble peut être jugée constitutive d'un abus si elle laisse croire que le propriétaire s'est prêté contre rémunération à la publicité[163].

Si une personne a consenti à une utilisation déterminée de son image, l'autorisation donnée ne couvrira pas nécessairement des modes de publication non prévus dans l'autorisation.

L'autorisation donnée pour la publication par voie de presse ne comprendra donc pas nécessairement la diffusion d'une photographie sur l'Internet et l'utilisation d'une photographie dans un contexte dévalorisant est fautive[164].

Le fait d'accepter de poser pour une photographie et de consentir ainsi à la prise d'un cliché n'emporte pas nécessairement autorisation de le publier[165], ou encore le fait de poser pour un photographe même professionnel, ne vaut pas abandon des droits sur l'image[166].

Ce principe est illustré par la procédure diligentée le 5 juillet 1996 par un groupe de modèles à l'encontre du service en ligne Compuserve.

---

[159] Paris 25 octobre 1982, D 1983.363, note Lindon.
[160] TGI Paris 5 janvier 1994, JurisData n°040196.
[161] Sur la photographie des biens, voir : P. Kayser, L'image des biens, D 1995.291.
[162] TGI Paris 1re Ch. 2 juin 1976, D 1977.364.
[163] Aix 1re Ch. 18 janvier 1993, Bull. Aix 1993-1, p.11.
[164] TGI Paris 15 février 1984, JurisData n°041036 : photographie de la personne utilisée pour figurer dans la catégorie des forcenés dans le jeu "la tête de l'emploi".
[165] TGI Paris 7 février 1994, JurisData n°040200.
[166] Paris 8 décembre 1993, JurisData n°024089.

Il est reproché à Compuserve d'avoir diffusé et commercialisé sur un de ses services des photographies sans autorisation. Les personnes photographiées sont des jeunes filles envisageant de devenir mannequins, qui avaient posé pour des photographes lors d'un « photoday », événement qui permet aux participants (photographes et modèles) d'exercer leurs talents. La participation à ces « photodays » n'emporte pas autorisation de commercialiser les photographies obtenues.

Le mémoire en demande invoque la gravité du préjudice subi par les jeunes filles en raison du caractère international de la diffusion. Compuserve est en effet une société de services en ligne qui revendique des accès dans 185 pays du monde à plus de 4,7 millions d'utilisateurs. Pour les demandeurs, la diffusion des photographies sur les services de Compuserve constitue un cas d'atteinte à la vie privée à l'échelle internationale[167].

Comme cette affaire le montre, la prudence s'impose avant de diffuser des photographies de personnes sur l'Internet. La photographie peut en outre être couverte par des droits d'auteur[168].

Enfin, l'article 226-1 du Code pénal punit d'un an d'emprisonnement et de 300 000 francs d'amende « le fait, au moyen d'un procédé quelconque, volontairement de porter atteinte à l'intimité de la vie privée d'autrui :

1° en captant, enregistrant ou transmettant, sans le consentement de leur auteur, des paroles prononcées à titre privé ou confidentiel ;

2° en fixant, enregistrant ou transmettant sans le consentement de celle-ci, l'image d'une personne se trouvant dans un lieu privé ».

La responsabilité du fait de l'information diffusée

La diffusion d'une information peut engager la responsabilité de son auteur[169]. La responsabilité sera contractuelle si le fournisseur du service est lié par un contrat de fourniture d'information aux utilisateurs du service. Le fait d'accéder à un service est-il suffisant pour que l'on puisse considérer qu'il y a contrat ?

A la différence de ce qui se passe en matière télématique, le fournisseur de service sur l'Internet ne reçoit pas nécessairement de rémunération liée à la connexion de l'utilisateur sur son site. En l'absence de contrepartie, et de volonté claire manifestée par l'utilisateur, il ne semble pas que l'on puisse parler de relation contractuelle.

L'étendue de la responsabilité contractuelle du fournisseur d'information dépend des obligations décrites dans le contrat et de l'objet de l'information.

Le fait de fournir des informations périmées et sommaires peut être constitutif d'une faute. En l'absence de contrat, la responsabilité est engagée sur le fondement de la responsabilité dite délictuelle[170] : il faut que l'information diffusée soit constitutive d'une faute, qu'elle porte préjudice à un tiers et qu'il y ait un lien de causalité entre la faute et le préjudice.

Il y a notamment faute dans les cas suivants :

L'information est vraie mais tendancieuse

Il a été jugé qu'il y avait faute dans le cas de critiques gastronomiques témoignant d'un parti pris de dénigrement[171].

---

[167] C. Louder v. Compuserve Inc., Robert Schwartz, Go Graphics, case n° BC 153274, Los Angeles Superior Court, texte du mémoire posté par : Eugène Volokh,<VOLOKH@LAW.UCLA.edu>, the Complaint in the Models v. Compuserve case, Law and Policy of Computer Communications, Cyberia-L, <cyberia-l@listserv.aol.com>, 15 juillet 1995.

[168] Voir infra

[169] Voir Géraldine Danjaume, la responsabilité du fait de l'information, JCP éd. G 1996, I, 3895.

[170] Articles 1382 et suivants du Code civil.

[171] TGI Lyon 18 mars 1994, D 1994, I.R.149.

L'information est vraie mais dangereuse

La publication de *Suicide, mode d'emploi* aurait pu engager la responsabilité de son auteur en raison du caractère dangereux des informations communiquées à des non-spécialistes[172].

On peut également citer le cas de l'affaire dite de la ciguë[173] : un éditeur a été condamné pour avoir commercialisé un ouvrage sur les fruits et plantes comestibles, dont la lecture fut à l'origine d'un empoisonnement, une lectrice ayant pris de la ciguë pour une carotte sauvage sur la foi d'une photographie (les plantes se ressemblent). Le tribunal a considéré que l'éditeur avait fait preuve d'un comportement fautif et « créé une situation dangereuse, en diffusant avec légèreté un ouvrage de vulgarisation comportant des lacunes ».

L'application de ce principe à l'Internet pourrait s'avérer délicat, compte tenu de son audience potentielle. Il n'y a pas de raison d'empêcher par exemple médecins et chimistes de communiquer sur leur spécialité par ce moyen. Les livres et les cours de chimie ne sont pas interdits. Une distinction pourrait être faite selon que l'information est vulgarisée de telle sorte qu'elle vise explicitement à délivrer des informations dangereuses pour la santé à des profanes, ou qu'elle est donnée en termes techniques.

Il faudrait également prouver le lien entre l'information donnée sur l'Internet et le préjudice subi.

L'information est erronée, fausse

En matière historique, la jurisprudence considère que « l'auteur d'une œuvre relatant des faits historiques engage sa responsabilité à l'égard des personnes concernées lorsque la présence des thèses soutenues manifeste(…) un mépris flagrant de la vérité »[174].

La jurisprudence impose aux professionnels, notamment aux journalistes et sociétés de renseignements commerciaux de vérifier le sérieux de leurs informations[175].

Tous ces principes sont susceptibles de s'appliquer à l'Internet. Cependant, même si la responsabilité encourue par l'éditeur d'une information peut sembler large, en pratique, il faut qu'il y ait un enjeu suffisamment important pour que la victime d'une information inexacte entame une procédure. Les décisions citées concernent l'information émise par des professionnels, ou des livres publiés par des éditeurs.

Des critères différents pourraient être dégagés selon que l'information est diffusée à titre professionnel ou non.

L'emploi de la langue française

La loi du 4 août 1994 relative à l'emploi de la langue française[176] rend obligatoire l'emploi de la langue française « dans la désignation, l'offre, la présentation, le mode d'emploi ou d'utilisation, la description de l'étendue de garantie d'un bien, d'un produit ou d'un service, ainsi que dans les factures et quittances » et dans « toute publicité écrite, parlée ou audiovisuelle ».

Les infractions à ces dispositions sont punies de peines d'amende[177].

Ces dispositions sont applicables lors de la commercialisation en France de biens, produits ou services, quelle qu'en soit l'origine. Elle apparaît donc applicable à tous les services d'information à vocation commerciale mis en place par les entreprises sur l'Internet. Une

---

[172] Géraldine Danjaume, La responsabilité du fait de l'information, JCP éd. G 1996, I, 3895, n°16.
[173] TGI Paris 28 mai 1986, D 1986, Flash n°25.
[174] Civ. 1re 15 juin 1994, JCP éd. G 1994, IV, 2077.
[175] TGI Paris 24 avril 1984, D 1985, I.R. 47.
[176] Loi n° 94-665.
[177] Décret n°95-240 du 3 mars 1995.

circulaire ministérielle[178] précise que ces dispositions sont destinées à assurer la protection du consommateur[179] et que les factures et autres documents échangés entre professionnels, personnes de droit privé françaises ou étrangères qui ne sont pas consommateurs ou utilisateurs finaux ne sont pas visés[180].

Cette réserve aura toutefois peu vocation à s'appliquer à l'Internet, dans la mesure où les services peuvent être indifféremment consultés par des professionnels ou des non-professionnels. En cas de traduction du service, la version française devra être « aussi lisible, audible et intelligible que la présentation en langue étrangère »[181].

Ne sont en revanche pas concernés les services d'information non commerciaux, par exemple un site Web d'information touristique sur une région mis en place par un office du tourisme.

L'entreprise qui souhaiterait utiliser l'Internet comme outil de promotion vis à vis de citoyens étrangers est donc néanmoins obligée de maintenir une version en langue française.

Les règles particulières en raison du produit ou du service offert

Les réglementations particulières en raison de la nature du produit ou du service en cause sont nombreuses. A cet égard, l'Internet ne doit pas être traité de manière différente des autres supports.

La publicité en ligne

Principes communs

La publicité en ligne doit respecter les règles générales applicables à l'activité publicitaire.

Notion de publicité

La publicité peut être définie comme l'ensemble des moyens employés pour faire connaître une entreprise, pour vanter un produit.

En pratique, il ne sera pas toujours aisé de distinguer la publicité proprement dite, à finalité incitative, de l'information.

En jurisprudence, la publicité a pu être définie comme « tous les moyens d'information et de suggestion à effet collectif utilisés par une entreprise afin d'acquérir, maintenir ou développer sa clientèle »[182], considérée comme s'appliquant à toute sollicitation du public, rémunérée ou non[183], à l'envoi ou la remise à des clients de documents commerciaux[184], à des annonces émanant de particuliers non-professionnels[185], à des annonces effectuées par

[178] Circulaire du 19 mars 1996, JO du 20 mars 1996.
[179] Article 2-1-3 de la circulaire, préc.
[180] Article 2-1-1 de la circulaire, préc.
[181] Article 4 de la loi du 4 août 1994.
[182] Limoges, 28 janvier 1977, décision citée par Me J.C. Fourgoux, La réglementation générale, n° spécial sur la publicité, Gaz. Pal. 27 mai 1993, p.11.
[183] Grenoble 8 octobre 1981, Rev.Conc.Cons. 1982, n°18-19.
[184] Crim. 21 mai 1974 D 1974.579.
[185] Crim. 24 mars 1987, Bull. Crim., p.385.

voie d'affiche (exemple : affichage des prix), même si elles ont un caractère purement informatif[186].

La notion de publicité est donc entendue largement et concerne toute offre de biens ou de services.

Le support de la publicité importe peu : la publicité peut être écrite, diffusée par la télévision, la radio, et même verbale[187].

La simple mise en place sur un site Web d'une plaquette d'information sur une entreprise constitue une forme de publicité. Constitue également une forme de publicité, l'envoi de prospectus par courrier électronique, ainsi que les annonces à des fins commerciales effectuées dans les forums de discussion[188].

Les règles de la Netiquette en matière de publicité

La Netiquette réprouve l'envoi de mailings publicitaires.

L'envoi de messages à caractère commercial dans les newsgroups est plus ou moins toléré, mais il existe des groupes qui acceptent les annonces commerciales[189].

La raison principale tient à ce que c'est le destinataire qui paie le coût des communications. Certains fournisseurs d'accès font même payer leurs clients en fonction du volume ou du nombre des messages reçus. La publicité peut également être comparée à une intrusion déplacée dans une discussion.

A titre anecdotique, on peut citer le cas de la société américaine Bridgestone (BFS), en conflit avec les syndicats. Des membres d'un syndicat ont imaginé poster sur Usenet de faux messages publicitaires prétendument émis par BFS. La publicité commerciale n'étant pas toujours très appréciée, ces envois ont généré en retour de nombreux messages de protestation de la part des internautes[190].

Ces règles ne résultent pas de la législation nationale, mais de l'autorégulation. Une violation de ce règles n'est pas sanctionnée juridiquement mais peut entraîner une réaction négative de la part des utilisateurs : mauvaise image de marque, messages de protestation par retour de courrier électronique.

L'exemple de ce cabinet d'avocats américain Canter & Siegel, qui avait, il y a quelques années, posté un message sur tous les groupes de news pour vanter ses services en matière de droit de l'immigration, ce qui déclencha une campagne de dénigrement à son encontre et amena son fournisseur d'accès à lui supprimer son accès, est souvent cité[191].

L'entreprise doit adapter sa stratégie commerciale aux spécificités de la communication sur l'Internet, elle doit également prendre en compte les règles de la Netiquette.

Ces règles sont des règles de bon sens et de politesse. Juridiquement, leur transgression entraîne la réprobation des internautes, comme la méconnaissance des règles de politesse entraîne la réprobation du corps social. On peut qualifier ces règles d'usage de l'Internet. Or les usages peuvent devenir source de droit[192] : le Code civil renvoie aux usages locaux en matière rurale et foncière (exemple : hauteur des clôtures, article 664 du Code civil ; distance des plantations, article 671 du Code civil), les usages professionnels tendent à régir les rapports des membres de la même profession dans l'exercice de celle-ci, les usages

[186] Crim. 2 octobre 1985, Bull. Crim., n°290.
[187] Crim. 13 décembre 1982, Bull. Crim., p.767.
[188] Sur les sollicitations par courrier électronique, voir infra
[189] Groupes de la hiérarchie <biz> ou groupes <fr.biz.produits> ou <fr.biz.publicite> par exemple.
[190] Robert W.Hamilton,<Robert_W._Hamilton@JONEDAY.COM>, Impersonation Torts, in Law and Policy of Computer Communications, Cyberia-L, <cyberia-l@listserv.aol.com>, 13 août 1996.
[191] Olivier Andrieu et Denis Lafont, Internet et l'Entreprise, éditions Eyrolles, 1995, p. 213.
[192] Gérard Cornu, Droit civil, Introduction, Les personnes, Les biens, précis Domat, éditions Montchrestien, 1988, n°423 et suivants.

conventionnels servent à définir dans les contrats, les obligations implicites (article 1135 du Code civil).

Ces règles de la Netiquette ont d'ailleurs reçu une consécration : la Chambre de commerce internationale (CCI) a récemment publié un guide du marketing interactif (ICC Guideline on interactive marketing communications)[193]. Dans ses recommandations, la CCI invite les commerçants à respecter Usenet en tant que lieu de rencontre public qui a ses propres usages et standards en ce qui concerne les messages commerciaux. En particulier, la CCI conseille d'éviter de poster de manière inconsidérée sur les forums sans tenir compte de leurs règles relatives à la publicité.

L'interdiction de la publicité mensongère

« Est interdite toute publicité comportant sous quelque forme que ce soit, des allégations, indications ou présentations fausses ou de nature à induire en erreur, lorsque celles-ci portent sur un ou plusieurs des éléments ci-après : existence, nature, composition, qualités substantielles, teneur en principes utiles, espèce, origine, quantité, mode et date de fabrication, propriétés, prix et conditions de vente de biens ou services qui font l'objet de la publicité, conditions de leur utilisation, résultats qui peuvent être attendus de leur utilisation, motifs ou procédés de la vente ou de la prestation de services, portée des engagements pris par l'annonceur, identité, qualités ou aptitudes du fabricant, des revendeurs, des promoteurs ou des prestataires ».[194]

La publicité trompeuse est un délit puni d'une amende de 250 000 francs et/ou d'un emprisonnement de 2 ans[195]. Cette interdiction s'applique bien évidemment à la publicité effectuée sur l'Internet. Notamment, lorsqu'une entreprise crée un site Web, elle devra veiller à ce que la présentation de ses produits et services ne puisse pas être considérée comme fausse ou de nature à induire en erreur.

A cet égard, l'interdiction englobe toute forme d'expression et vise aussi bien les textes écrits que les dessins, les photographies, les accompagnements sonores. La jurisprudence considère par exemple qu'il y a publicité trompeuse en cas de disproportion entre des mentions attractives et des mentions restrictives[196] ou lorsque l'image est trompeuse.

Ainsi, l'image qui n'est pas accompagnée d'un texte explicatif, ou un agrandissement d'un petit objet non signalé peut induire en erreur. Par exemple, est mensongère la publicité pour un zoom constituée de six clichés avec agrandissement progressif des personnes photographiées sans préciser que celles-ci s'étaient rapprochées du photographe[197].

Un tribunal a considéré qu'il y avait publicité mensongère si les produits mis en vente ne correspondaient pas à la photographie de ceux présentés sur le dépliant publicitaire[198].

Les entreprises doivent être particulièrement attentives à ce type de problèmes lorsqu'elles utilisent des photographies et dessins pour représenter les produits et services offerts. Il faut en effet savoir que les couleurs, tailles des caractères et des photographies, l'aspect général des pages Web varient en fonction du logiciel de l'utilisateur, de son ordinateur et de son écran.

Il pourrait par exemple s'avérer nécessaire de compléter les photographies par des mentions écrites indiquant plus précisément la dimension exacte et les couleurs des produits, pour éviter toute ambiguïté.

---

[193] Disponible sur le site Web de la CCI à : <http://www.1.usa1.com/~ibnet/897state.html>, 12 juin 1996.
[194] Article L121-1 du Code de la consommation.
[195] Articles L121-6 et L213-1 du Code de la consommation.
[196] Crim. 3 janvier 1983, Consommateurs Actualités 1983, n°402 : disproportion entre la mention "5 ans de garantie" et les conditions particulières de cette garantie.
[197] Crim. 26 mars 1984, Bull. Crim., p.322.
[198] TGI Saint-Etienne 11 fèvrier 1988, BID 1988, n°7, p.48.

La loyauté de la publicité

L'article 11 du Code international des pratiques loyales prévoit que :

« La publicité doit pouvoir être nettement distinguée, comme telle, quels que soient la forme et les supports utilisés ; lorsque le message publicitaire est diffusé dans les médias qui comportent également des informations ou des articles rédactionnels, il doit être présenté de telle façon que son caractère publicitaire apparaisse instantanément. »

Le Bureau de vérification de la publicité a repris cette règle dans ses recommandations[199].

Les usages professionnels ont ainsi consacré le principe de la loyauté de la publicité : la frontière entre publicité et information doit être nettement tracée. Cette règle de base a été reprise par les lois sur la presse écrite et télévisuelle. L'article 43 de la loi du 30 septembre 1986 relative aux services audiovisuels soumis à déclaration précise que « les messages publicitaires diffusés par les services mentionnés au présent article doivent être présentés comme tels ».

Ce principe de la loyauté devrait donc également être respecté pour la publicité sur l'Internet.

Régimes particuliers

Il existe plusieurs réglementations particulières en raison de la nature particulière du service ou du produit offert, pour des motifs d'ordre public (exemple : armes à feu), de santé publique (exemple : médicaments), de protection du consommateur (exemple : services financiers). Je ne vais pas examiner toutes ces réglementations particulières[200]. Le principe général est qu'elles s'appliquent indépendamment du support utilisé, y compris sur l'Internet.

Je prendrai à titre d'illustration la réglementation concernant le tabac et l'alcool.

Il peut également exister des régimes spéciaux en raison du support utilisé. Il convient d'examiner si ces régimes particuliers concernent l'Internet.

En fonction du support

La télévision

Il existe des règles particulières en matière de publicité et de parrainage pour les services de télévision, définies par un décret du 27 mars 1992[201]. Les services de communication audiovisuelle autorisés sont soumis au contrôle du CSA.

Le décret du 27 mars 1992 définit la publicité comme « toute forme de message télévisé diffusé contre rémunération ou autre contrepartie (…) ».

C'est bien la publicité télévisée qui est concernée par ce texte et non toute forme de publicité audiovisuelle.

La radio

Le décret du 6 avril 1987[202] fixe le régime applicable à la publicité et au parrainage des émissions des services privés de radiodiffusion sonore par voie hertzienne terrestre ou par satellite.

Un autre décret fixe le régime des services de radio distribués par câble [203].

Tous ces décrets ne s'appliquent pas aux radios diffusant sur les réseaux informatiques, sauf si elles étaient diffusées à partir de ces supports particuliers.

---

[199] Identification de la publicité, GIP, septembre 1989.
[200] Pour une vue d'ensemble, voir Lamy économique 1996, n°2197 et suivants.
[201] Décret n° 92-280.
[202] JO du 7 avril 1987.
[203] Décret n° 87-796 du 29 septembre 1987, JO du 30 septembre 1987.

La presse écrite

La loi du 1er août 1986 prohibe la publicité financière clandestine, et ce que l'on désigne par « publicité rédactionnelle », qui doit être précédée de la mention « publicité « ou « communiqué ». Cette loi ne concerne que la presse écrite[204].

La publicité visible d'une voie ouverte à la circulation

Une loi du 29 décembre 1979 réglemente la publicité, les enseignes et pré-senseignes visibles de toute voie ouverte à la circulation : rues, routes, autoroutes, voies ferrées, etc.

Bien que l'on fasse parfois référence aux « autoroutes » de l'information pour désigner les réseaux informatiques, il est évident que cette réglementation ne concerne que les voies pouvant être empruntées de manière physique.

En fonction du produit

Le tabac

Depuis le 1er janvier 1993, toute publicité relative au tabac est interdite sauf exceptions limitées pour les points de vente[205], les infractions à ces dispositions étant punies d'une peine d'amende de 500 000 francs.

Cette interdiction ne s'applique pas seulement à la publicité directe, mais également à toute propagande directe ou indirecte en faveur du tabac. Compte tenu de la sévérité de la loi, elle semble exclure en pratique toute évocation en des termes positifs du tabac qui pourrait être considérée comme une incitation à fumer.

L'alcool

Il existe un certain nombre de sites Web consacrés aux vins et au champagne[206]. Ces services, qui ne sont pas nécessairement français, dispensent des informations sur les vins et l'œnologie, et offrent également du vin à la vente.

En matière de publicité pour l'alcool, les règles suivantes sont applicables.

L'article L17 du Code des débits de boisson énumère les cas où la propagande et la publicité pour les boissons alcoolisées sont autorisées.

Parmi les moyens autorisés figurent :

- la presse écrite, sauf dans les publications destinées à la jeunesse ;
- la radiodiffusion sonore pour les catégories de radio et dans les tranches horaires déterminées par décret (des restrictions inapplicables sur l'Internet où en tout état de cause, le service est accessible en permanence).
- « Sous forme d'envoi par les producteurs, les fabricants, les importateurs, les négociants, les concessionnaires ou les entrepositaires, de messages, de circulaires commerciales, de catalogues et de brochures, dès lors que ces documents ne comportent que les mentions prévues à l'article L18 et les conditions de vente des produits qu'ils proposent. »

Les « messages » incluent les messages transmis par Minitel[207]. On peut considérer que cette énumération inclut la publicité sur l'Internet.

L'article 18 limite les mentions que peut comporter la publicité autorisée en faveur des boissons alcoolisées : indication du degré volumique d'alcool, de l'origine, de la dénomination, de la composition du produit, du nom et de l'adresse du fabricant, des agents et dépositaires ainsi que du mode d'élaboration, des modalités de vente et du mode de consommation du

[204] Voir infra
[205] Loi n°91-32 du 10 janvier 1991.
[206] Olivier Puech, « L'Internet sans modération », *Planète Internet* n° 6 mars 1996, p.48.
[207] JO déb. Sénat 14 décembre 1990, p.5060.

produit, ainsi que les références relatives aux terroirs de production et aux distinctions obtenues.

En outre toute publicité, à l'exception de celle destinée aux professionnels, doit être assortie d'un message précisant que l'abus d'alcool est dangereux pour la santé.

Toutes ces dispositions doivent évidemment être respectées par les éditeurs de services Web commerciaux consacrés aux vins. Les non-professionnels amateurs de vin qui réaliseraient un site sur le vin devraient veiller à ce que les informations données ne comportent pas d'incitation à la consommation d'alcool.

Les infractions aux dispositions examinées sont punies d'une peine d'amende de 500 000 francs.

La publicité transfrontière

Dans la mesure où un service Internet est accessible depuis différents pays, la publicité va être soumise à des réglementations nationales diverses.

Publicité étrangère reçue en France

Il suffit que la publicité soit reçue ou perçue en France pour que la réglementation en matière de publicité s'applique[208].

Or, les législations étrangères peuvent se révéler moins contraignantes que la législation française en matière de publicité.

Ainsi, la publicité pour le tabac, même si elle est réglementée, est autorisée aux Etats-Unis (une situation qui pourrait changer), et au Canada[209]. Au niveau européen, une directive du 3 octobre 1989 relative à la télévision transfrontière[210] soumet la publicité pour l'alcool à des conditions restrictives applicables à tous les Etats membres de la Communauté. En matière de tabac, il existe une proposition de directive qui prévoit l'interdiction de la publicité pour le tabac[211].

Toutefois, l'Internet n'est pas limité à l'Europe.

La question de la réception en France de publicités interdites s'est posée à propos de la télévision, notamment au sujet de retransmissions d'événements sportifs ayant lieu à l'étranger où apparaissent des marques de boisson et de tabac. La chaîne américaine CNN, que l'on reçoit sur le câble, diffuse parfois des publicité pour l'alcool prohibées à la télévision française. En matière de tabac, une décision a interdit la rediffusion de compétitions sportives se déroulant dans des pays dont le régime publicitaire pour ces produits est moins strict, dès lors que ces images sont diffusées en France[212].

Le législateur a dû intervenir pour autoriser les retransmissions télévisées des compétitions de sport mécanique qui se déroulent dans des pays où la publicité pour le tabac est autorisée[213].

Dans un autre domaine, on peut également citer le cas de la publicité comparative, qui n'est autorisée en France que sous certaines conditions (elle doit porter sur des produits et services de même nature, elle doit être limitée à une comparaison objective et ne porter que sur des caractéristiques essentielles, significatives, pertinentes et vérifiables des biens ou services, et

[208] Article L121-5 du Code de la consommation.
[209] O. Hance, Business et Droit d'Internet, Best Of Editions 1996, p. 130.
[210] JOCE L289 du 17 octobre 1989.
[211] JOCE C 129 du 21 mai 1992.
[212] TGI Quimper, Référé, 6 novembre 1992, Gaz. Pal. 19 et 20 mai 1993, p.27.
[213] Article 7 de la loi n° 93-121 du 27 janvier 1993.

l'annonceur doit communiquer avant toute diffusion sa publicité aux professionnels concernés)[214]. Dans d'autres pays, la publicité comparative peut être soumise à des conditions différentes : strictement encadrée en Italie, elle n'est pas réglementée par un texte spécial au Royaume-Uni[215].

Il est évident qu'à moins de supprimer l'Internet en France, il n'est pas en pratique possible d'empêcher que des services Internet localisés dans d'autres pays fassent de la publicité conforme à la législation qui leur est applicable, même si celle-ci est moins sévère que la loi française.

Le problème est plus délicat si l'entreprise qui a mis en place un site a des filiales ou des établissements dans plusieurs pays, car les tribunaux français ont alors la possibilité de poursuivre les filiales établies en France.

Quelle réglementation respecter ?

La publicité étrangère reçue en France doit en théorie respecter la loi française, mais l'inverse est également vrai. Par exemple, dès lors que les Emirats Arabes Unis, pays où l'alcool est strictement prohibé, est connecté à l'Internet, il ne devrait pas y avoir de site Web consacré au vin. Cet exemple est extrême, mais le principe reste qu'en théorie, toutes les réglementations étrangères en matière de publicité ont vocation à s'appliquer.

Cela est en pratique impossible à respecter. Cet aspect du droit de la publicité doit cependant être pris en compte par une entreprise qui disposerait d'établissements dans plusieurs pays et commercialiserait des produits et service susceptibles de rentrer dans une catégorie faisant l'objet d'une réglementation particulière, et notamment les services financiers, assurances, médicaments, tabac, alcool, activités juridiques, médicales, comptables.

Un exemple des difficultés soulevées par cette multiplicité des lois applicables à la publicité sur l'Internet nous est fournit par les avocats américains, qui sont soumis à des règles en matière de publicité, différentes selon l'Etat où ils exercent. Il ne leur est même pas possible de faire le choix de respecter la législation la plus sévère, dès lors que les conditions posées d'un Etat à l'autre sont parfois contradictoires[216].

Au niveau européen, une harmonisation des règles en matière de publicité commerciale est envisageable. Il existe par exemple des propositions sur la pratique de la publicité comparative[217]. Le guide de la CCI sur le marketing interactif, sans prendre position sur la question de l'application extra-territoriale de la législation en matière de publicité précise que les communications commerciales devraient être « légales », en ce sens qu'elles devraient respecter les lois du pays dont la communication est originaire.

Jeux, loteries, concours

Les sociétés utilisent comme technique de promotion des ventes la participation à des jeux variés faisant intervenir à des degrés divers le hasard. Les jeux organisés par les entreprises sont régis par une loi du 21 mai 1836, toujours en vigueur.

Sont prohibés les jeux répondant aux conditions cumulatives suivantes :

- passant par une offre faite au public ;
- exigeant un sacrifice pécuniaire ;
- jouant sur l'espérance d'un gain ;
- faisant intervenir, même partiellement, le hasard.

---

[214] Articles L121-8 à L121-13 du Code de la consommation.
[215] O. Hance, Business et Droit d'Internet, Best Of Editions 1996, p. 385, note 28.
[216] William E.Hornsby, Jr., The Ethical Boundaries of Selling Services in Cyberspace, <http://www.computerbar.org/netethics/abawill.htm>.
[217] O. Hance, Business et Droit d'Internet, Best Of Editions 1996, p. 133.

La condition de l'offre au public est facilement remplie sur l'Internet dès lors que le service de communication ne présente pas un caractère privé.

L'espérance d'un gain est l'essence même des jeux. Les concours qui ne donnent aucune place au hasard, même minime, sont licites.

Les jeux entièrement gratuits sont licites.

Il suffit d'une participation financière même infime du joueur, pour que le jeu soit prohibé. La dépense d'un timbre a été considérée comme constitutive d'un sacrifice[218].

Les jeux offerts par voie télématique impliquent une participation financière, liée au temps de connexion[219]. Ce raisonnement est-il applicable aux jeux offerts sur l'Internet ? Beaucoup d'utilisateurs ont accès à l'Internet par un modem et paient donc leur communication téléphonique pour se connecter. Même si le prix d'une communication téléphonique est bien inférieur au prix d'une connexion sur un service télématique, la prohibition des loteries semple pouvoir s'appliquer à l'Internet, sauf si le jeu ne fait pas intervenir le hasard ou ne joue pas sur l'espérance d'un gain.

Les offres d'emploi

On trouve sur l'Internet des offres et des demandes d'emploi. Deux forums Usenet sont consacrés à l'emploi : <fr.emplois.offres>, qui reçoit des offres de France, de Suisse, du Canada et de Belgique, et <fr.emplois.demandes>.

Pourtant l'article L311-4 du Code du travail précise qu'« il est interdit à toute personne de faire connaître ses offres ou demandes d'emploi soit par voie d'affiche apposée en quelque lieu que ce soit, soit par tout autre moyen de publicité ».

Toutefois, les insertions d'offres et de demandes d'emploi dans la presse sont autorisées, sous certaines conditions : caractère public de l'origine de l'annonce (la levée de l'anonymat doit être possible), communication simultanée des offres à l'ANPE, interdiction des mentions discriminatoires, respect des règles concernant la surface occupée par les offres ou demandes d'emploi dans le journal.

La notion de presse au sens de cette loi vise les journaux, revues ou écrits périodiques, c'est-à-dire la presse écrite[220].

Toutes les annonces relatives à l'emploi que l'on trouve sur Minitel sont tolérées en l'absence de base légale expresse[221].

Il devrait en être de même sur l'Internet en attendant qu'une loi ne vienne un jour clarifier la situation.

Pourquoi cette interdiction, qui peut sembler quelque peu surprenante en période de chômage ?

Elle est fondée sur deux principes :

- éviter le placement (défini comme la mise en relation en vue de la conclusion d'un contrat de travail) rémunéré, la simple diffusion d'annonces n'étant pas considérée comme un placement ;
- respecter le rôle du service public confié à l'ANPE.

[218] Douai 20 septembre 1990, BRDA 1990/22 p. 8.
[219] Lamy informatique n° 1915.
[220] JO déb. Sénat 10 septembre 1987 p.1246.
[221] Bertrand Wallon, Télématique et offres d'emploi, Droit Social n°6, juin 1989, p.488.

Les droits d'auteur

Les concepteurs de sites d'information, notamment de sites Web, les utilisateurs de l'Internet sont confrontés sans cesse à la question des droits d'auteur, qu'il s'agisse de savoir l'usage qu'ils peuvent faire du travail d'autrui, des données en tous genres qu'ils trouvent sur l'Internet, des œuvres que l'on peut se procurer hors réseau, ou qu'il s'agisse de savoir si ce qu'ils créent et mettent sur l'Internet est protégé par le droit d'auteur.

Les œuvres protégées

La notion d'œuvre

Les droits d'auteur sont un ensemble de droits appartenant à l'auteur et à ses ayants droit (éditeurs, producteurs, cessionnaire, héritiers, etc.).

Les droits d'auteur s'appliquent à toute œuvre de l'esprit, quels qu'en soient le genre, le mérite ou la destination[222].

Sont par exemple protégées les œuvres littéraires (livres, brochures, dictionnaires), musicales, architecturales, les peintures, dessins, photographies, et également l'emballage du Pont-Neuf par Christo[223], les cartes postales, les jeux vidéos[224], les conférences, les cartes géographiques, les logiciels. Des dessins de carrosserie, un modèle de panier à salade[225], un décapsuleur[226] se sont vu reconnaître la protection du droit d'auteur.

La notion d'œuvre de l'esprit est donc particulièrement large.

Pour qu'une œuvre de l'esprit soit protégée par le droit d'auteur, il faut qu'elle soit originale, c'est-à-dire qu'elle soit le reflet de la personnalité de l'auteur, d'une activité créatrice propre. Les simples idées ne sont pas protégées par le droit d'auteur, qui protège en revanche l'expression, la mise en forme des idées. Pour reprendre l'exemple de Christo, si l'emballage du Pont-Neuf est une œuvre protégée, cet artiste ne dispose pas d'un monopole sur l'idée d'emballer des monuments dans un tissu[227].

Pour bénéficier de la protection reconnue par le droit d'auteur, aucune formalité n'est exigée, l'œuvre est protégée du seul fait de sa création. Nul besoin d'un dépôt ou d'apposition de la mention « copyright » ou « tous droits réservés ». L'absence de mention sur une photographie, un article ne signifie pas qu'ils peuvent être utilisés librement, mais sa présence est recommandée. Elle permet notamment de repérer aisément qui est titulaire des droits et en droit américain, elle permet d'obtenir des dommages et intérêts plus élevés en cas de procès.

Il ne faut pas confondre le terme « copyright » éventuellement désigné sous le symbole © ou le terme « copyright » que l'on appose sur une œuvre pour indiquer qu'elle est protégée et que son exploitation n'est pas libre, et le copyright désignant la législation sur le droit d'auteur dans les pays anglo-saxons.

Tous les types d'œuvres que l'on peut trouver sur l'Internet sont ainsi protégés par le droit d'auteur : photographies, extraits musicaux, graphismes, articles…

Les messages postés dans les services de discussions publiques (newsgroups, listes de diffusion) peuvent être également des œuvres de l'esprit protégeables par le droit d'auteur, s'ils sont originaux.

---

[222] Article L112-1 du Code de la propriété intellectuelle.
[223] Paris, 14e Ch. 13 mars 1986, Gaz. Pal. 1986, I, p.238.
[224] Assemblée plénière, 7 mars 1986, affaire Atari, D.1986.405.
[225] Crim. 2 mai 1961, D.1962.502 note Greffe.
[226] Crim. 9 octobre 1974, RIDA, juillet 1975, p.176.
[227] TGI Paris, 26 mai 1987, Légipresse mars 1989, n°59,III, p.21 note Dérieux.

L'URL est-il protégé par le droit d'auteur ?

L'URL est un fait, une donnée brute, comme une adresse ou un numéro de téléphone, il n'est donc pas à ce titre protégé par le droit d'auteur[228].

Il n'y a pas de raison d'écarter les sites Web de la liste très variée des œuvres de l'esprit. Un site Web peut être protégé par le droit d'auteur dès lors qu'il constitue un ensemble original. Les éléments distincts tels que photographies, logos, textes, utilisés pour composer le site peuvent relever à titre individuel du droit d'auteur.

Le site Web peut être qualifié de ce que l'on appelle œuvre multimédia[229], laquelle présente deux caractéristiques :

- il s'agit d'une œuvre numérisée qui peut combiner textes, images fixes et animées, vidéo, programmes informatiques ;
- il s'agit d'une œuvre appréhendée de manière interactive, on n'accède pas directement à l'œuvre prise dans sa globalité, mais par l'intermédiaire d'un logiciel de navigation, aux différentes données composant l'œuvre multimédia arrangées de manière arborescente.

Un site Web est par la nature même du protocole utilisé pour le construire, le HTML, conçu pour relier les données grâce à des liens hypertextes et hypemédia, de nature interactive. Il s'agit bien évidemment d'une œuvre numérisée, à laquelle on peut intégrer aussi bien du texte et de l'image (cas le plus fréquent), que du son ou de la vidéo.

Le site Web peut également être rattaché à une catégorie voisine mais distincte du droit d'auteur : la base de données.

Les bases de données

Une directive européenne concernant la protection juridique des bases de données a été récemment adoptée, le 11 mars 1996[230]. Cette directive doit être transposée en droit français avant le 1er janvier 1998.

La directive définit les bases de données comme :

« 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 d'une autre manière »(article premier).

La directive précise en outre que « les bases de données qui, par le choix ou la disposition des matières, constituent une création intellectuelle propre à leur auteur sont protégées comme telle par le droit d'auteur » (article 3-1).

La directive ne vise pas le contenu de la base, mais la structure de la base qui, par le choix ou la disposition des matières constitue une création intellectuelle propre à son auteur. Cette création est protégée indépendamment de la protection éventuellement applicable au contenu[231].

Un service Web semble bien pouvoir relever du champ d'application de ce texte[232]. De l'avis de plusieurs juristes ayant commenté la directive, une œuvre multimédia doit pouvoir être rangée dans la catégorie des bases de données[233].

---

[228] P.J. Benedict O'Mahoney, Web Issues, Copyright Website, <http://www.benedict.com>, 13 novembre 1995.

[229] Les œuvres multimédia suscitent une abondante littérature juridique en raison des questions multiples qu'elles soulèvent en droit d'auteur. On peut citer par exemple :
P.Y. Gautier, Les œuvres multimédia en droit français, RIDA 1994, n°160 p.91 ;
X. Linant de Bellefonds (sous la direction de), Le multimédia face au droit, édition Des Parques 1995 ;
F. Olivier et E. Barby, Le multimédia à l'épreuve du droit français, JCP éd. G 1995, II, n°3879 ;
P. Sirinelli, Industries culturelles et nouvelles techniques, Rapport au Ministère de la culture, Documentation française 1994.

[230] Directive 96/9/CE JOCE N° L77 du 27 mars 1996.

[231] M.A. Gallot Le Lorier, Banques de données et droit d'auteur, Gaz.Pal., 18 juin 1996, p. 4.

[232] En ce sens : O.Hance, Business et Droit d'Internet, Best of Editions 1996, p. 78.

Les droits conférés à l'auteur

Les droits moraux

L'auteur dispose de droits moraux qui présentent la particularité en droit français d'être perpétuels et inaliénables : seul l'auteur et, après sa mort, ses héritiers peuvent revendiquer ces droits moraux.

Le droit moral comporte :

- le droit de première divulgation, seul l'auteur a le droit de rendre publique et d'autoriser l'exploitation de l'œuvre qu'il a créée (article L121-2 du CPI) ;
- le droit au respect de son nom et de sa qualité pour toute utilisation publique d'une œuvre, même dans l'hypothèse où l'auteur a cédé ses droits d'exploitation à un tiers ;
- le droit au respect de l'œuvre. Ce droit vise à protéger l'intégrité de l'œuvre qui ne doit pas être dénaturée, modifiée, altérée, mutilée ou sortie de son contexte. Par exemple, le fait de superposer un logo lors de la télédiffusion d'un film[234], ou de coloriser sans autorisation, un film conçu en noir et blanc[235] ont été considéré comme une atteinte à l'intégrité de l'œuvre.

Il n'est pas inintéressant de préciser que le Copyright américain ne comprend aucune reconnaissance spécifique de ce droit, qui est en revanche reconnu dans les pays de l'Union européenne et au Canada de manière plus ou moins marquée. Mais la France a la conception la plus dogmatique de ces droits moraux[236].

Les droits patrimoniaux

Ce sont les droits qui permettent à l'auteur d'obtenir une rémunération pour l'exploitation de son œuvre et de déterminer comment son œuvre sera exploitée.

Ils comportent :

Le droit de reproduction

La reproduction consiste dans la fixation matérielle de l'œuvre par tout procédé qui permet de la communiquer au public d'une manière indirecte (article L122-3 du CPI) : impression, dessin, photographie, enregistrement mécanique, cinématographique ou magnétique.

Le droit de représentation

Il s'agit du droit de communiquer l'œuvre au public par un procédé quelconque (article L122-2). La télédiffusion, qui est une forme de représentation, est définie par le Code de la propriété intellectuelle comme « la diffusion par tout procédé de télécommunication de sons, d'images, de documents, de données et de messages de toute nature ».

Les droits des auteurs de bases de données

Le fabriquant d'une base de données, en plus de la protection éventuellement accordée par le droit d'auteur, a le droit d'interdire l'extraction et/ou la réutilisation de la totalité ou d'une partie substantielle, évaluée de façon quantitative ou qualitative, du contenu de la base de

---

[233] Claude Retornaz, La position commune arrêtée par le Conseil, le 10 juillet 1995, sur la protection juridique des bases de données, Cahiers Lamy droit de l'informatique, janvier 1996, (I), n° 47 ; Nathalie Mallet-Poujol, La directive concernant la protection juridique des bases de données : la gageure de la protection privative, Droit de l'informatique et des télécoms, 1996/1, p. 7 n°5.

[234] Paris 25 octobre 1989, D 1990, som.54.

[235] Civ. 1re 28 mai 1991, affaire "Asphalt Jungle", JCP 91 éd. G., II, n° 21 732.

[236] Olivier Hance, Business et Droit d'Internet, Best Of Editions 1996. p.80.

données, lorsque l'obtention, la vérification ou la présentation de ce contenu attestent un investissement substantiel du point de vue qualitatif ou quantitatif (article 7 de la directive).

A priori cette disposition concerne plutôt les grandes bases de données informationnelles, puisqu'un « investissement substantiel » est exigé pour que ce droit de s'opposer à la réutilisation des données s'applique.

L'utilisation d'œuvres protégées par le droit d'auteur

Les concepteurs de sites Web doivent être particulièrement attentifs lorsqu'ils utilisent des œuvres dites préexistantes. En effet, toute représentation ou reproduction intégrale ou partielle, traduction, adaptation, transformation, arrangement d'une œuvre réalisée sans le consentement de l'auteur ou de ses ayants droit (héritiers et cessionnaires des droits d'auteur comme les éditeurs et les producteurs, sociétés de gestion des droits d'auteur) est illicite (article L122-4 du CPI).

Contrairement à ce que l'on a pu entendre dans les médias à propos de l'affaire Gübler[237], il n'y a ni vide juridique ni zone de non-droit en la matière, les droits d'auteur s'appliquent à l'Internet comme aux autres supports de diffusion des œuvres.

Or lorsqu'une œuvre est intégrée dans un site Internet, il y a à la fois reproduction et représentation.

La mémorisation des données dans la mémoire de l'ordinateur est une forme de reproduction, de l'avis unanime des juristes[238].

La question de savoir si il y a représentation est plus discutée. La mise à disposition des utilisateurs de textes, images, et aujourd'hui de son semble bien être une forme de communication de l'œuvre au public[239], une interprétation qu'autorisent les termes très généraux du texte concerné[240].

La numérisation d'une œuvre, impliquant la codification en signes binaires et donc une modification de l'œuvre, implique non seulement des actes de reproduction, mais encore des actes d'adaptation ou de modification qui sont également soumis à autorisation à ce titre.

L'utilisation d'une œuvre pour l'incorporer dans un site d'information nécessite à la fois d'obtenir les droits de reproduction et de représentation.

Il a ainsi été jugé que la mise à disposition sur un site Web d'œuvres de Michel Sardou et de Jacques Brel (il s'agissait notamment de textes de leurs chansons) constituait une reproduction et une utilisation collective de ces œuvres. En l'absence d'autorisation des titulaires des droits d'auteur sur ces œuvres, les éditeurs des deux sites concernés ont reçu interdiction de mettre sur leurs sites de telles œuvres à disposition des utilisateurs du réseau[241]. A l'occasion de ces affaires, le juge a autorisé la diffusion d'un communiqué à la presse rappelant que « toute reproduction par numérisation d'œuvres musicales protégées par le droit d'auteur susceptible d'être mise à la disposition de personnes connectées au réseau Internet doit être autorisée expressément par les titulaires ou cessionnaires des droits ».

---

[237] Quelques jours après la mort de François Mitterrand, les éditions Plon ont publié un livre rédigé par le docteur Gübler, ancien médecin personnel de François Mitterrand, et M. Gonod, journaliste, dans lequel le médecin révélait que le président Mitterrand se savait atteint d'un cancer depuis le début de son premier septennat. La famille Mitterrand a obtenu en référé l'interdiction de ce livre à la vente, pour atteinte à la vie privée, décision confirmée en appel. Quelques jours après l'interdiction prononcée par le tribunal, le responsable d'un cybercafé bisontin prenait l'initiative, en invoquant la liberté d'expression, de reproduire le livre et de le mettre en libre accès sur son site Web. Le livre était ensuite repris sur des sites américains et anglais, notamment sur le site du MIT, une prestigieuse université américaine, à l'initiative d'un libertaire américain, toujours au nom de la liberté d'expression.
De nombreux articles ont été consacrés à cette affaire dans la presse lorsqu'elle a éclaté, voir par exemple : Meryem Marzouki, Besançon, paradis du surf et Valérie Sédallian et Philippe Langlois, « Le grand secret le plus partagé du monde », *Planète Internet* n°6 mars 1996, p. 80 et 28.

[238] Voir Lamy droit de l'informatique 1996, n° 546.

[239] Lamy droit de l'informatique 1996, n°569.

[240] Alain Bensoussan (sous la direction de), Internet, Aspects juridiques, éditions Hermès 1996, p.45.

[241] TGI Paris, ordonnance de référé, 14 août 1996, Affaire Michel Sardou, REF 60139/96, et affaire Jacques Brel, REF 60138/96, D 3 octobre 1996.

Les exceptions au principe de l'autorisation préalable

Il existe cependant des exceptions au principe de l'autorisation préalable que je vais maintenant examiner :

Le domaine public

Cinquante ans après la mort de l'auteur[242], les droits d'exploitation cessent et l'œuvre tombe dans le domaine public. Le projet Gutenberg aux Etats-Unis ou l'Association des bibliophiles universels en France[243] ont ainsi entrepris de numériser et de diffuser sur l'Internet les grandes œuvres du patrimoine littéraire tombées dans le domaine public[244].

Le droit de citation

L'article L122-5 du CPI autorise « sous réserve que soient indiqués clairement le nom de l'auteur et la source, les analyses et courtes citations justifiées par le caractère critique, polémique, pédagogique, scientifique ou d'information de l'œuvre à laquelle elles sont incorporées ».

Le droit de citation est donc soumis à des conditions précises : la citation doit être brève, elle doit mentionner le nom de l'auteur et la source, elle doit répondre à un des critères énoncés, elle doit faire partie d'une œuvre distincte.

Le droit de citation doit être manié avec prudence. Conçu à l'origine pour les œuvres littéraires, son application à d'autres genres s'avère plus délicate.

En matière de citation d'œuvres d'art, la jurisprudence est particulièrement restrictive[245].

Par exemple, saisie d'une affaire concernant la reproduction, dans le catalogue d'un commissaire priseur en vue de leur vente, d'œuvres du peintre Maurice Utrillo, elle a considéré que « la reproduction d'une œuvre, quel que soit son format, ne peut s'analyser en une courte citation »[246].

Au sujet d'une diffusion par Antenne 2, dans une émission consacrée aux chefs-d'œuvre en péril, des statues de Maillol installées aux Tuileries, la Cour de cassation a posé le principe que « la représentation d'une œuvre située dans un lieu public n'est licite que lorsqu'elle est accessoire par rapport au sujet principal représenté ou traité », ce qui n'était pas le cas dans cette affaire, les statues ayant été considérées comme volontairement présentées pour elles-mêmes[247]. La Cour de cassation a confirmé cette jurisprudence en jugeant que ne constituait pas une courte citation autorisée par la loi la diffusion d'œuvres d'un peintre au cours d'une émission de télévision qui était consacrée à l'actualité théâtrale et avait montré pendant 49 secondes sur une émission d'une heure des peintures murales se trouvant dans le théâtre des Champs-Elysées[248].

Cette jurisprudence empêche toute reproduction sans autorisation d'une œuvre d'art, qu'il s'agisse de peintures, de photographies, de sculptures, d'œuvres architecturales, sauf dans l'hypothèse où cette reproduction aurait été l'accessoire d'un sujet principal, par exemple si elle se fond dans le paysage environnant. Elle fondée sur l'idée que l'œuvre d'art est un tout indivisible.

---

[242] Un projet de loi prévoit de faire passer ce délai à 70 ans.
[243] Site Web : <http://www.cnam.fr/ABU>.
[244] Michel Arseneault, « Internet nouvelle académie française », *le Monde*, supplément multimédia, 29 janvier 1996, p.27.
[245] Sur les questions soulevées par la reproduction des œuvres d'art, voir P. Kayser, l'Image des biens, D1996.291.
[246] Assemblée plénière 5 novembre 1993, D 1994.481.
[247] Cass. 1re, 4 juillet 1995, D1995, IR.201.
[248] Civ. 1re 4 juillet 1995 JCP G 1995, II, n° 22486

Vous pourriez par exemple inclure une photographie de la tour Eiffel dans votre site (œuvre du domaine public), mais pas de la pyramide du Louvre, ou de la géode de la Villette sans l'autorisation des architectes.

En matière musicale, il n'existe pas de décision qui se soit prononcée sur la question du droit de citation. On peut penser qu'elle devrait être possible dans le respect des conditions légales[249], mais les auteurs ne sont pas unanimes.

La question se pose également en matière de citation d'œuvres vidéo.

Dans les cas où les citations sont autorisées, peut-on faire une œuvre constituée d'un grand nombre de citations ?

La question s'est posée dans une affaire « Microfor c/ *le Monde* ». La société Microfor avait réalisé un répertoire indexant des articles de presse et des articles du *Monde diplomatique*. L'indexation était effectuée par mots-clés, par ordre chronologique avec une fiche signalétique qui reprenait des citations de chaque article. La Cour de cassation a estimé que la société Microfor avait pu réaliser sa banque de données sans le consentement du journal *le Monde*.

En effet, elle a jugé que « les résumés constitués uniquement de courtes citations de l'œuvre ne dispensaient pas le lecteur de recourir à celle-ci, étaient indissociables de la section analytique de la publication par le jeu de renvois figurant dans cette section, et que cet ensemble avait le caractère d'une œuvre d'information[250] ».

La copie privée

Sont autorisées « les copies ou reproductions strictement réservées à l'usage du copiste et non destinées à une utilisation collective » (article L122-5 2° du CPI). Cette exception concerne les seules copies à usage personnel faites à l'initiative du copiste.

Dans l'affaire évoquée ci-dessus concernant la reproduction d'œuvres de Michel Sardou et de Jacques Brel[251], les éditeurs du site ont invoqué pour leur défense qu'ils avaient effectué les reproductions en cause pour leur seul usage personnel sur leur « domicile privé virtuel » que constituait selon eux leur site Web.

Cette argumentation a été rejetée par le juge pour lequel la mise à disposition à des utilisateurs de l'Internet d'œuvres protégées par le droit d'auteur favorise l'utilisation collective desdites œuvres.

L'exception de la copie privée ne peut donc concerner la mise à disposition d'œuvres sur un site de communication publique.

La solution est différente en ce qui concerne les logiciels pour lesquels ne sont pas autorisées les copies privées mais seulement les copies de sauvegarde (article L122-6 du CPI).

Les œuvres musicales

Pour la diffusion d'œuvres musicales, le régime de l'autorisation préalable est remplacé par un régime de redevance. Cette redevance est perçue par la SACEM[252] auprès de toute personne diffusant de la musique, et est calculée en fonction du chiffre d'affaires et de l'activité. Initialement prévu pour la radiodiffusion (article L214-1 du CPI), ce régime a été étendu à la télévision par la jurisprudence. Il sera certainement étendu à la diffusion d'œuvres sur l'Internet. Laurence Bony, responsable des services média audiovisuel à la SACEM a précisé

---

[249] L. Bochurberg, Le droit de citation en matière audiovisuelle, Gaz. Pal. 28 octobre 1995 ; Vivant, Pour une compréhension nouvelle de la notion de courte citation en droit d'auteur, JCP éd. G 1989, I, n°3372.

[250] Assemblée plénière, 30 octobre 1987.

[251] TGI Paris, ordonnance de référé, 14 août 1996, affaire Michel Sardou, REF 60139/96, et affaire Jacques Brel, REF 60138/96, D 3 octobre 1996.

[252] Société des auteurs compositeurs et éditeurs de musique, 225, avenue Charles de Gaulle, 92521 Neuilly.

que « l'Internet n'échappe pas à la réglementation stricte des autres supports, radio et télévision par exemple »[253].

Le redevable de la redevance est le diffuseur, c'est-à-dire logiquement l'éditeur du site et non la personne, quel que soit son statut, qui fournit de l'accès à l'Internet.

La SACEM semble toutefois considérer que le fait de mettre des ordinateurs connectés au réseau Internet à la disposition du public équivaut à la diffusion des œuvres musicales que l'on peut télécharger sur l'Internet. Sont notamment visés les cybercafés[254]. Cependant, si cette interprétation était confirmée, toutes les personnes qui fournissent des accès à l'Internet devraient payer une redevance à la SACEM pour diffusion d'œuvres musicales ! En réalité, ce sont les utilisateurs qui vont éventuellement télécharger des œuvres musicales sur le réseau, et non les cybercafés qui diffusent de la musique auprès de leurs clients.

Les droits des utilisateurs sur les œuvres en libre accès sur l'Internet

Le Web

Un site Web peut être considéré comme une œuvre intellectuelle protégée par le droit d'auteur.

Il en résulte logiquement que l'on ne peut pas reproduire librement, recopier, distribuer, commercialiser ce que l'on trouve sur les sites Web des autres.

Cependant, il est logique que tous les actes de reproduction nécessaires à la consultation du site Web soient autorisés. Le fait de sauvegarder des pages Web sur son propre disque dur et de les imprimer porte-t-il atteinte au droit d'auteur ? Cette pratique courante ferait-elle de tous les internautes des pirates ?

Une première réponse est de considérer que cela relève du droit de faire des copies privées, pour son usage personnel.

La doctrine américaine développe également l'idée de « la licence implicite » : la personne qui met en libre accès un site Web sur l'Internet autorise implicitement de telles utilisations, ce qui ne signifie pas qu'elle autorise les utilisateurs à faire tout ce qu'ils veulent du matériel qu'ils trouvent sur les sites Web[255]. Cependant, cette doctrine de l'autorisation implicite pourrait être accueillie avec plus de réticence dans les pays européens et notamment en France[256].

Une autre solution serait d'appliquer le principe posé par la directive sur les bases de données qui prévoit que l'utilisateur légitime d'une base de données couverte par le droit d'auteur peut effectuer tous actes de reproduction permanente ou provisoire, de traduction, d'adaptation, qui sont nécessaires à l'accès au contenu de la base et à son utilisation normale par lui-même sans l'autorisation de l'auteur de la base (article 6-1 de la directive).

On peut également relever que techniquement, c'est le serveur (Web ou FTP) qui envoie les données en direction de l'usager, de sa propre volonté, et non l'usager qui vient les chercher : il se contente de les demander.

Les forums public

Même un message posté dans un forum de discussion peut bénéficier de la protection du droit d'auteur s'il est original, et son auteur devrait autoriser toutes les reproductions de ses messages, un principe assez problématique lorsque l'on connaît le mode de propagation des messages sur les serveurs de news. L'idée est que lorsque vous postez un message, vous

[253] Propos cités par Xavier de Moulins-Beaufort, « Chantons sur le Web », *le Monde*, supplément multimédia 15 avril 1996, p. 29.
[254] Lettre de la SACEM à l'Internet café, Marseille, du 2 septembre 1996.
[255] Oppendahl and Larson, Web Law FAQ, <http://www.patents.com/weblaw.sht>, 3 mars 1996.
[256] O. Hance, Business et Droit d'Internet, Best Of Editions 1996, p. 89.

donnez la permission aux serveurs de news de recopier vos messages. Comme pour les services Web, ces reproductions sont nécessaires pour que les messages puissent être consultés par les autres.

Les différents logiciels utilisés ont également la particularité de permettre avec une grande facilité de reprendre des messages déjà postés et de les rediffuser sur d'autres groupes de discussion. Cette pratique courante n'est pas conforme à la stricte application du droit d'auteur. La théorie de la doctrine implicite considère que l'on donne l'autorisation implicite de reposter un message d'un forum à un autre forum ayant pour thème des sujets similaires[257].

Lorsqu'il est répondu à un message, le nom de l'auteur original d'un message n'est pas toujours cité. Il y a cette fois atteinte au droit moral (droit à la paternité)[258].

Cela sans compter les problèmes théoriques soulevés par les sites qui archivent les messages postés dans des forums : devraient-ils obtenir l'autorisation de tous les auteurs des messages ?

En réalité, dans toutes ces hypothèses, le droit d'auteur semple peu adapté, et les réponses pourraient davantage venir de la Netiquette que de la loi sur le droit d'auteur.

Les logiciels

En droit français et européen, l'utilisateur d'un logiciel a le droit, lorsque cela est nécessaire à l'utilisation du logiciel, d'accomplir des actes nécessaires à la correction des erreurs, d'en déterminer les idées et principes qui sont à sa base, de le décompiler aux fins d'interopérabilité[259].

Sur l'Internet, de nombreux logiciels sont distribués en freeware ou en shareware. Quels sont les droits de l'utilisateur sur ces logiciels en libre accès ?

Un freeware est un logiciel dont les droits d'utilisation sont gratuits. Cela ne signifie pas que le logiciel est dans le domaine public. L'auteur du logiciel n'a aucunement cédé ses droits d'exploitation. La commercialisation est éventuellement autorisée dans les conditions fixées par l'auteur, qui peut interdire la vente pour un prix supérieur au coût du support et aux frais de distribution. La licence dite GNU, la plus fréquente chez les « freeware », autorise la revente à n'importe quel prix, mais interdit d'interdire la redistribution.

Le shareware est un logiciel qui est mis à disposition du public contre paiement d'une redevance dont l'utilisateur n'est obligé de s'acquitter que s'il est satisfait du logiciel. Le fait de continuer à utiliser le logiciel après la période de test sans avoir payé la rétribution demandée est en principe illicite. On voit également apparaître les « pizzaware », les « beerware », les « postcardware », où la rémunération normalement acquittée par l'utilisateur dépend de l'imagination de l'informaticien : paiement en pizza, en bière, par l'envoi d'une carte postale.

Lorsque le logiciel est ainsi téléchargé, il peut comprendre une notice, qui constituera alors la licence d'utilisation du logiciel téléchargé. Toute utilisation non conforme à la licence est alors illicite.

Les sanctions

« Toute reproduction, représentation, diffusion, par quelque moyen que ce soit, d'une œuvre de l'esprit en violation des droits de l'auteur tels qu'ils sont définis et réglementés par la loi

---

[257] P.J. Benedict O'Mahoney, Newsgroups, Copyright Website, <http://www.benedict.com>, 4 juin 1995.

[258] Mark A. Lemley, Rights of Attribution and Integrity in Online Communications, 1995, Journal of Online Law, <http://warthog.cc.wm.edu/law/publications/jol/>, article 2, § 12 et s.

[259] Article L122-6-1 du CPI et directive du 14 mai 1991 concernant la protection juridique des programmes d'ordinateur, JOCE 17 mai 1991, n° L122, p.42.

est une contrefaçon » (article L335-3 du CPI) et « toute représentation ou reproduction intégrale ou partielle faite sans le consentement de l'auteur ou de ses ayants droit ou ayants cause est illicite. Il en est de même pour la traduction ou la transformation, l'arrangement ou la reproduction par un art ou un procédé quelconque » (article L122-4 du CPI).

L'auteur a le choix entre exercer des poursuites civiles pour obtenir des dommages et intérêts et des poursuites pénales, car la contrefaçon est un délit pénal passible de 2 ans d'emprisonnement et de 2 millions de francs d'amende (article L335-2 du CPI).

Les plaignants peuvent faire pratiquer des saisies, dans les conditions prévues par la loi (articles L332-1 et suivants). Il s'agit généralement de saisies d'exemplaires de l'œuvre contrefaite en vue d'une procédure ultérieure.

Concernant les infractions commises sur l'Internet en matière de droit d'auteur, les sociétés d'auteurs peuvent être autorisées à se doter d'agents assermentés qui pourront dresser des constats d'infraction.

Par arrêté du ministre de la Culture en date du 21 mars 1996, l'APP, Agence pour la protection des programmes, une association qui s'occupait traditionnellement de logiciels, a été ainsi autorisée à avoir des agents assermentés autorisés à constater les infractions au droit d'auteur sur l'Internet.

Elle étend son champ d'action à toute œuvre numérique et non seulement aux logiciels. Les nouveaux pouvoirs reconnus à l'APP ont été utilisés par des éditeurs à la demande desquels des procès-verbaux de constats d'infraction de publication illicites de textes ou de chansons appartenant au répertoire de Jacques Brel et de Michel Sardou, ont été dressés le 16 juillet 1996[260].

Ce n'est pas parce que de nombreux actes de contrefaçon commis sur l'Internet ne sont pas poursuivis que l'impunité est assurée et les poursuites engagées contre quelques uns pourraient servir d'exemple aux autres.

Aspects internationaux

La plupart des pays ont une législation en matière de droit d'auteur, même si les règles ne sont pas identiques d'un pays à l'autre. Le problème vient toutefois de ce que certains pays, notamment asiatiques, sont plus laxistes en matière de poursuite des infractions au droit d'auteur. Il existe également plusieurs conventions internationales ayant pour vocation de permettre une protection minimale et quasi planétaire des œuvres[261].

Les deux principales sont :

- la Convention de Berne du 9 octobre 1886, plusieurs fois révisée ;
- la Convention de Genève du 6 septembre 1952.

Le traité de la Convention de Berne est géré par l'OMPI, Organisation mondiale de la propriété intellectuelle, dont le siège est à Genève.

[260] Communiqué de presse de l'APP du 25 juillet 1996.

[261] Voir Claude Colombet, Le droit international de la propriété littéraire et artistique, Précis de propriété littéraire et artistique, éditions Dalloz, 7e édition, 1994, n° 441 et s.

La création de sites Web

Les difficultés posées par la législation en matière de droit d'auteur aux créateurs de sites Web

Identification des titulaires des droits

Le premier obstacle auquel le concepteur d'un site va se heurter va être d'identifier le titulaire des droits d'auteur. Il n'existe pas d'organisme qui répertorie toutes les œuvres, comme l'INPI en matière de marques et brevets, dès lors qu'une œuvre intellectuelle est protégée indépendamment de toute formalité. Pour remédier à ce type de problème, il existe divers projets comme le projet SESAM d'instituer un centre d'administration collective des droits qui permettrait de s'adresser au même organisme pour obtenir les autorisations et s'acquitter du paiement des droits d'auteur. SESAM serait une société regroupant plusieurs sociétés françaises d'auteurs[262]. C'est ce que l'on appelle la gestion collective des droits. Cette formule de la gestion collective pose cependant un certain nombre de difficultés pratiques et juridiques à sa mise en œuvre[263].

Les autorisations nécessaires

L'autorisation va nécessiter de conclure un contrat écrit, et chacun des droits cédés doit faire l'objet d'une mention distincte dans l'acte de cession. Le domaine d'exploitation des droits cédés doit être délimité quant à son étendue et sa destination, quant au lieu et quant à la durée (article L131-3 du CPI).

Une autorisation est-elle nécessaire lorsque l'on possède déjà des droits d'exploitation d'une œuvre ?

Tout dépend de ce qui aura été prévu dans le contrat déjà signé. Le principe est que l'autorisation donnée pour un support n'est pas nécessairement valable pour une diffusion sur d'autres supports. Le CPI précise que la cession du droit de représentation n'emporte pas celle du droit de reproduction, la cession du droit de reproduction n'emporte pas celle du droit de représentation, et que lorsqu'un contrat comporte cession totale de ces droits, la portée en est limitée aux modes d'exploitation prévus au contrat (article L122-7 du CPI).

Cette règle pose des problèmes aux éditeurs de journaux pour la mise en place de leurs sites Web. Les journaux veulent en effet pouvoir utiliser les mêmes articles et photographies que ceux utilisés pour la version papier de leur magazine. Or, notamment pour les articles écrits par les journalistes, le principe est que la rémunération accordée au journaliste pour sa collaboration ne couvre, sauf convention expresse, que la première publication. Tout autre reproduction, adaptation, sous quelque forme que ce soit, ne peut être faite sans l'autorisation de l'auteur et paiement d'un droit[264]. Cette règle est également valable pour les journalistes salariés[265].

Le problème se pose également pour les photographes, et plusieurs procès ont opposé aux Etats-Unis des photographes en free-lance à des magazines qui avaient réutilisé des photographies fournies par ces photographes sans qu'aucun contrat de cession de droits ne soit

---

[262] A côté de la SACEM pour la musique, il existe d'autres sociétés d'auteurs pour chaque catégorie d'œuvre comme la SACD (Société des auteurs compositeurs dramatiques), 11 bis rue Ballu, 75 009 Paris ou la SCAM (Société civile des auteurs multimédia), 38 rue du Faubourg Saint-Jacques (audiovisuel).

[263] Sur la gestion collective voir par exemple :

Dr P. Bernt Hugenholtz, Droits de licence dans un environnement multimédia digital, et Jean-Loup Tournier, L'avenir de la gestion collective des droits d'auteur, interventions à un colloque organisé par la Commission consultative juridique de la commission européenne, la société de l'information : droit d'auteur et multimédia, Luxembourg, le 26 avril 1995, disponibles sur le Web, respectivement à : <http://oops.ip.lu/legal/fr/950426/hugenh.html#H> et <http://oops.ip.lu/legal/fr/950426/tournier.html#H> ;

P. Sirinelli, Industries culturelles et nouvelles techniques, Rapport au ministère de la Culture, Documentation française 1994.

[264] Abrégé du droit de la presse, édition du Centre de formation et de perfectionnement des journalistes, 1994, p.106.

[265] Article L761-9 du Code du travail.

signé. Dans l'affaire Playboy Entreprises v. Dumas, un tribunal américain a retenu qu'en l'absence de convention expresse, l'usage de l'industrie du magazine fait que les droits sur les photographies ne sont cédés que pour la première publication[266].

Les contrats avec les journalistes et les photographes vont devoir être renégociés, mais les auteurs peuvent refuser la cession des droits de diffusion en ligne sans compensation supplémentaire. La bataille fait actuellement rage aux Etats-Unis entre les journalistes et les magazines. Le groupe de presse américain Time a ainsi conclu un accord l'année dernière avec la moitié de ses photographes qui ont obtenu que leur forfait journalier passe de 400 dollars à 500 dollars pour, en contrepartie, autoriser Time à utiliser leurs photographies sans percevoir de nouveaux droits, dans le cas où les publications du groupe étaient diffusées sur de nouveaux supports numériques. En France, la FNAPPI, (Fédération nationale des agences de presse, photos et informations) est en litige avec les encyclopédies Bordas qui ont utilisé les mêmes photographies pour l'encyclopédie papier que pour leur CD-Rom.[267]

La rémunération

La cession par l'auteur des droits sur son œuvre doit comporter une participation proportionnelle aux recettes provenant de la vente ou de l'exploitation (article L131-4 du CPI). Ce principe ne va pas être aisé à appliquer à la diffusion en ligne, et la détermination de l'assiette de la rémunération proportionnelle peut poser de nombreuses difficultés tant juridiques que pratiques[268]. La Cour de cassation a indiqué que la redevance de l'auteur doit être calculée en fonction du prix de vente au public[269]. Ce critère est assez difficilement transposable lorsqu'il n'y a pas vente d'un support. En outre certains sites se rémunèrent sur la publicité, pas sur l'exploitation directe des œuvres, et un site Web n'a pas nécessairement pour objet l'exploitation des œuvres qu'il contient, à la différence du cas des CD-Rom par exemple. Certains proposent de retenir alors comme assiette pour les œuvres multimédia le chiffre d'affaires de l'éditeur[270].

La rémunération au forfait est cependant autorisée dans les cas suivants :

- la base de calcul de la participation proportionnelle ne peut être pratiquement déterminée ;
- les moyens de contrôler la participation font défaut ;
- les frais des opérations de calcul et de contrôle seraient hors de proportion avec les résultats à atteindre ;
- la nature ou les conditions de l'exploitation rendent impossible l'application de la règle de la rémunération proportionnelle, soit que la contribution de l'auteur ne constitue pas l'un des éléments essentiels de la création intellectuelle de l'œuvre, soit que l'utilisation de l'œuvre ne présente qu'un caractère accessoire par rapport à l'objet exploité ;
- en cas de cession d'un logiciel.

La rémunération au forfait pour l'exploitation d'œuvres intégrées dans un site Web semble relever des cas où la rémunération au forfait est autorisée.

Les droits moraux

L'intégration d'une œuvre dans un site Web pourrait être considérée comme une atteinte au droit moral de l'auteur si le contenu du site reflète une tendance, des valeurs qui heurtent ses convictions profondes. Il peut y avoir également dénaturation de l'œuvre, détournement de son sens premier si elle est sortie de son contexte. La numérisation, en facilitant les possibili-

---

[266] Mark F. Radcliffe, Multimedia production issues, Droit de l'informatique et des Télécoms, 1996/1 p.23.

[267] Sylvaine Villeneuve, « Auteurs en quête de droits multimédias », *Libération*, cahier multimédia, 5 janvier 1996.

[268] Voir par exemple en matière audiovisuelle, Dominique Sauret, Rémunération des ayants droit et exploitation vidéographique de l'œuvre audiovisuelle, Gaz. Pal. 12 octobre 1995, p.33.

[269] Civ. 1re, 9 octobre 1984, affaire "Masson", Bull. I, n°252.

[270] Lionel Bochurberg, Une logique du mode de rémunération selon la nature des auteurs, intervention à une conférence « Droits d'auteur et multimédia » organisée par l'Observatoire des industries du multimédia, 11 et 12 avril 1995, Paris, disponible à : <http://www.argia.fr/lij>

tés de manipulation, fait craindre les altérations susceptibles de fausser la connaissance de l'œuvre telle qu'elle a été créée : changement des couleurs, superposition de logos, insertion d'images. Il y a, dans toutes ces hypothèses, atteinte au droit moral et plus particulièrement au droit au respect de l'œuvre[271]. Le respect du droit moral dans les œuvres multimédias et en tout état de cause sur l'Internet se révèle assez délicat. Les producteurs et éditeurs considèrent que ce droit moral est un facteur d'incertitude juridique et il semble que les auteurs soient amenés un jour ou l'autre à faire des concessions en ce domaine[272].

Tous ces problèmes auxquels sont confrontés de manière aiguë les producteurs de CD-Rom et de CD-I et de banques de données, risquent, en ce qui concerne les concepteurs de sites Web, de les dissuader d'utiliser des œuvres existantes pour agrémenter leurs sites lorsqu'ils n'y sont pas obligés par l'objet de leur site.

Les entreprises qui hébergent des sites Web devront en tout cas veiller à inclure dans les contrats d'hébergement qu'il font signer à leurs clients des clauses de garantie quant à l'étendue des droits de propriété intellectuelle dont dispose le réalisateur sur le contenu de son site, au cas où leur responsabilité serait recherchée.

Une entreprise a par exemple inclus la clause suivante dans ses conditions générales d'hébergement : « L'éditeur garantit X (le serveur d'hébergement) être en propre ou par le biais de licences, titulaire de l'intégralité des droits portant sur les marques, brevets, logiciels, cités et/ou utilisés dans le contenu du service ainsi que l'ensemble des droits de propriété intellectuelle pouvant porter sur les éléments du contenu du service. » D'autres formules de clauses ont été proposées comme :

« le site <nom du serveur> déclare disposer de l'ensemble des droits de reproduction et de représentation et plus généralement des droits d'exploitation attachés aux données ou œuvres qu'il supporte (…) »[273].

Les droits sur la création du site Web

Un site Web peut constituer une œuvre relevant du droit d'auteur ou une base de données.

Qui va être titulaire des droits sur le site Web ainsi créé ?

La question se pose dans les cas suivants :

- le site est réalisé par des salariés ;
- le développement du site est confié à une société tierce spécialisée dans cette activité.

Les droits de propriété intellectuelle sur le site appartiennent-ils automatiquement à l'entreprise pour le compte de laquelle le site a été réalisé ?

L'article L11-1 du CPI nous dit : « L'existence ou la conclusion d'un contrat de louage d'ouvrage (contrat de travail) ou de service (cas des contrats de commande) n'emporte aucune dérogation à la jouissance du droit reconnu par l'alinéa 1er (droit de l'auteur sur son œuvre). »

Sauf en matière de logiciel, le fait qu'un site ait été créé par un salarié dans l'exercice de ses fonctions n'emporte pas à lui seul cession des droits d'auteur au profit de l'employeur en l'absence de convention expresse[274].

Les exceptions à ce principe concernent les logiciels (article L113-9 du CPI) et les journalistes pour la première publication de l'article.

---

[271] Philippe Langlois, Le droit moral des auteurs et l'Internet, L'Internet Juridique, <http://www.argia.fr/lij/ArticleMars3.html>, mars 1996.
[272] Hubert Bitan, Les rapports de force entre la technologie du multimédia et le droit, Gaz.Pal. 27 janvier 1996, p.12 ; Sophie Dangu, Multimédia : faut-il repenser le droit moral ? Cahiers Lamy informatique, octobre 1995, (France), p.7.
[273] Nicolas Valluet, « Portraits de contrat », interview accordée à la revue *Expertises* avril 1996, p.143.
[274] Civ.1re 16 décembre 1992, JCP éd. E 1993, I, n°246.

Or, les entreprises ne vont pas nécessairement penser à faire signer des contrats de cession de droits à leurs employés.

Cependant, le site réalisé par des salariés sur instruction de leur employeur peut recevoir la qualification d'œuvre dite collective :

« est dite collective l'œuvre créée sur l'initiative d'une personne physique ou morale qui l'édite, la publie et la divulgue sous sa direction et dans laquelle la contribution personnelle des divers auteurs participant à son élaboration se fond dans l'ensemble en vue duquel elle est conçue, sans qu'il soit possible d'attribuer à chacun d'eux un droit distinct sur l'ensemble réalisé » (article L113-2 al.3 du CPI).

Le processus de création d'un site Web peut correspondre au cas de figure envisagé par ce texte.

La directive sur les bases de données ne se prononce pas sur la question de la titularité des droits sur les œuvres réalisées par les salariés. Il appartiendra à chaque Etat de préciser éventuellement dans sa législation que « lorsqu'une base de données est créée par un employé dans l'exercice de ses fonctions ou d'après les instructions de son employeur, seul l'employeur est habilité à exercer tous les droits patrimoniaux afférents à la base ainsi créée » (considérant n°29).

Le problème se pose également pour les sites Web dont la réalisation a été confiée à une entreprise extérieure. Sauf en matière de publicité, le contrat de commande n'emporte pas à lui seul cession des droits sur le site Web. En pratique, c'est souvent la même société qui a développé le site qui l'héberge sur son serveur. La question des droits sur le site peut se poser lorsque le client décide de changer de serveur d'hébergement. En l'absence de clause dans le contrat ayant prévu le transfert des droits d'auteur, la société ayant développé le site Web peut empêcher son client de transférer son site ailleurs et de réutiliser certains éléments, notamment graphiques (logo par exemple), créés pour son site.

Les entreprises devront donc veiller à faire inclure dans les contrats de développement une clause de transfert des droits d'auteur inspirée par exemple de la clause suivante :

« De convention expresse, la propriété de l'application ci-dessus définie est attribuée au client. A cette fin, le fournisseur transfère au client, qui l'accepte, l'intégralité des droits d'exploitation ci-après décrits et relatifs à l'application précitée, à savoir : le code HTML, les logos etc.

La présente cession est consentie pour le monde entier et pour la durée des droits d'auteur.

Les droits cédés aux présentes comprennent notamment le droit de reproduction, le droit de représentation, le droit de diffusion, le droit de traduction, le droit d'adaptation, le droit d'arrangement, et ce sous toutes les formes, par tous procédés et sur tous supports, connus et inconnus à ce jour, notamment pour les réseaux et les services en ligne d'accès à distance, la presse, la publicité, l'édition et autres. »

Une application pour un site Web peut également intégrer des petits programmes informatiques : moteur de recherche, formulaire d'inscription en ligne. Il conviendra également de préciser le sort de ces petits programmes informatiques, et de prévoir également leur cession avec les éléments correspondants : code source qui est nécessaire pour pouvoir faire évoluer le programme (à la différence du code HTML, le code source des programmes informatiques inclus dans les sites ne peut pas être consulté par l'utilisateur), documentation correspondante. Toutefois, les entreprises informatiques seront certainement plus réticentes à céder leurs droits d'exploitation sur ces programmes qui reflètent leur savoir-faire.

Enfin, si certains éléments utilisés pour le site ont été commandés à une personne extérieure (photographie, logo notamment), il conviendra là aussi de prévoir une cession des droits d'auteur au bénéfice du commanditaire, qu'il s'agisse du client directement ou de l'entreprise informatique qui développe le site Web.

Les liens hypertextes

La construction de liens

Pour inclure un lien depuis un élément quelconque d'une page Web vers une autre page Web qui peut relever d'un site différent, il suffit d'inclure dans le code HTML utilisé pour décrire les pages Web la commande suivante : lien hypertexte. Il s'agit donc d'une commande vraiment élémentaire. Cette pratique constitue-t-elle une atteinte au droit d'auteur ?

La description de la commande montre l'analogie avec les citations : faire un lien c'est un peu comme citer les œuvres des autres. Il n'y a donc là rien de choquant sur le principe et les citations sont expressément autorisées par le CPI.

Réaliser une liste de lien est-il protégé par le droit d'auteur ?

C'est exactement le cas de figure des bases de données traditionnelles. Si vous mettez quelques liens sur une page Web vers d'autres sites, il n'y a pas là quelque chose de bien original, et si quelqu'un vous reprend l'idée de faire la même liste de lien, vous ne pourrez pas invoquer une atteinte au droit d'auteur.

Il s'agit d'une simple compilation non protégée en soi par le droit d'auteur[275].

En revanche, si vous avez organisé vos liens d'une manière particulière, référencé de nombreux sites, les avez classé par thème, genre, fourni quelques explications, en d'autres termes, si vous avez fait preuve d'une création intellectuelle dans le choix des liens, leur disposition, l'organisation de la structure du site, vous pouvez revendiquer une protection pour votre base de liens au titre du droit d'auteur. C'est la solution de la directive européenne.

Un site comme celui de Yahoo[276], qui n'est pas un simple moteur de recherche mais répertorie et classe les sites Web de l'Internet, est le parfait exemple de la base de données élaborée. Il s'agit même d'un exemple de base ayant nécessité un « investissement substantiel » au sens de la directive européenne. D'autres sites moins ambitieux peuvent révéler une création intellectuelle.

Les liens sur les autres sites

La question suivante qui se pose est de savoir si l'on peut faire librement des liens sur les sites des autres. En effet, à la différence de la citation, le lien hypertexte vous amène directement sur le site référencé.

La Netiquette recommande de demander l'autorisation à l'administrateur d'un site avant de faire un lien sur son site, mais cette règle est tombée en désuétude aujourd'hui. Lorsque vous mettez en place un site Web, l'objectif est bien évidemment d'obtenir le plus de référencement possible.

Le principe est donc que les liens sur les sites des autres peuvent en principe être effectués librement. On considère que l'éditeur d'un site donne l'autorisation implicite aux autres créateurs de pages de faire des liens sur son site. Cela résulte de la conception même du Web créé pour permettre de faire des liens hypertextes entre les documents [277].

Cependant, il est des cas où le lien est fait d'une manière telle qu'il est préjudiciable au site sur lequel le lien est fait.

---

[275] C. Retornaz, La position commune arrêtée par le Conseil, le 10 juillet 1995, sur la protection juridique des bases de données, Cahiers Lamy droit de l'informatique, janvier 1996, (I), n° 47.

[276] Site Web : <http://www.yahoo.com>.

[277] P.J. Benedict O'Mahoney, Web Issues, Copyright Website, <http://www.benedict.com>, 13 novembre 1995.

Par exemple, le lien est accompagné d'un commentaire désobligeant, ou donne une fausse idée du site sur lequel le lien est réalisé. Le cabinet d'avocats Oppendahl & Larson, qui maintient un site sur l'Internet consacré aux droits de propriété intellectuelle en fournit une illustration. Une société qui réalise des sites Web expliquait qu'elle fournissait des sites à ceux qui n'en avaient pas les moyens et pour donner un exemple avait fait un lien sur un article du cabinet d'avocat en question, ce qui donnait l'impression que ce cabinet n'avait pas les moyens d'avoir son propre site[278].

Dans ce cas, la Netiquette recommande de supprimer le lien si le site sur lequel un lien a été effectué le demande.

Cependant, le droit de critique est autorisé, et dans ce contexte, le lien accompagnant la critique devrait pouvoir être maintenu. L'article L122-5 du CPI autorise d'ailleurs les courtes citations à des fins critiques.

En donnant l'autorisation de faire des liens sur son site, donne-t-on également l'autorisation de faire des liens directement sur les pages individuelles du site ?

Certains considèrent que dans ce cas, il faut demander l'autorisation, mais en pratique, cette règle est peu respectée. Certains sites peuvent comporter des milliers de documents, si l'on ne donne pas le lien sur le document précis, le lecteur pourrait d'ailleurs ne pas retrouver le document en question facilement. C'est un peu comme lorsque l'on cite un livre sans donner la page où figure une information précise : pour la retrouver le lecteur devrait lire tout le livre.

Certains sites contiennent explicitement un avertissement au terme duquel les liens sur les fichiers individuels du site ne sont pas permis sans l'autorisation de l'administrateur du site[279].

L'idée est que, dans ce cas, l'internaute risque de ne pas avoir une connaissance directe de l'objet du Web et que la page en question risque d'être sortie de son contexte ou que le travail effectué par le créateur du site soit approprié par d'autres. Cela peut arriver si au lieu de faire un lien sur un site en expliquant ce que le site contient, le premier site fait de multiples liens sur le second site en reprenant toutes les rubriques du second, de telle sorte que l'utilisateur ne se donnera même pas la peine de voir la page d'accueil du second site, alors que c'est ce site qui a fourni en réalité tout le travail de constitution de la base de données.

En droit, ces questions pourraient s'analyser en une atteinte au droit moral du créateur du Web : atteinte au droit de paternité, ou à l'intégrité de l'œuvre selon les circonstances.

Une solution pratique à ce genre de problèmes est de mettre un lien sur la page d'accueil et d'afficher le nom de l'éditeur sur toutes les pages du site. Il est de toute façon recommandé de mettre un lien ou un texte en bas de chacune des pages d'un service Web, pour permettre à l'internaute de s'y retrouver.

Il existe un nouveau procédé pour faire des liens assez pernicieux. Lorsque l'utilisateur active un lien hypertexte réalisé avec la commande « HREF », il se connecte à une autre page, voire à un autre site. Mais la technique dite des « IMG » permet d'insérer directement en ligne des documents graphiques émanant d'un autre site, sans quitter le premier site (on dit faire des références « inline »). L'utilisateur a cette fois directement l'impression que l'élément provient de la page consultée, il n'a pas connaissance de l'existence du site d'où l'image provient[280].

Les « frames », qui permettent de diviser une page Web en plusieurs fenêtres indépendantes, permettent une appropriation du même genre.

---

[278] Oppendahl & Larson,Web law FAQ, May I freely link to the sites of others, <http://www.patents.com/weblaw.sht>, 5 février 1996.

[279] Par exemple sur le site « SPACE : Above and Beyond, <http://www.rampages.onramp.net/~brummet/space.htm> avait été insérée la mention suivante : "Inserting direct links to the individual files or file sections, without permission of sfb@netcom.com is prohibited. Linking to the page itself is both permitted and appreciated".

[280] Norderhaug, T. & Oberding, J.(1995), Hyperlinking versus Inlining, Designing a Web of Intellectual Property, Computer Networks and ISDN Systems, 27(6), p. 1037, disponible à : <http://www.ifi.uio.no/~terjen/pub/webip/950220.html>.

Ce genre de possibilités ne ravit pas tout le monde. Par exemple, un étudiant de l'université de Priceton, Dan Wallach, avait fait une page Web sur Dilbert Hack, un dessinateur humoristique américain. L'éditeur de ce dessinateur, United Media, maintient également un site sur l'Internet sur lequel il reproduit des dessins de Dilbert Hack. Dan Wallach a donc fait des références inline (en ligne) sur les bandes dessinées reproduites sur le site de United Media. Les avocats de United Media ont écrit à l'étudiant pour lui demander de retirer ces références inlines de son site, invoquant une violation des droits d'auteur de leur client. Dan Wallach a finalement obtempéré[281].

En droit, la question est de savoir s'il y a contrefaçon puisqu'il n'y a pas reproduction. En réalité, en droit français, il y a atteinte au droit de représentation, car l'œuvre est communiquée au public directement sur le site qui fait le lien inline et il y a atteinte au droit moral. Si un lien s'analyse en une citation, dans cette hypothèse, l'auteur et la source ne sont pas cités.

Avant de faire de telles références inline, il est donc recommandé de demander l'autorisation à l'administrateur du site contenant l'image sur laquelle on veut faire cette référence.

[281] Sur cette affaire voir : Dilbert Hack page Archives, <http://www.cs.priceton.edu/~dwallach/dilbert>.

La responsabilité en raison des liens se trouvant sur le site

Sans contenir d'informations prohibées par la loi française, un site peut faire des liens sur des sites qui en contiennent.

Il faut déjà distinguer selon qu'il s'agit de liens directs ou indirects.

Par exemple, le site de l'Union des étudiants juifs de France[282] contient un lien sur la rubrique Judaism du site Yahoo, lequel fait un lien dans une sous-rubrique sur l'holocauste, sur des sites véhiculant des idées révisionnistes. Le négationnisme est en effet couvert par la liberté d'expression aux Etats-Unis, et Yahoo a pour principe de donner l'accès à l'information sans porter de jugement, il classe donc également les sites du Ku Klux Klan ou des négationnistes[283].

On ne peut être responsable que de ce que l'on contrôle, et il ne serait guère réaliste de demander aux administrateurs de sites de contrôler les liens que font les sites sur lesquels ils font eux-mêmes des liens.

Qu'en est-il en ce qui concerne les liens directs ? D'un côté, lorsque l'on cite un livre, cela ne signifie pas que l'on est responsable du contenu de ce livre.

D'un autre côté, faire un lien peut donner une certaine légitimité à un site, cela signifie que ce site présente un intérêt, cela n'est donc pas totalement neutre.

Si par exemple un site officiel du gouvernement français faisait un lien sur une page Web d'un particulier critiquant les essais nucléaires, ou reproduisant une marionnette des Guignols de l'info, cela pourrait prêter à confusion.

Un autre exemple amusant nous est fournit par la campagne présidentielle américaine : Bill Clinton a fait un voyage officiel au Japon et un site Web est créé à cette occasion. Un lien a été fait depuis le site de la Maison Blanche sur le site japonais. Bob Dole reproche ce lien à Bill Clinton, arguant de ce que cela montre son manque d'indépendance vis-à-vis des Japonais. Clinton réplique que cela démontre le manque de connaissance de l'Internet de Bob Dole[284].

En droit, voir sa responsabilité engagée en raison des liens que l'on fait, semble quelque peu exagéré. Tout dépend en pratique des conditions dans lesquelles ce lien est fait. En droit civil, il faudrait que ce lien constitue une faute, et que cette faute ait occasionné un préjudice.

En droit pénal, cela semble étendre, sur le principe même, de manière déraisonnable, le champ des infractions pénales. Or, la loi pénale s'interprète strictement et toute infraction pénale doit avoir été prévue par un texte, c'est le principe de la légalité des délits et des peines.

Par exemple, faire un lien pourrait-il être assimilé à de la provocation à la haine raciale ? Soit cette provocation résulte du contenu même du site, et dans ce cas, les textes concernés s'appliquent, soit elle est le fait du site sur lequel le lien est fait. Or la provocation ne se conçoit que faite de manière directe.

On peut très bien faire des liens sur des sites dont on n'approuve pas les idées à titre de contre-exemple.

---

[282] Site Web : < http://azathoth.esil.univ-mrs.fr/~benarous/uejf.html>.

[283] Voir Jérôme Thorel, interview de Srinija Srinivasan, chargée de l'ontologie, c'est-à-dire du classement des sites chez Yahoo, « le dilemme de Srinija, Ontologiquement Yahoo », *Planète Internet* n°10, juillet/août 1996, p.33.

[284] Dole Blast Clinton for link to Japanese, Internet Political Report, =A9 1996 the Internet Guild, <report@iguild.org>.

Ainsi la Harvard Law Library (bibliothèque de droit de l'université de Harvard) a mis un place un site Web intitulé « A Guide to Hate Groups on the Internet »[285] (Un guide des sites Web des groupes « haineux » sur l'Internet).

Que l'on approuve ou non ce type de démarche typiquement américaine[286], cela montre en tout cas que tout est une question de contexte et il semble dangereux de vouloir étendre la responsabilité pénale des éditeurs de site aux liens qu'ils peuvent effectuer vers d'autres sites, sauf si la manière dont le lien était effectué pouvait lui-même être constitutif de l'infraction concernée.

En réalité, les liens effectués sur un site engagent plus l'image de marque du site que sa responsabilité.

[285] Site Web : <http://www.law.harvard.edu/library/guides/hateweb/hate.html>.

[286] L'objectif des éditeurs du site hébergés sur le serveur de la prestigieuse université de Harvard est en donnant cette liste de groupes racistes, antisémites et pronant la violence, de mieux faire comprendre et de dénoncer à leur manière ce phénomène. Le site comprend également des liens vers les organisations qui luttent contre ces groupes racistes. Les groupes référencés ne semblent guère apprécier cette contre-publicité et être ainsi montrés du doigt.

Quatrième partie

Le contrôle du flux des informations

La responsabilité des acteurs dans le flux des informations

La diffusion, la communication, la mise à disposition d'informations disponibles sur l'Internet font intervenir une variété d'acteurs : auteurs de messages, éditeurs de services Web, fournisseurs d'accès, serveurs d'hébergement, fournisseurs de services en ligne, opérateurs de télécommunication.

Avec la découverte de l'Internet par le grand public et les médias, est né un débat sur la question du contrôle des informations circulant sur les réseaux. Parmi les centaines de milliers de services existant et les millions de messages échangés chaque jour, il s'en trouvera nécessairement qui seront illégaux au regard de la loi d'un des pays dont les ressortissants sont connectés.

Les acteurs de la communication sur l'Internet sont donc susceptibles de voir leur responsabilité recherchée à des degrés divers.

Les utilisateurs, éditeurs, serveurs, fournisseurs d'accès, opérateurs localisés en France sont soumis aux lois françaises. Dans quelle mesure leur responsabilité peut-elle être engagée en raison des informations qui circulent sur l'Internet ?

Les fournisseurs de contenu

J'ai examiné la réglementation applicable aux services fournissant du contenu, qu'il s'agisse d'auteurs de messages, d'éditeurs de sites Web ou de services en ligne[287].

L'émetteur d'une information est présumé responsable du contenu de cette information. C'est donc en principe sur lui que pèse la responsabilité née de l'émission d'une information préjudiciable ou illicite.

Dans certains cas, l'auteur n'est cependant pas considéré comme auteur principal de l'infraction.

La responsabilité légale du directeur de la publication

Les services de communication publique s'analysent au regard de la loi du 30 septembre 1986 en services de communication audiovisuelle.

[287] Voir supra

Cette loi a prévu que tout service de communication est tenu d'avoir un directeur de la publication. Ce directeur de la publication doit être majeur, avoir la jouissance de ses droits civils et n'être privé de ses droits civiques par aucune condamnation judiciaire.

Lorsque le service est fourni par une personne morale, le directeur de la publication est le représentant légal de cette personne morale (gérant, président, etc.). Lorsque le service est fourni par une personne physique, le directeur de la publication est cette personne physique[288].

Le législateur a étendu aux services de communication audiovisuelle le régime de responsabilité de la presse écrite, où sont responsables à titre principal des délits commis par voie de presse les directeurs de publication et les éditeurs[289]. A leur défaut, sont responsables, dans l'ordre : les auteurs, les imprimeurs, les vendeurs, les distributeurs et les afficheurs.

L'article 93-3 de la loi du 30 septembre 1986 prévoit que lorsque l'une des infractions visées par la loi de 1881 (cas par exemple de la diffamation, de l'incitation à la haine raciale, de la négation de crimes contre l'humanité) est commise par un moyen de communication audiovisuel, le directeur de la publication est poursuivi comme auteur principal, lorsque le message a fait l'objet d'une fixation préalable à sa communication au public. L'auteur est alors poursuivi comme complice. Ce n'est qu'à défaut de directeur de la publication que l'auteur est poursuivi comme auteur principal, et à défaut d'auteur le producteur.

Ce système de responsabilité en cascade a été étendu à d'autres infractions, par exemple au délit de mise en péril des mineurs pour diffusion de messages à caractère pornographique ou violent[290].

Toutefois, dans toutes les hypothèses où il n'y a pas de directeur de la publication (messages diffusés dans les newsgroups, pages Web personnelles), ces dispositions ne jouent pas, l'auteur émetteur de l'information étant à la fois auteur, éditeur et directeur de la publication.

Elles joueront en revanche pour les services disposant d'une personne assumant la responsabilité éditoriale du service .

Listes de diffusion publiques et forums de discussion modérés

Le modérateur de la liste filtre les messages avant de les poster sur la liste ou le forum. Selon les règles en usage de ce type de services, le modérateur s'assure simplement que les messages sont en accord avec le thème du groupe de discussion, mais sans exercer de censure. La responsabilité pesant sur ces modérateurs au regard des textes pourrait soit décourager ce type d'initiatives (il s'agit de personnes bénévoles), soit les obliger à censurer davantage de messages au moindre doute.

Par exemple, le modérateur d'un newsgroup diffusant les annonces de séminaires pourrait décider de ne pas transmettre d'annonces relatives à des conférences organisées par certains groupes si l'intitulé de la conférence laissait croire que des thèmes négationnistes y seront abordés, bien que la simple annonce d'une conférence ne puisse à elle seule constituer le délit de négationnisme.

Au sujet de ces modérateurs, le rapport de l'Association des utilisateurs d'Internet souligne : « Il est important pour la survie de ce système (notamment les listes et forums modérés), de tenir compte du fait que les modérateurs sont des bénévoles qui n'ont pas de connaissance juridique dans l'immense majorité des cas. Le fait qu'ils prennent de leur temps pour rendre service à tous doit être apprécié à sa juste valeur, et dans les cas où un manque de discernement pourra leur être reproché, ils devront pouvoir faire valoir leur bonne foi.[291] » Si nul

[288] Article 93-2.
[289] Article 42 de la loi du 29 juillet 1881 sur la liberté de la presse.
[290] Article 227-24 du Code pénal.
[291] Pour une intégration sereine et un développement harmonieux d'Internet dans la société française, rapport de l'AUI, disponible à :<http://www.aui.fr/Rapports/RAUI-070696.html>, 7 juin 1996.

n'est censé ignorer la loi, le fait que le rôle du modérateur ne corresponde pas en pratique à celui d'un directeur de la publication d'un journal devrait pouvoir être pris en compte.

Sites Web

Le régime de la responsabilité du directeur de la publication, c'est-à-dire de l'éditeur du service est applicable aux sites créés par des personnes morales, qu'il s'agisse de sociétés commerciales, d'organismes de droit public ou d'associations.

Services en ligne

Les services en ligne de type Compuserve, AOL, Infonie sont responsables en tant qu'éditeurs de la publication pour la partie de leurs services qui concerne la fourniture de contenu.

Même dans les hypothèse où aucun texte de loi ne prévoit la responsabilité d'un directeur de la publication, d'une manière générale, chaque fois qu'existera à côté de l'auteur une personne assumant un rôle d'éditeur, le responsable éditorial pourra voir sa responsabilité engagée conjointement avec celle de l'auteur.

Le droit de réponse

Toujours dans le cadre de la transposition aux services de communication du régime de la presse écrite, la loi a étendu aux services de communication audiovisuelle le droit de réponse :

« Toute personne physique ou morale dispose d'un droit de réponse dans le cas où des imputations susceptibles de porter atteinte à son honneur ou à sa réputation auraient été diffusées dans le cadre d'une activité de communication audiovisuelle. »[292]

Ce texte, qui semble davantage adapté à la télévision ou à la radiodiffusion, est également applicable à l'Internet. Il ne concerne toutefois que l'atteinte à l'honneur ou à la réputation. Cela constitue une différence importante avec le droit de réponse de la presse écrite, ouvert à toute personne nommée ou désignée dans un journal, indépendamment de toute diffamation[293].

Le demandeur doit préciser les imputations sur lesquelles il souhaite répondre et la teneur de la réponse qu'il souhaite faire.

Cette demande doit être adressée par lettre recommandée avec demande d'avis de réception[294].

Le demandeur au droit de réponse doit présenter sa demande dans les 8 jours suivant la diffusion du message.

Or, concernant les services d'information, la date à laquelle le message litigieux a été mis en ligne ne va pas nécessairement être connue de la personne visée. Le décret d'application a précisé que pour les services de vidéographie (Minitel), la demande est présentée dans les 8 jours de la réception du message, ce qui soulève les mêmes incertitudes : comment la personne visée va-t-elle prouver la date à laquelle elle a « reçu » le message ?

Le texte précise que la réponse doit être « diffusée de manière à ce que lui soit assurée une audience équivalente à celle du message.[295] »

---

[292] Loi n°82-652 du 29 juillet 1982, article 6 alinéa 1er.
[293] Article 13 de la loi du 29 juillet 1881.
[294] Décret n°87-246 du 6 avril 1987, article 2.
[295] Article 6 alinéa 4 de la loi du 29 juillet 1982.

La diffusion de la réponse doit intervenir dans un délai maximum de 30 jours à compter de la date du message contesté, et dans un délai de 20 jours pour les « services de vidéographie », à compter de la date de contestation du message[296].

Toute personne morale qui assure, à quelque titre que ce soit, un service de communication audiovisuelle doit désigner un « responsable du droit de réponse ». En conséquence, tous les services Web mis en place par des personnes morales sont censés avoir un tel responsable, ce qui en pratique est assez rarement le cas.

Enfin, concernant les services de vidéographie, les « messages et documents nécessaires à l'administration de la preuve des imputations doivent être conservés pendant un délai de 8 jours à compter de la date à laquelle ils ont cessé d'être mis à disposition du public.[297] »

Il s'agit d'une obligation pénalement sanctionnée d'une peine d'amende prévue pour les contraventions de 5e classe (soit une amende de 10 000 francs).

Les auteurs de messages dans les forums de discussion devraient donc conserver une copie de tous leurs messages postés dans des listes et des newsgroups sous peine d'amende pour chaque message non conservé ! En outre la notion de « cessation de mise à disposition du public » est assez aléatoire en la matière : certains serveurs de news conservent les messages plus longtemps que d'autres, et les messages sont archivés sur des sites selon des délais variables (quelques mois, une année). Doit-on considérer que tant que le message est archivé il est mis à disposition du public ?

Ce droit de réponse conçu pour des médias comme la presse, la radio et la télévision n'est guère adapté au cas des services télématiques et Internet. Concernant les services de discussion publique, il existe heureusement un moyen fort simple d'exercer son droit de réponse : c'est de poster à son tour un message dans le forum ou la liste où ce message a été diffusé. S'il s'agit d'un groupe modéré, la demande est effectuée auprès du modérateur de la liste.

L'examen des modalités du droit de réponse montre une nouvelle fois que la logique de la loi sur la communication audiovisuelle ne correspond pas toujours à la réalité des services Internet.

L'étendue de la responsabilité des auteurs de messages et éditeurs de site au regard des caractéristiques de l'Internet

La propagation des informations

Une fois qu'une information est affichée sur un newsgroup, mise en ligne sur un site Web, elle peut se propager très rapidement dans le monde entier, de telle sorte que sa suppression du site à partir de laquelle elle a été diffusée ne sera pas toujours suffisante pour la faire disparaître, et elle va rester dans la mémoire de certains ordinateurs, dans les archives de certains sites, voire être placée sur d'autres sites.

C'est notamment ce qui est arrivé avec la diffusion par un cybercafé de Besançon du livre du docteur Gübler et de M. Gonod sur le président Mitterrand : compte tenu du caractère très médiatique de cette affaire, de l'intérêt qu'elle a suscité partout dans le monde, d'autres personnes se sont empressées de reproduire le livre et de le mettre à disposition sur d'autres sites localisés à l'étranger. Lorsque le site français a été fermé, le livre était toujours disponible sur l'Internet.

Au-delà de ses aspects particuliers, cette affaire pose la question de la responsabilité de la personne qui prend l'initiative de diffuser sur l'Internet des messages, des informations manifestement illicites ou préjudiciables à un tiers en connaissance de cause. L'Internet est

[296] Article 5 du décret du 6 avril 1987.
[297] Article 8 décret du 6 avril 1987.

choisi comme moyen de diffusion précisément parce qu'il permet de propager rapidement des informations de toute nature.

Ce type de problèmes a été soumis à un juge dans une affaire Yves Rocher c/ BNP-Banexi.

M. Yves Rocher avait établi une brochure exprimant ses griefs à l'encontre du groupe BNP-Banexi dans le cadre du litige et de la polémique qui s'est engagée entre ces personnes suite au rachat de la société Petit Bateau par la société de M. Yves Rocher.

Cette brochure a été largement diffusée auprès de la presse, mais également sur l'Internet. Estimant lesdites informations diffamatoires à leur égard, la BNP et la Banexi ont saisi le juge des référés afin de lui demander, entre autres, qu'il soit fait injonction à M. Yves Rocher de faire disparaître sous astreinte du réseau Internet toute mention des informations incriminées.

Yves Rocher a fait valoir en défense qu'aucun contrôle de l'accès et de la diffusion des informations sur le réseau ne pouvait être exercé.

Le juge lui a répondu :

« Attendu cependant que toute personne ayant pris la responsabilité de faire diffuser publiquement, par quelque mode de communication que ce soit, des propos mettant en cause la réputation d'un tiers doit être au moins en mesure, lorsque comme en l'espèce cette divulgation est constitutive d'un trouble manifestement illicite, de justifier des efforts et démarches accomplies pour faire cesser l'atteinte aux droits d'autrui ou en limiter les effets.[298] »

Si une personne prend l'initiative de diffuser des informations manifestement illicites, elle ne peut pas se retrancher derrière la nature de l'Internet pour mettre devant le fait accompli les personnes auxquelles cette divulgation porte préjudice. Le juge n'a pas demandé dans cette affaire la disparition totale des informations en cause du réseau, mais qu'il soit justifié des démarches accomplies.

Quels types de démarches peuvent être effectuées pour faire disparaître une information du réseau ?

Si l'information a été mise en place sur un site d'information, elle peut tout à fait être retirée de ce site. Généralement, une information effacée sur son site d'origine est aussi effacée automatiquement des sites qui l'avaient copié automatiquement (miroirs).

S'agissant des messages postés dans les newsgroups, il existe certaines commandes (commande de cancel permise par la plupart des logiciels de lecture des forums) qui permettent d'envoyer un message d'effacement, qui va être diffusé de serveur de news en serveurs de news. Il est techniquement possible de retrouver la trace de l'envoi de cette commande dans un groupe spécifique nommé « control ». Cependant, il n'existe aucune garantie que le message sera totalement effacé de tous les serveurs de news, et il existe en outre des sites d'archivage automatique des articles qui ne prennent pas nécessairement en compte cette commande. Enfin, il est préférable d'envoyer la commande avant que le message ne disparaisse du serveur de news, sinon la procédure d'annulation est beaucoup plus difficile.

Ainsi, si des efforts peuvent être faits pour faire disparaître certaines informations, il n'est pas possible de garantir qu'une information aura été totalement effacée, et c'est de manière bien imprudente que M. Yves Rocher avait déclaré au juge que « les informations incriminées ont été effacées du réseau Internet ».

Les liens sur un service qui contenait des informations dont le retrait a été ordonné

La société Calvacom, fournisseur d'accès Internet hébergeait sur son serveur le service Web de l'association Relais et Châteaux. L'association décide de changer de serveur

[298] TGI Paris, référé, 16 avril 1996, REF 54240/96.

d'hébergement, et le contrat est dénoncé. Cependant, Calvacom maintient sur l'URL qui servait de page d'accueil au Web de l'association (<http://www.calvacom.fr/relais/accueil.html>) une sorte de page Web Relais et Châteaux non officielle avec des liens sur les pages Web des membres de l'association avec lesquels elle reste contractuellement liée.

Par ailleurs, Relais et Châteaux reste référencée sous l'ancienne URL : (<http://www.calvacom.fr/relais/accueil.html>) dans différents moteurs de recherche Internet. L'association saisit le juge des référés et lui demande d'ordonner sous astreinte à la société Calvacom de supprimer par tous moyens le référencement — Calvacom Relais et Châteaux — du service litigieux sur le réseau Internet, ainsi que toutes références à Relais et Châteaux.

Par une décision en date du 23 mai 1996[299], le juge des référés du tribunal de grande instance de Paris a notamment fait interdiction à Calvacom de maintenir sur Internet le site fédérateur Relais et Châteaux et de conserver l'adresse URL : <http://www.calvacom.fr/relais/accueil.html>.

Cette affaire témoigne d'une certaine confusion entre la nature de l'adresse URL, la nature des liens et le référencement dans les moteurs de recherche.

Une adresse URL ne peut pas être en soit protégée par un droit de propriété intellectuelle[300]. Ce qui était plus précisément reproché à Calvacom, c'était de continuer à utiliser le nom « Relais et Châteaux », qui est une marque déposée. Si l'interdiction d'utiliser la marque d'autrui entraîne la modification de l'URL utilisée, ce sera en conséquence de cette interdiction et non parce que c'est l'URL en elle-même qui est protégée.

Lorsque l'on créé un site Web, il est d'usage de le référencer dans les grands moteurs de recherche internationaux, comme Yahoo ou Opentext, et français, comme l'UREC. Ce référencement est effectué de manière informelle, en ligne, aucun contrat ne se crée entre la personne référencée et le moteur de recherche, qui est libre de vous inclure ou non dans sa base.

C'est souvent la personne qui a développé le service qui s'occupe de réaliser ce référencement.

Lorsque l'adresse URL d'un site est modifiée, comme dans le cas de Relais et Châteaux, la même démarche doit être accomplie pour faire enregistrer la nouvelle adresse. Les modalités vont varier d'un site à l'autre et le concours de la personne ayant référencé le site peut s'avérer nécessaire. En raison du nombre de sites créés chaque jour, la demande de modification ne sera pas nécessairement prise en compte par le moteur, ou ne sera pas effective avant plusieurs semaines, voire plusieurs mois. Le site risque de continuer à être référencé sous l'ancienne adresse pendant longtemps dans certains services. C'est pourquoi il est important pour éviter de tels ennuis d'avoir son propre nom de domaine, car l'adresse de la page d'accueil du site restera toujours identique[301]. Le fait que Relais et Châteaux ait continué à être référencé sous l'ancienne adresse URL n'aurait donc pas dû, en soi, être reproché à Calvacom. Seul le concours de Calvacom pour faire des modifications auprès des moteurs de recherche pourrait être ordonné si elle refusait de s'y prêter amiablement et si sa collaboration était nécessaire.

Si un site est hébergé sous le nom de domaine d'un autre site, il peut s'avérer utile de préciser ce type de détails dans le contrat relatif au développement et à l'hébergement du site.

En revanche si Calvacom continuait à maintenir des documents relevant des droits de propriété intellectuelle de l'association, elle pourrait voir sa responsabilité engagée. Ce ne sont pas les liens effectués sur l'URL <http://www.calvacom.fr/relais/accueil.html> qui auraient

[299] REF 56551/96.
[300] Voir supra
[301] Voir supra

du être reprochés à Calvacom, mais d'avoir maintenu sur son serveur un contenu, des informations qui portent atteinte aux droits de propriété intellectuelle de son ancienne cliente.

Quant aux multiples liens qui ont pu être effectués sur un service par d'autres sites, au fur et à mesure qu'il devient plus connu, sans que l'éditeur du service n'en soit nécessairement informé, il sont hors du contrôle de l'éditeur du service.

Il existe pourtant une tendance chez les plaignants à solliciter la suppression des liens. Par exemple, au sujet de sites qui avaient reproduit sans autorisation des textes de chansons de Michel Sardou et de Jacques Brel, il était demandé au juge de « faire injonction aux défendeurs de supprimer les liens avec les sites renvoyant vers leurs serveurs et sites pour les adresses litigieuses sous telle astreinte qu'il plaira de fixer.[302] »

Cette demande n'a pas été accordée par le juge qui a considéré comme suffisant que l'accès au site comportant des œuvres contrefaites ait été supprimé.

En effet, ce qui doit être enlevé, c'est l'information elle-même si son contenu est critiquable. En revanche, on ne saurait rendre l'éditeur d'un site responsable des actes accomplis par des tiers sur lesquels il n'a pas de maîtrise.

Il faut rappeler qu'un lien s'analyse en une citation. Si un livre est estimé contrefaisant, il ne viendrait pas à l'idée des demandeurs de solliciter le retrait de toutes les citations qui auraient été faites du livre en question. Il devrait en être de même pour les liens.

Les serveurs d'hébergement

Le serveur d'hébergement met à la disposition de l'éditeur d'un service les moyens techniques en vue de permettre l'accès à l'application du service par les usagers de l'Internet.

Il fournit un espace de mémoire sur son propre serveur. Le serveur peut être une université, qui permet à ses étudiants d'avoir leur propre page personnelle, un employeur, un fournisseur d'accès grand public, une société dont l'activité est de développer et d'héberger des services.

L'étendue de la responsabilité du serveur

Le serveur n'est pas en principe responsable du contenu des services qu'il héberge. Il ne fournit pas du contenu, il n'est pas éditeur ou directeur de la publication.

En matière télématique, au sujet de services pornographiques, la responsabilité du centre serveur n'avait pas été retenue[303].

Cependant, le serveur d'hébergement pourrait voir sa responsabilité engagée en tant que complice. L'article 121-7 prévoit en effet que :

« Est complice d'un crime ou d'un délit la personne qui sciemment, par aide ou assistance, en a facilité la préparation ou la consommation. »

L'article 227-23 incrimine la simple diffusion d'images pédophiles, et l'article 227-24 le transport ou la diffusion d'images à caractère violent, pornographique ou de nature à porter atteinte à la dignité humaine susceptibles d'être vues par un mineur.

Le serveur pourrait-il être poursuivi comme complice par fourniture de moyens ou comme auteur direct des infractions en matière de diffusion d'images pornographiques ?

Les infractions doivent être examinées au regard du principe posé par l'article 121-3 du Code pénal : « il n'y a point de crime ou de délit sans intention de le commettre », sauf les cas où la loi a expressément prévu qu'un délit peut être commis par simple négligence.

---

[302] TGI Paris, référé, 14 août 1996, affaire Jacques Brel, REF 60 138/96 et affaire Michel Sardou, REF 60 139/96, Dalloz 3 octobre 1996.
[303] Crim. 15 novembre 1990 Bull. Crim. 1990, n° 388 et Crim. 17 novembre 1992, Petites Affiches 12 avril 1993, n° 44, p.4.

Le serveur ne fournit pas de contenu, il n'a pas de raison de contrôler les informations mises en ligne par les éditeurs dont il héberge les services.

Cependant, l'attention du serveur peut être attirée sur le fait qu'un des services qu'il héberge contient des informations illicites ou portant atteinte aux droits de tiers. Cette information du serveur, quelle que soit la manière dont elle est réalisée, suffit-elle à pouvoir engager sa responsabilité comme complice ?

Tout dépend de la nature de l'infraction commise. Si le service hébergé contient du matériel pédophile ou du matériel clairement pornographique en libre accès, il contient dans ce cas des information manifestement illicites, et il semble que le serveur d'hébergement pourrait voir sa responsabilité engagée s'il continuait à héberger un tel service, sans que les informations litigieuses aient été retirées.

Cette responsabilité ne devrait pas être trop étendue. Le délit ne sera pas toujours flagrant, il peut nécessiter l'avis d'un spécialiste.

Prenons l'exemple du droit d'auteur. Un serveur est informé qu'un service qu'il héberge contient des informations qui portent atteinte au droit d'auteur du plaignant. L'éditeur du service lui répond que l 'œuvre est évoquée dans le cadre de son droit de citation. Si le juge saisi décide que la reproduction de l'œuvre excédait les limites du droit de citation, le serveur va-t-il voir sa responsabilité engagée pour avoir continué à héberger le service ?

Cela ne semblerait pas raisonnable. Dans le cadre de l'affaire UEJF[304], la société Axone, un des fournisseurs d'accès mis en cause déclarait que :

« Elle estime ne pas avoir à se substituer, ni aux auteurs dans l'appréciation de cette responsabilité, ni au juge dans la qualification juridique que la diffusion des informations peut mériter ; qu'il revient donc normalement aux victimes ou au ministère public de se pourvoir en justice à l'encontre des auteurs (…) elle ne peut agir que dans les cas où de toute évidence et sans excuse possible lesdites informations tombent sous le coup de la loi, sous peine pour elle, en se substituant au juge de ne plus fournir à ses clients le service qu'ils sont en droit d'attendre.[305] »

Le serveur d'hébergement connaît normalement l'identité et les coordonnées de la personne physique ou morale dont il héberge le service, et devrait pouvoir les fournir en cas de besoin.

En revanche, le serveur d'hébergement ne devrait pas avoir à fournir d'appréciations juridiques, à se substituer au juge.

En droit français, les personnes qui estimeraient qu'un service diffuse des informations qui leur portent préjudice (diffamation, violation des droits d'auteur, contrefaçon de marque) disposent d'une procédure efficace pour faire valoir leur droits : la procédure de référé, procédure qui a déjà été utilisée à plusieurs reprise (affaires Yves Rocher / BNP en matière de diffamation[306], Calvacom /Relais et Châteaux en matière de droit d'auteur et de marque[307], affaires Jacques Brel et Michel Sardou en matière de droits sur des œuvres musicales[308]), pour demander au juge de faire cesser une atteinte manifeste à leurs droits. Si l'auteur ou l'éditeur d'un site refuse de tenir compte de leur demande, il leur appartient de saisir le tribunal. Le rapport de synthèse de la mission interministérielle sur l'Internet présidée par Mme Falque-Pierrotin[309] évoque la possibilité de mettre en place une procédure d'injonction.

[304] Voir infra
[305] TGI Paris, Référé, 12 juin 1996, REF 53061/96.
[306] TGI Paris, référé, 16 avril 1996, REF 54240/96.
[307] TGI Paris, référé, 23 mai 1996, REF 56551/96.
[308] TGI Paris, référé, 14 août 1996, affaire Jacques Brel, REF 60 138/96 et affaire Michel Sardou, REF 60 139/96., Dalloz 3 octobre 1996.
[309] 16 mars 1996-16 juin 1996, disponible à <http://www.telecom.gouv.fr/francais/activ/techno/missionint.htm>.

Dans tous les cas, hormis les infractions flagrantes (ce qui peut arriver notamment en matière de pornographie), la responsabilité des serveurs ne devrait pas être étendue de manière excessive.

En outre, les serveurs peuvent être tenus contractuellement envers leurs clients.

Si leur mise en cause dans un procédure judiciaire peut s'avérer nécessaire afin de leur rendre une éventuelle décision opposable et leur ordonner de prendre les mesures techniques en leur pouvoir pour faire cesser la diffusion d'une information, en revanche, leur rôle ne doit pas être confondu avec celui des fournisseurs de contenu.

On risquerait d'aboutir à un système où les serveurs auraient le choix entre engager leur responsabilité contractuelle envers leurs clients ou délictuelle envers des tiers.

En pratique, la responsabilité du serveur risque d'être systématiquement recherchée. C'est par exemple le cas dans l'affaire des chansons de Michel Sardou et de Jacques Brel reproduites par des étudiants de l'ENST (Ecole nationale supérieure des télécommunications) et de l'Ecole centrale de Paris sur leurs pages personnelles. Les écoles ont été mises en cause en même temps que les étudiant fautifs. Dès réception des assignations, les écoles ont mis en place des mesures conservatoires afin de rendre les sites inaccessibles et ont diffusé à l'ensemble de leurs élèves un rappel de la réglementation en matière de propriété intellectuelle. Dans le cadre du référé, le juge ne s'est pas prononcé sur la responsabilité des écoles. Si l'affaire est poursuivie au fond, cette dernière risque néanmoins d'être recherchée.

Quels sont les moyens mis à la disposition des serveurs pour se prémunir contre la multiplication de leurs mises en cause ?

Les clauses de garantie

Les contrats d'hébergement devront bien évidemment prévoir une clause de garantie de l'éditeur du service au bénéfice du serveur.

Par exemple : « Le client est seul responsable du contenu de son service WEB et garantit le serveur contre tout recours de tout tiers formé à quelque titre que ce soit. »

Une clause de ce type ne sera pas suffisante pour écarter tous les risques : elle n'est pas opposable aux non contractants, l'éditeur pourrait s'avérer insolvable.

Le serveur ne peut donc pas se retrancher derrière son seul rôle technique pour éviter de voir sa responsabilité mise en cause.

Les codes de déontologie

Les serveurs peuvent être amenés à inclure dans leurs contrats, outre le rappel de la réglementation, des recommandations dites de nature déontologique. Par exemple, France Télécom avait inséré de telles recommandations déontologiques dans les contrats qui la liait aux fournisseurs de services télématiques. Les manquements à la déontologie sont alors sanctionnés sur un fondement contractuel. La Cour de Paris a ainsi décidé, dans une affaire où France Télécom avait décidé de résilier la convention la liant à un fournisseur qui diffusait des messages pornographiques préenregistrés, que :

« Si France Télécom n'a pas à se substituer au ministère public pour poursuivre les infractions à l'ordre public et aux bonnes moeurs, elle conserve la faculté de veiller au respect des obligations souscrites par les fournisseurs de services sur les kiosques téléphoniques et, en cas de violation, de procéder à la résiliation des conventions suivant la procédure contractuellement prévue.[310] »

[310] Paris, 1re Ch. A, 13 octobre 1992, Midratel c/France Télécom, D 1993, IR. 32.

L'approche déontologique a également été choisie par certains fournisseurs d'accès grand public. Les fournisseurs d'accès Calvacom, Internet Way, Imaginet et Francenet ont ainsi demandé au juge dans le cadre de l'affaire UEJF[311] qu'il leur soit donné acte que :

« Elles ont déjà mis en œuvre des moyens d'information et de sensibilisation et que notamment elle imposent et imposeront contractuellement à leurs abonnés et annonceurs, l'obligation formelle de se conformer aux dispositions de la loi du 29 juillet 1881, à peine de rupture immédiate et à leur seul tort du contrat les liant à elles, sauf à ce qu'il soit remédié immédiatement à toute violation constatée. »

C'est également la voie suivie par Renater[312], le réseau universitaire français (Réseau national pour la technologie, l'enseignement et la recherche) ou du réseau universitaire belge[313].

Le professeur canadien Pierre Trudel explique :

« Ceux qui ont la maîtrise d'un lieu (un site) dans le réseau ont la possibilité d'adopter des politiques relativement à l'accès au site, aux comportements acceptés et aux actes prohibés. La plupart des institutions universitaires se sont dotées de politiques ou de règles délimitant les droits et prérogatives de ceux qui font usage des capacités informatiques des institutions.

Les rationalités sur lesquelles s'appuient ces politiques découlent souvent d'un souci de favoriser l'usage rationnel des ressources de l'institution, le respect des droits fondamentaux et de la dignité des personnes.[314] »

Toutes ces chartes déontologiques relèvent de ce que l'on appelle l'autoréglementation, elles n'ont pas seulement vocation à régir l'hébergement des services Web mais d'une manière générale, l'accès des utilisateurs au réseau Internet.

Elles transforment des règles légales en règles contractuelles.

Les Anglo-saxons les désignent sous le terme de « Acceptable Uses policies ». Elles viennent fixer le cadre général des obligations des utilisateurs dans l'usage des ressources mises à leur disposition.

Ces chartes participent à la sensibilisation, à la responsabilisation et à la formation des utilisateurs et éditeurs de services aux respect des règles légales applicables en France et qui sont nombreuses. En fonction de la nature et des buts poursuivis par le serveur d'hébergement, certains types d'utilisation peuvent être interdits. Par exemple, les universités excluent les utilisations à des fins commerciales.

L'autorégulation peut permettre de lutter contre les comportements les plus abusifs.

La résiliation du contrat d'hébergement de l'utilisateur devrait être effectuée selon une procédure déterminée prévue par la charte déontologique ou le contrat d'accès.

Comme avec les clauses de garanties, l'existence d'une charte ou de règles de nature déontologiques contractuelles ne feront pas obstacle à ce que les tiers cherchent à engager la responsabilité des serveurs.

Compte tenu des risques de mise en cause de la responsabilité des serveurs en raison des informations hébergées, il ne faudrait pas que cette autoréglementation dégénère en une censure déguisée et devienne arbitraire. Concernant les fournisseurs d'accès grand public, la meilleure garantie contre l'arbitraire reste sans doute la concurrence entre ces fournisseurs d'accès. Cependant, en l'absence de nom de domaine propre, il peut s'avérer peu pratique de

---

[311] Voir infra

[312] Site Web :<http://www.renater.fr>.

[313] Olivier O. Hance, Belgique, l'acceptable use policy du réseau Belnet : variations prospectives sur la notion d'autoréglementation, Droit de l'Informatique et des Télécoms 1995/3, p.52.

[314] Protection des droits et des valeurs dans la gestion des réseaux ouverts, intervention à une conférence organisée par le Centre de recherche en droit public de l'université de Montréal sur Les autoroutes électroniques : usages, droit et promesses, Montréal, 13 mai 1994, disponible à : <http://www.droit.umontreal.ca/CRDP/Conferences/AE/index_fr.html>.

changer de fournisseur d'accès, comme en témoigne l'affaire Relais et Châteaux c/ Calvacom[315].

Si la responsabilité des serveurs d'hébergement est trop largement entendue, les pages personnelles des fournisseurs d'accès grand public et des universités pourraient bien disparaître ou être menacées. Cela ne déplairait sans doute pas à certains, auxquels cette liberté de communication offerte ainsi au grand public déplaît fortement. Non seulement une telle tendance ne supprimera pas les contenus illicites qui pourront toujours être diffusés depuis l'étranger, mais elle ne pourrait qu'appauvrir l'Internet en France.

Le contenu non commercial, qui participe à la diffusion de la culture française (dont on nous répète qu'elle n'est pas assez présente sur l'Internet) et à la vie associative, culturelle et sociale, risquerait d'être entravé dans son développement.

Il doit d'ailleurs être souligné que le fait que l'Internet devienne exclusivement commercial n'est aucunement une garantie que certains services illicites ne feront pas leur apparition, bien au contraire[316]. Et le Minitel rose est là pour nous le rappeler.

Le fournisseur d'accès

La responsabilité du fournisseur d'accès est sans doute celle qui a suscité le plus de polémiques, avec la multiplication des affaires judiciaires tant en France qu'à l'étranger.

Le fournisseur d'accès peut assumer des fonctions diverses. J'ai examiné le cadre de cette responsabilité lorsqu'il agit en tant que serveur d'hébergement. Le fournisseur d'accès peut également avoir des fonctions de simple transporteur, de relais des forums de discussion sur ses serveurs de news, des sites Web sur ses serveurs relais ou caches et des messages postés par ses utilisateurs.

Le fournisseur d'accès est un point d'accès et de relais à l'Internet. Il peut également être amené à stocker de l'information sur ses serveurs pour en améliorer la communication. Cette fonction de stockage fait partie de la fonction de transport. La mise en place d'un serveur de news, qui est inhérente à la technique même de Usenet, permet à l'utilisateur d'accéder plus rapidement et sans encombrer le réseau aux forums de discussion.

Concernant les services Web, les fournisseurs d'accès ont mis en place des serveurs relais, sur lesquels ils font des copies des sites Web les plus demandés, et où ils stockent les services qui ont déjà été consultés. Lorsqu'un utilisateur demande un site particulier, s'il se trouve déjà sur le cache, le temps de transmission est notablement diminué et cela évite d'encombrer le réseau. Tout cela fait partie des techniques de communication et de transport de l'information, une fois que la procédure est mise en place, tout est automatique et sans intervention humaine.

Le fournisseur d'accès transporte également les messages émis et reçus par ses utilisateurs, qu'il s'agisse de messages de courrier électronique ou de messages diffusés dans des newsgroups.

Le fournisseur est dans toutes ces hypothèses un transporteur d'information. Il n'est pas responsable du comportement des utilisateurs et du contenu des informations auxquelles il donne accès.

Ce point est d'ailleurs rappelé dans les contrats des fournisseurs d'accès commerciaux.

Pour la société Grolier, « le service d'accès n'est pas un service d'information ou télématique mais seulement un service de connexion entre l'équipement et le centre serveur aux fins de transmission de données entre réseaux au sein d'Internet, Grolier n'exerçant aucun contrôle

[315] Voir supra
[316] Les services pornographiques font partie des services les plus rémunérateurs.

sur les contenus, nature ou caractéristiques des données qui transitent par l'intermédiaire du centre serveur.[317] »

Pour France Télécom, « France Télécom Interactive ne pourra en aucun cas être responsable du contenu des services consultés, de la nature des données interrogées, transférées et d'une manière générale de toute information consultée par l'abonné »[318].

Néanmoins, à la différence du transporteur, le fournisseur d'accès peut accéder aux informations qu'il diffuse, il a les moyens techniques de limiter la diffusion de certaines informations. C'est en raison de cette situation intermédiaire entre le fournisseur de contenu, qui décide l'information qu'il diffuse et le transporteur, qui n'a pas accès au contenu de ce qu'il transporte que la situation du fournisseur d'accès est inconfortable. Il a techniquement des moyens de contrôle qu'il lui est en réalité impossible d'exercer compte tenu de la masse d'informations disponibles, de la quantité de messages qui transitent, qui vont relever en outre de juridictions différentes. Aucun texte ne lui impose d'ailleurs un tel contrôle. Informé du caractère illicite d'un message, il peut le supprimer de son serveur, mais il ne peut pas être juge des conflits entre particuliers.

La responsabilité des fournisseurs doit être examinée en fonction de leurs différents rôles.

Le fournisseur d'accès transporteur

Il s'agit notamment du cas où le fournisseur d'accès transporte le courrier électronique. Le secret des télécommunications lui interdit même de prendre connaissance du contenu de ces communications sauf dans les cas spécifiés par la loi[319]. Il est donc tenu d'une obligation de neutralité quel que soit le message transmis par ce moyen. On relèvera que cette obligation va lui interdire en pratique d'exercer quelque contrôle que ce soit sur les messages émis et reçus des listes de diffusion, qui sont également des services de communication publics, car il n'est pas possible de distinguer un message à destination de correspondants déterminés d'un messages à destination d'un nombre indéterminé de personnes.

Le fournisseur d'accès relais des messages de ses abonnés

Différentes actions judiciaires ont mis en cause la responsabilité du fournisseur d'accès, soit en raison de son rôle de relais technique, soit en raison de messages envoyés par ses abonnés.

Il ne s'agit pas nécessairement de décisions de juridictions françaises. Ces décisions sont néanmoins particulièrement intéressantes car elle montrent que quel que soit le pays concerné, les problèmes posés par la nature de la fonction de fournisseur d'accès sont les mêmes. Il se dégage de cette jurisprudence internationale de grands principes qui peuvent tout à fait être examinés et analysés à la lumière du droit français.

Eléments de jurisprudence internationale

Pour participer aux newsgroups et autres forums de discussion publics, les utilisateurs vont envoyer leur message sur le serveur de leur fournisseur d'accès qui les relaiera ensuite aux autres serveurs de même nature. Le point de départ de la diffusion publique du message s'exerce à partir du serveur du fournisseur d'accès.

Ce cas de figure a notamment donné lieu à trois décisions des tribunaux américains, et à une décision d'un tribunal hollandais, en matière de diffamation et de droit d'auteur.

---

[317] Article 4 des conditions générales du service Club Internet .
[318] Article 9 des conditions générales du service Wanadoo.
[319] Voir supra

Cubby, Inc. v. Compuserve[320]

Parmi les services que fournit Compuserve à ses abonnés figure l'accès à divers forums[321] publics. Un de ces forums est consacré à l'industrie du journalisme. Une des publications, disponible sur ce forum, Rumorville USA contenait des propos diffamatoires sur le demandeur. La responsabilité de Compuserve pour les propos diffamatoires et mensongers a donc été recherchée. Pour sa défense, Compuserve n'a pas contesté le caractère diffamatoire des propos tenus, mais a invoqué le fait qu'elle ne pouvait pas être tenue pour responsable parce qu'elle n'avait pas connaissance et n'avait pas de raison d'avoir connaissance des propos en cause[322]. Cette argumentation a été suivie par le juge qui a relevé qu'on ne pouvait pas demander à Compuserve d'examiner chaque publication qu'il transporte pour relever les éventuels messages diffamatoires.

Statton Oakmont, Inc. v. Prodigy[323]

Il s'agit d'une affaire similaire concernant la publication d'un message diffamatoire sur un des forums de Prodigy, un autre fournisseur de services en ligne comme Compuserve. Dans cette affaire, la responsabilité de Prodigy a été retenue. Le juge américain a en effet relevé que Prodigy se présentait elle-même au public et à ses abonnés comme exerçant un contrôle sur le contenu de ses services[324] : « Prodigy held itself out to the public and its members as controlling the content of its computer bulletin boards ». En outre, Prodigy exerçait ce contrôle avec des logiciels de filtrage spécifique et au moyen de lignes de conduite données aux personnes chargées de la surveillance. C'est la propre politique de Prodigy d'exercer un contrôle éditorial sur ses forums de discussion qui a eu pour conséquence que sa responsabilité soit engagée en raison de propos diffamatoires, et ce, bien que Prodigy ait invoqué qu'elle ne pouvait pas contrôler les 60 000 messages quotidiens de ses abonnés.

Quelle est la différence entre les deux décisions ?

Les fournisseurs d'accès peuvent voir leur responsabilité engagée s'ils s'engagent dans une politique de contrôle de leurs abonnés. Cela peut sembler paradoxal, mais c'est pourtant bien à un tel résultat qu'aboutit une telle décision.

A l'occasion de l'affaire UEJF[325], certains fournisseurs d'accès français ont pris certains engagements quant au contrôle de leurs abonnés et demandé au juge des référés de leur donner acte que :

« Elles ne peuvent que s'engager à développer leurs meilleurs efforts pour, dans l'hypothèse où l'un de leurs abonnés ou l'un de leurs annonceurs contreviendrait aux dispositions de la loi du 29 juillet 1881 (qui inclut les diffamations et injures) de manière suffisamment évidente :

- soit d'obtenir qu'il cesse ses agissements ;
- soit de rompre le contrat de prestation qui les lie à cet abonné ou à cet annonceur, dans le respect des conditions générales dudit contrat, qui sont à ce jour, spécifiques à chacune des quatre société ;

et ce afin de tenter d'empêcher, autant que faire se peut, la promotion et la diffusion involontaires, à partir de leurs pages Web et forums de discussion propres, de tout message ou propos contraire à la loi du 29 juillet 1881 et notamment raciste, antisémite ou négationniste. »

---

[320] 776 F. Supp. 135 (SDNY 1991).

[321] C'est-à-dire qu'il faut être abonné de Compuserve pour y avoir accès, mais le principe est le même que les forums de discussions publiques Usenet.

[322] Compuserve "cannot be held liable for the statement because it did not know and had no reason to know of the statement".

[323] NY Sup. Ct. n° 31063/94, May 25, 1995 ; voir : Jonathan Rosenoer, Online Defamation, Cyberlaw,<http://www.cyberlaw.com>, 1995.

[324] "We make no apology for pursuing a value system that reflects the culture of the millions of American families we aspire to serve. Certainly non responsible newspaper does less when it chooses the type of advertising it publishes, the letters it prints, the degree of nudity and unsupported gossip its editors tolerate".

[325] Voir infra

Le fait d'avoir pris de tels engagements, sans les réserves mentionnées par d'autres fournisseurs d'accès également assignés dans cette affaire, pourrait justement servir d'argument à des personnes qui voudraient voir engager leur responsabilité.

Religious Technology Center v. Netcom Inc., Klemesrud[326]

Dans cette affaire, Denis Erlich, un ancien membre de la secte de l'église de scientologie, a posté sur un BBS (Bulletin Board Service) des messages reproduisant les écrits de L. Ron Hubbard, fondateur de cette secte et dont elle détient les droits d'auteur. Le BBS est lui-même relié à l'Internet via Netcom, l'un des plus gros fournisseurs d'accès américain. L'église de scientologie a donc cherché à engager la responsabilité de Netcom pour contrefaçon. Le tribunal a écarté la responsabilité directe de Netcom, sa responsabilité en tant qu'auteur de la contrefaçon.

Sinon, a souligné le juge, c'est la totalité de l'Internet qui serait responsable d'activités qui ne peuvent pas être raisonnablement empêchées. Des milliards de bits de données circulent à travers l'Internet et sont nécessairement stockés sur des serveurs à travers le réseau.

Cependant dans cette affaire, Netcom avait reçu une mise en demeure du conseil de la secte indiquant qu'Erlich avait porté atteinte à ses droits d'auteur. Netcom n'a donné aucune suite à cette notification.

Dès lors que Netcom a été informée des activités contrefaisantes de M. Erlich, la question se pose de savoir si Netcom savait ou aurait du savoir que de telles activités étaient contrefaisantes.

Si le juge a posé ce principe, il ne s'est toutefois pas prononcé sur la responsabilité de Netcom et a également relevé concernant les demandes de l'église de scientologie qu'il y avait peu de preuves que Netcom savait ou aurait dû savoir que M. Erlich reproduisait sans autorisation les écrits en cause et n'était pas fondé à invoquer l'exception de « fair use » (une sorte de droit de citation), spécialement compte tenu du fait que Netcom n'a reçu de notification qu'après que tous les messages sauf un ont été diffusés.

L'affaire avait été renvoyée à une audience ultérieure puis a fait l'objet d'une transaction entre Netcom et l'église de scientologie[327].

Spaink[328]

En Hollande, un utilisateur, K. Spaink, a posté des documents protégés par le droit d'auteur. Les titulaires de ces droits d'auteur ont assigné 22 fournisseurs d'accès hollandais. Selon le demandeur, ils avaient un rôle actif dans la distribution des documents en cause. Les fournisseurs d'accès se sont défendus en invoquant le fait qu'ils devaient être comparés à des opérateurs de télécommunication et qu'ils ne pouvaient exercer aucun contrôle sur le contenu des informations transmises.

Le tribunal hollandais a considéré qu'en principe les fournisseurs d'accès n'étaient pas responsables des actes de contrefaçon des utilisateurs. Mais le tribunal n'a pas retenu l'argument de l'analogie entre les fournisseurs d'accès et les opérateurs de télécommunication. Le tribunal a relevé qu'un fournisseur d'accès pouvait être responsable si la contrefaçon était manifeste et si le fournisseur d'accès avait connaissance de la contrefaçon.

---

[326] United State District Court for the Northen District of California, 21 novembre 1995, n° C 95-20091 MW disponible à : <http://www.cybercom.net/~rnewman/scientology/erlich/whyte-11.21.95> ou <http://www.eff.org/pub/Legal/Cases/Scientology_cases>.

[327] Star Tribune Online,<http/www.startribune.com>

[328] Scientology v. Access providers and Karin Spaink, Vonnis in kort geding van 12 maart 1196, citée par : Maurits Beerepoot, Liability of Access and Service Providers for online content, Intervention à la conférence organisée par l'Union des Avocats Européens, Les autoroutes de l'information et le multimédia : un nouveau défi, Monaco, 3 mai 1996, disponible à : <http://www.iway.fr/groupecx/uae/Beerepoot.html>.

Quelle est la tendance qui se dégage de ces décisions quant à la responsabilité du fournisseur d'accès, relais des messages de ses abonnés ?

Le seul fait qu'un utilisateur émette des messages illicites ne suffit pas à engager la responsabilité du fournisseur d'accès de cet utilisateur.

En fonction du nombre d'abonnés, des milliers de messages peuvent transiter chaque jour sur le serveur du fournisseur d'accès. En tant que relais technique, il n'a pas à exercer de contrôle éditorial sur les messages de ses abonnés.

A l'occasion de l'affaire UEJF[329], la société Axone a par exemple précisé que :

« Un contrôle systématique à son initiative des informations disponibles sur le réseau, y compris celles provenant de ses propres clients, est tout à fait exclu » .

La société Oléane a indiqué que :

« Elle ne se considère tenue et ne s'engage à aucune obligation de vérification systématique de l'ensemble des informations publiées sur le réseau ».

Cependant, à partir du moment où le fournisseur d'accès a connaissance qu'un message particulier est contraire à la réglementation, et qu'il ne fait rien pour empêcher que ledit message continue à être diffusé, sa responsabilité peut éventuellement être engagée. La notion de « connaissance » reste toutefois particulièrement floue. Dans l'affaire Netcom, le juge a indiqué que la simple notification d'une violation des droits d'auteur par le titulaire des droits ne serait pas nécessairement suffisante pour valoir « connaissance » de la contrefaçon. Le fournisseur d'accès n'est pas toujours en position de savoir s'il y a effectivement contrefaçon, et il peut être trop tard, au moment où il est informé de la teneur d'un message d'un de ses abonnés, pour arrêter une diffusion qui a déjà eu lieu.

Ainsi, si la notion de connaissance du contenu d'un message par le fournisseur d'accès peut sembler satisfaisante au premier abord, elle va être difficile à appliquer en pratique et sa portée demeure incertaine[330].

Comme dans le cas du serveur d'hébergement, le fournisseur d'accès n'a pas à porter d'appréciations juridiques. C'est pourtant à une telle conséquence que l'amène la mise en place de certaines procédures.

Après ses mésaventures judiciaires avec l'église de scientologie, Netcom a élaboré une procédure qu'elle entend suivre si on lui notifie qu'un des messages de ses abonnés a porté atteinte aux droits d'auteur d'un tiers[331].

Les conditions générales de son contrat de fourniture d'accès prévoient qu'il est interdit d'utiliser les services fournis par Netcom pour distribuer illégalement des documents, quel qu'en soit le format, couvert par des droits de propriété intellectuelle.

Le titulaire des droits d'auteur qui s'estime victime d'une atteinte à ses droits d'auteur doit contacter Netcom à l'adresse e-mail : <copyrite@netcom.com>.

Il doit fournir à Netcom suffisamment de détails sur le message posté. Il doit également fournir à Netcom :

- son numéro d'enregistrement ;
- une copie de l'œuvre protégée ;

[329] Voir infra

[330] Henry H. Perrit, Jr., Computer Crimes and Torts in the Global Information Infrastructure : Intermediaries and Jursidiction, University of Oslo, 12 octobre 1995, disponible à :<http://www.law.vill.edu/chron/articles/oslo/oslo12.htm>.

[331] Intellectual Property Rights on the Internet, <http://www.netcom.com/about/protectcopy.html>, 1st August 1996.

- une attestation que l'œuvre originale est bien sa propriété, qu'une partie importante de ce travail a été recopié et que l'utilisation de l'œuvre n'entre pas dans le cadre des exceptions au droit d'auteur.

La personne visée dans la plainte peut répondre.

Pendant que Netcom effectue une enquête, elle retire temporairement le message critiqué ou en empêche l'accès.

Si Netcom conclut que le plaignant a soulevé une demande qui apparaît légitime, elle continue d'empêcher la diffusion du matériel en question, sinon, elle rétablit l'accès.

Netcom organise donc en réalité une « mini-procédure », alors qu'*a priori*, elle n'a ni les compétences, ni les qualités pour le faire. Certes, une contrefaçon peut être manifeste, par exemple si on reproduit entièrement un livre sans avoir l'autorisation de l'éditeur. Et la procédure a le mérite d'être beaucoup plus rapide qu'une procédure judiciaire. Elle ne supprime pas néanmoins les interrogations sur l'étendue de la responsabilité du fournisseur d'accès et entraîne de nouvelles questions. Et s'il s'avère que le fournisseur d'accès supprime abusivement un message jugé ultérieurement non contrefaisant ? Il engagerait alors sa responsabilité contractuelle. Si au contraire il décide qu'un message ne l'est pas alors qu'en réalité il l'est ?

On risque cette fois de se retrouver dans le cas de l'affaire Prodigy, et la responsabilité du fournisseur d'accès risque d'être retenue pour avoir mis en place une procédure de contrôle des messages qu'il n'y a pas de raison de limiter aux infractions relatives au droit d'auteur.

Concernant Usenet, une autre interrogation se pose. Compte tenu de la rapidité de propagation des messages sur Usenet, lorsqu'un message est envoyé, il se retrouve très rapidement sur tous les serveurs de news qui diffusent le groupe dans lequel le message est affiché.

L'intervention éventuelle du fournisseur d'accès pour annuler un message ou au moins en diminuer la propagation ne peut donc se faire qu'*a posteriori*.

Si la responsabilité du fournisseur d'accès peut être engagée à partir du moment où il a connaissance du contenu illicite d'un message, il paraîtrait raisonnable de limiter cette responsabilité aux cas où son caractère illicite apparaît de façon manifeste : images manifestement pornographiques, violentes, reproduction intégrale de l'œuvre d'un artiste connu, messages clairement injurieux, racistes, etc.

Le fait que le fournisseur d'accès ait exercé ce type d'action ne devrait pas ensuite servir d'argument pour lui imputer une responsabilité éditoriale, chaque cas particulier devant être analysé au regard des principes suivant :

- le fournisseur d'accès a-t-il eu connaissance ou aurait-il dû avoir connaissance de la teneur d'un message particulier ?
- si oui, ledit message est-il manifestement en infraction avec la loi pénale ?

Le fournisseur d'accès ne pourrait être tenu pour responsable que dans l'hypothèse où il serait répondu affirmativement à ces deux questions et sa part de responsabilité appréciée en fonction de la marge de manœuvre et des possibilités techniques dont il disposait pour bloquer la diffusion, notamment s'il lui est demandé d'intervenir trop tardivement.

En revanche, le fournisseur d'accès doit pouvoir fournir les coordonnées de son client aux fins de poursuites judiciaires éventuelles et il lui appartient d'éviter des ouvertures de compte sans demander le moindre renseignement à ses clients relatif à leur identité.

S'il ne pouvait pas fournir ces renseignements aux autorités judiciaires, il semble que sa responsabilité pourrait alors être engagée et en tout cas recherchée.

La fourniture de connexion à des services extérieurs

Les affaires judiciaires

Compuserve

Au début de l'année 1996, Compuserve avait supprimé l'accès à environ 200 newsgroups de la hiérarchie <alt.sex>, sous la pression du ministère public allemand. Compuserve a ainsi non seulement coupé l'accès aux dits newsgroups pour ses abonnés allemands, mais également pour l'ensemble de ses abonnés dans le monde entier. L'accès a été rétabli par la suite par Compuserve, à l'exception de 5 groupes suspectés d'être le véhicule d'images pédophiles. A la place d'un blocage général, Compuserve propose à ses abonnés des logiciels de filtrage[332].

Deux affaires judiciaires françaises posent la question de la responsabilité du fournisseur d'accès pour avoir donné accès à des services sur lesquels il n'exercent aucun contrôle direct.

UEJF v. Calvacom, Eunet, Axone et autres[333]

L'Union des étudiants juifs de France, après avoir constaté qu'était disponible sur l'Internet des messages et des documents négationnistes, prohibés en France par la loi Gayssot[334], a assigné neuf fournisseurs d'accès en référé afin qu'il leur soit ordonné sous astreinte d'empêcher leurs clients d'accéder à des messages et documents de ce type.

Pour l'UEJF, les fournisseurs d'accès participaient à la diffusion d'écrits négationnistes et engageaient leur responsabilité tant civile que pénale.

Les fournisseurs d'accès ont répliqué que ce que demandait l'UEJF était matériellement impossible, qu'un contrôle systématique, et en temps réel, était irréalisable, qu'en ce qui concernait les informations disponibles sur les réseaux, ils vendaient un accès et non de l'information et qu'en conséquence ils avaient un rôle de transporteur et de transitaire en ce qui concerne cette fonction.

En cours d'instance, l'UEJF avait demandé la désignation de l'Institut de recherche criminelle de la gendarmerie nationale pour déterminer s'il existait des mesures techniques appropriées pour bloquer l'accès à des serveurs négationnistes.

Cette demande a été rejetée, le juge précisant que :

« Il est défendu aux juges de (se) prononcer par voie de disposition générale et réglementaire sur les causes qui leur sont soumises ; que, par ailleurs, la liberté d'expression constitue une valeur fondamentale, dont les juridictions de l'ordre judiciaire sont gardiennes, et qui n'est susceptible de trouver de limites, que dans des hypothèses particulières, selon des modalités strictement déterminées.

Attendu que la mesure d'instruction sollicitée, si elle serait certes de nature à permettre la collecte d'informations intéressantes, en particulier sur un plan technique, ne présenterait cependant pas d'utilité dans le cadre de la présente instance, dont l'issue ne saurait être marquée par l'institution d'un système global de prohibition et de censure préalable, qui au demeurant, eu égard à l'effet relatif de cette décision, ne concernerait qu'une partie des membres de la profession, et encore de manière provisoire; que s'il est bien certain, et les codéfendeurs se sont dans l'ensemble accordés à le reconnaître, que les craintes manifestées par l'Union des étudiants juifs de France sont hautement respectables, elles ne peuvent cependant conduire à des constatations générales, dépourvues de surcroît de conséquences

---

[332] Michel Alberganti, « Le débat se poursuit en Allemagne sur le contrôle de l'information en ligne », *le Monde*, 13 mars 1996, p. 22.

[333] TGI Paris, référé, 12 juin 1996, Petites Affiches, 10 juillet 1996, p.22, voir décision reproduite en annexe.
Des informations sur cette affaire sont disponibles à : <http://www.aui.fr/Groupes/GT-RPS/UEJF/uejf.html> ; voir aussi : Réflexions sur la censure, interviews de A. Braun, secrétaire national de l'UEJF et de P.Robin, dirigeant du fournisseur d'accès Imaginet, propos recueillis par Y. Eudes, *le Monde* supplément multimédia, 15 avril 1996, p.28.

[334] Article 2 bis de la loi du 29 juillet 1881.

pratiques, ou encore à des interdictions que seule la démonstration de manquements précis pourrait le cas échéant légitimer. »

La demande de l'UEJF a donc été rejetée car elle était trop générale et imprécise.

Affaire World-Net et France-Net

Le 7 mai 1996, les dirigeants de deux fournisseurs d'accès à l'Internet, Worldnet et France-net[335], ont été mis en examen pour diffusion d'images à caractère pédophile. Il est reproché à ces deux fournisseurs d'avoir relayé sur leur serveur de news des images à caractère pédophile, et de les avoir mis à disposition de leurs abonnés. Cette affaire a entraîné de nombreuses protestations des fournisseurs d'accès français, parmi lesquels certains ont coupé l'accès à leurs serveurs de news pendant quelques jours. Le réseau des universités a, suite à cette affaire, supprimé l'accès à l'intégralité de la hiérarchie <alt>[336]. L'instruction de l'affaire est toujours en cours. On ignore dans quels newsgroups les messages en question ont été trouvés.

La responsabilité du fournisseur d'accès concernant l'accès aux forums de discussion

L'ensemble des newsgroups dans le monde est évalué à plus de 17 000. Chaque jour, des centaines de milliers de messages sont envoyés sur ces forums. Le processus de propagation des messages diffusés entre les serveurs de news est donc automatisé. Cependant, rares sont les fournisseurs d'accès qui relaient l'intégralité des forums. Le fournisseur d'accès a en effet le choix de relayer ou de ne pas relayer un newsgroup particulier. Une fois qu'il accepte un newsgroup, il n'exerce pas de contrôle sur les messages postés dans le forum, il ne vérifie pas si les messages correspondent bien à la thématique du groupe.

Si on applique les principes relatifs à la responsabilité du fournisseur d'accès déjà dégagés ci-dessus, le fournisseur d'accès ne peut être tenu responsable du contenu des messages envoyés dans les forums et qu'il relaie sur son serveur de news. Cependant, le fournisseur d'accès, informé que par son canal se commettent des infractions, peut voir sa responsabilité engagée. Si le fournisseur d'accès continue à relayer un newsgroup notoirement consacré à des activités illégales, il peut voir sa responsabilité engagée.

Comment déterminer si un newsgroup est illégal ?

On peut se baser en partie sur l'intitulé. Par exemple, <alt.binaries.pictures.erotica.children> peut laisser supposer que le groupe contient des images pédophiles. En revanche, <alt.binaries.pictures.children>, continent vraisemblablement des photos d'enfants, mais pas nécessairement pédophiles.

Si une sélection peut être faite dans quelques cas particuliers sur l'intitulé du forum, ce type de sélection va vite atteindre ses limites.

Le groupe <alt.homosexual> n'est pas *a priori* pornographique, mais consacré à des discussions sur l'homosexualité. Le groupe <alt.sex> n'est pas nécessairement pornographique.

Le newsgroup <alt.binaries.warez> est connu des internautes pour diffuser des logiciels piratés[337]. Peu de gens savent que « warez » signifie logiciel piraté.

Seul un examen des messages postés dans un forum particulier permet de vérifier s'il est dédié ou non à des activités illégales.

---

[335] Sur cette affaire, voir : Edouard Launet, « Descente de gendarmes sur l'Internet », *Libération* 8 mai 1996, p.9 ; Michel Alberganti, « Internet, la justice et l'éthique », *le Monde*, 10 mai 1996, p.12 ; Yves Eudes, « Censure sur le Net Acte II », *le Monde*, supplément multimédia, 20 mai 1996, p. 28.

[336] Il s'agit des newsgroups créés sans procédure de vote des internautes, de façon moins formelle. On y trouve aussi bien des groupes à thématique sexuelle, qui sont donc très controversés et accusés de servir à véhiculer toutes sortes d'images attentatoires à la dignité humaine qu'elles soient violentes, pornographiques ou pédophiles, que des newsgroups de fans-clubs, de discussions médicales, sur la cuisine, sur des sujets scientifiques, l'informatique, la religion, etc.

[337] Adam M. Schenck, Alt.binaries.warez : the case for the Internet service provider's liability for third party usenet posts, <http://www.law.miami.edu/~froomkin/seminar/papers/schenck1.htm>, 1996.

Autre interrogation, suffit-il qu'un newsgroup contienne des messages illégaux pour que le newsgroup dans son entier soit considéré comme tel ?

Notamment, que doit-on décider en France concernant le forum <alt.revisionism> qui est consacré aux discussions sur le révisionnisme, ce qui n'est en soi pas prohibé, et contient à la fois des messages révisionnistes et des messages combattant de tels propos.

Des forums qui seraient supprimés à cause d'un nom trop évocateur pourraient réapparaître sous un autre nom. La surveillance de tout ce qui transite nécessite en réalité une surveillance constante.

En témoigne une note de la police anglaise aux fournisseurs d'accès[338]. Afin de lutter contre la pornographie, cette note suggère aux fournisseurs d'accès anglais de supprimer 133 newsgroups suspectés de contenir des messages à caractère pornographique.

Cependant précise la note, « le contenu change continuellement, et vous devrez vous rendre compte par vous-même de la nature du contenu avant de prendre des mesures. De plus cette liste n'est pas exhaustive et nous vous demandons de surveiller vos newsgroups et de prendre les mesures nécessaires contre ceux qui se trouveraient contenir du matériel pornographique. »

En réalité, il est demandé par la police anglaise aux fournisseurs d'accès d'exercer un contrôle étroit sur leurs newsgroups, contrôle qui en pratique va se révéler matériellement difficile s'il concerne un grand nombre de groupes. On ne peut pas raisonnablement demander aux fournisseurs d'accès d'exercer une surveillance constante de tous les messages de Usenet, et ce d'autant plus que si les groupes de la hiérarchie <alt.sex> et <alt.binaries> sont éliminés, les personnes qui diffusaient des messages pornographiques dans ces groupes risquent de continuer à les envoyer, mais dans d'autres newsgroups.

Aspects de droit pénal international

L'Internet pose un autre type de problème : s'agissant d'un réseau international, certains documents vont être licites dans le pays à partir duquel le message est émis, mais illicites dans un autre pays raccordé au réseau.

Par exemple, la mise en place de sites ou la diffusion de messages niant l'holocauste est prohibée en France, alors qu'au Canada et aux Etats-Unis, on considère que de telles idées sont une opinion à ce titre protégé par les dispositions constitutionnelles garantissant la liberté d'expression.[339]

Plus près de nous, les paris sur le football interdits en France, sauf pour la Française des jeux, sont autorisés dans d'autres pays à commencer par le Royaume-Uni[340].

On peut également trouver des sites hollandais sur le cannabis[341].

La loi française est-elle applicable à tous ces messages et sites ?[342]

Le droit pénal est fondé sur la notion de territorialité : ce qui se passe à l'étranger échappe à l'ordre répressif français. Cela pour deux raisons : chaque Etat est souverain, et il est en outre nécessaire que l'auteur du délit puisse être poursuivi et appréhendé dans le pays où ont lieu les poursuites. Il existe des conventions internationales d'extradition mais qui sont basées sur deux grands principes : on n'extrade pas ses propres nationaux et la double incrimination, à savoir que les faits doivent être punis dans le pays requérant l'extradition et dans le pays requis. Ces procédures d'extradition sont lourdes et sont en pratique surtout utilisées pour les crimes graves, comme le terrorisme et le meurtre.

---

[338] Dave Banisar <banisar@epic.org>, UK Bans 133 newsgroups, In GILC Mailing List <gilc@mail.privacy.org>, 19 août 1996.
[339] Yves Eudes, « Internet alerte aux Néo-nazis », *le Monde*, supplément multimédia, 12 février 1996, p. 26.
[340] Euro 96 : bookmakers en quête de mise, Cyberscope été 1996, n° 1, p.88.
[341] Yves Eudes, « Cannabis Connection », *le Monde* supplément multimédia, 8 avril 1996, p.29.
[342] « Règlements de comptes à Gigastorage », *Planète Internet* n° 8 mai 1996, p.6.

Un exemple intéressant des difficultés qui peuvent se poser en droit pénal international nous est donné par l'affaire Gigastorage. En France, un dossier d'instruction est couvert par le secret d'instruction. Christian Proust, président du Conseil général de Belfort, estimant que ce secret se retournait contre lui, et voulant montrer que le dossier du juge contre lui était vide, a fait diffuser le dossier d'instruction par une agence de presse californienne.

Il s'agit d'un cas où la loi française peut s'appliquer : il y a recel de violation du secret de l'instruction, et l'infraction de violation du secret de l'instruction a nécessairement été commise en France. Seulement, la procédure pénale française est radicalement différente de la procédure pénale américaine. Le secret de l'instruction n'existe pas aux Etats-Unis car il n'y a pas d'instruction au sens où nous l'entendons, il n'y a pas de juge d'instruction, mais un procureur et un prévenu qui vont chacun rechercher et réunir les preuves à l'appui de leur thèses (innocence ou culpabilité). Les systèmes judiciaires sont conçus de manières différentes.

Il existe des cas où l'ordre répressif français se voit doté d'une compétence dite extra-territoriale pour connaître les infractions commises hors de France.

L'article 113-5 du Code pénal prévoit que la loi française est applicable à quiconque s'est rendu complice d'un crime ou d'un délit commis à l'étranger si le crime ou le délit est puni à la fois par la loi française et par la loi étrangère et s'il a été constaté par une décision définitive de la juridiction étrangère. Ce texte pose donc une exigence de réciprocité d'incrimination.

La loi française est également applicable aux délits commis par des Français hors du territoire de la République si les faits sont punis par la législation du pays où ils ont été commis. Là encore le fait doit être puni par les deux pays[343].

La loi française est également applicable à tout crime, ainsi qu'à tout délit puni d'emprisonnement, commis par un Français ou un étranger hors du territoire, si la victime est de nationalité française au moment de l'infraction (article 113-7 du Code pénal). La poursuite du délit ne peut être exercée qu'à la requête du ministère public (article 113-8 du Code pénal) et doit être précédée d'une plainte de la victime ou d'une dénonciation officielle par l'autorité du pays où le fait a été commis.

La notion de victime laisse penser que ces dispositions s'appliquent à des crimes et délits commis sur des personnes particulières et déterminées.

On voit donc à l'examen de ces textes que la compétence des tribunaux français pour des infractions commises à l'étranger n'est pas automatique et est généralement subordonnée à un principe de double incrimination : la loi pénale française s'applique si les faits sont également punis dans le pays où ils ont été réalisés. En application de ces textes, la loi française ne devrait pas être appliquée à des informations émises depuis l'étranger et licites dans le pays d'émission.

Cependant, l'article 113-2 du Code pénal est beaucoup plus large que les précédents puisqu'il précise que :

« L'infraction est réputée commise sur le territoire de la République dès lors qu'un de ses faits constitutifs a eu lieu sur ce territoire. »

Si un des actes caractérisant l'infraction a été commis en France, la loi française s'applique.

Notamment dans tous les cas où la diffusion est un élément de l'infraction, à partir du moment où l'information est diffusée en France, la loi française s'applique, bien que l'auteur de l'infraction n'ait lui même commis aucun délit au regard de la loi qui lui est applicable.

La question de l'application de la loi française à des sites Web localisés à l'étranger pourrait d'ailleurs se poser. En effet, la manière d'accéder aux sites Web est différente de la manière d'accéder aux news. Le contenu d'un site Web peut être directement rapatrié par l'utilisateur,

[343] Cette condition de la double incrimination n'est pas exigée en cas de crime commis par un Français à l'étranger.

sans transiter par un serveur du fournisseur d'accès. Peut-on localiser dans cette hypothèse un élément de l'infraction en France ? Cela est moins évident que dans le cas où le fournisseur d'accès relaie un serveur de news, puisque le serveur de news est nécessairement localisé chez le fournisseur d'accès.

Ainsi le droit pénal, traditionnellement appliqué de manière territoriale, va souvent avoir avec l'Internet une assise extra-territoriale. En pratique, l'auteur de l'infraction sera protégé par la législation étrangère à laquelle il est soumis.

D'où encore une fois la tentation de se retourner contre les fournisseurs d'accès faute de pouvoir atteindre les auteurs des messages et les éditeurs des sites incriminés.

Eléments de réflexion sur la responsabilité des fournisseurs d'accès pour la fourniture de connexion à des services étrangers

Un auteur considère qu'à partir du moment où un fournisseur d'accès a son siège ou sa succursale en France la responsabilité du fournisseur d'accès peut être engagée en tant qu'auteur de l'infraction, que le message délictueux provienne de France ou de l'étranger. Toutefois l'auteur de l'article assimile le fournisseur d'accès au fournisseur de services télématiques[344].Or, la situation n'est pas la même : le fournisseur de services télématiques fournit du contenu, alors que le fournisseur d'accès fournit de l'accès. Si la loi française est applicable, en revanche, la responsabilité du fournisseur d'accès ne peut résulter du seul fait qu'il fournit des accès à l'Internet, sauf à considérer ce seul acte comme délictueux !

Etendre de manière exagérée la responsabilité des fournisseurs d'accès parce qu'ils permettent d'accéder à des informations illégales témoignerait d'une méconnaissance des mécanismes de fonctionnement de l'Internet et du rôle joué par les fournisseurs d'accès. Aucun texte ne les oblige à contrôler toutes les informations qui transitent leur intermédiaire. On ne peut engager leur responsabilité sous le seul constat général que se commet sur l'Internet des délits.

Un rapport de l'Office fédéral de la justice suisse[345] indique ainsi que :

« Comme relevé précédemment, la mondialisation d'Internet place la justice pénale des divers Etats devant de grandes difficultés lorsqu'il s'agit de poursuivre et de punir les auteurs d'infractions. En ce qui concerne les délits d'opinion notamment, qui revêtent une grande portée pratique, il est certes également possible de poursuivre le fournisseur pour complicité lorsque l'auteur principal de l'infraction se trouve à l'étranger. Cela ne doit toutefois pas déboucher sur une extension excessive de la responsabilité pénale du fournisseur. En l'occurrence, cette responsabilité doit au contraire se fonder sur les critères applicables de façon générale. »

Il n'apparaît pas souhaitable de faire peser sur le fournisseur d'accès une responsabilité en cascade du type de celle pratiquée en matière d'infractions de presse, où est responsable le directeur de la publication, à défaut les auteurs, à défaut l'imprimeur, à défaut les vendeurs, distributeurs et afficheurs[346].

La responsabilité du fournisseur d'accès serait en effet systématiquement recherchée chaque fois que l'auteur d'une information ne pourrait pas être identifié ou serait résidant étranger, et il verrait sa responsabilité engagée pour des actes qu'il ne peut pas contrôler.

Le rapport de synthèse de la mission interministérielle sur l'Internet présidée par Mme Falque-Pierrotin[347] souligne à cet égard que :

« Compte tenu des risques de délocalisation de l'activité en ligne en cas de présomption de responsabilité, même par défaut, du serveur d'hébergement, la mission recommande

[344] Denis Perier-Daville, Internet : du rêve au cauchemar, Gaz. Pal. 20 février 1996, p.2.
[345] Rapport d'un groupe interdépartemental sur des questions relevant du droit pénal, du droit de la protection des données et du droit d'auteur suscitées par Internet, mai 1996, disponible à : <http://www.admin.ch/ejpd/d/bj/internet/inbearbf.htm>.
[346] Article 42 de la loi du 29 juillet 1881.
[347] 16 mars 1996-16 juin 1996, disponible à <http://www.telecom.gouv.fr/francais/activ/techno/missionint.htm>.

l'adoption du système de droit commun, plus simple et mieux adapté à la démarche empirique et graduelle que nécessite l'Internet. »

On relèvera que le Defamation Law Act de 1996[348] adopté par le Royaume-Uni contient une disposition qui concerne la responsabilité des fournisseurs d'accès et leur permet de dégager leur responsabilité en cas de messages diffamatoires :

« Une personne ne sera pas considérée comme auteur, éditeur ou directeur de la publication d'une déclaration si elle est seulement impliquée dans le traitement, la réalisation de copies, la distribution ou la vente d'un média électronique dans ou sur lequel la déclaration est enregistrée, ou dans le fonctionnement de tout équipement par le moyen duquel la déclaration est récupérée, copiée ou distribuée. »

Le Communication Decency Act américain prévoit que :

« Aucune personne ne sera tenue comme coupable de la violation des sous-sections (a) ou (d) (diffusion d'images indécentes susceptibles d'être vues par des mineurs) seulement pour avoir fournit un accès ou une connexion à ou à partir d'une installation, d'un système, ou d'un réseau qui ne se trouve pas sous le contrôle de cette personne, incluant la transmission, le téléchargement, le stockage intermédiaire, les logiciels d'accès, ou d'autres capacités en relation qui sont accessoires à la fourniture d'un tel accès ou d'une telle connexion qui n'inclut pas la création du contenu de la communication.[349] »

La régulation de l'Internet

Certains pensent que le filtrage est une solution aux difficultés pratiques posées par le contrôle de l'information qui circule sur l'Internet. S'agissant d'un réseau international, d'autres estiment que toute démarche nationale est illusoire et préconisent le recours à des accords internationaux.

Le filtrage

Il existe deux types de filtrage des informations disponibles sur le réseau.

Le filtrage par l'utilisateur

Il existe des logiciels qui permettent à l'utilisateur de bloquer l'accès à certains sites[350].

L'utilisateur peut se créer sa propre liste de sites interdits. Il peut aussi utiliser la liste fournie par le fournisseur du logiciel qui répertorie un grand nombre de sites considérés immoraux.

Par exemple, le logiciel Cyberpatrol[351] propose douze catégories qu'il est possible de désactiver ou d'activer en fonction des choix effectués ; on trouve la catégorie « violence », mais aussi « nudité partielle et nudité artistique ».

Les logiciels de filtrage vont pouvoir également utiliser la norme PICS, (Platform for Internet Content Selection). Il s'agit d'un standard mis au point par le World Wide Web Consortium pour établir une classification des serveurs Web en fonction du contenu à partir de plusieurs critères : degré de violence, d'érotisme, etc.

---

[348] Disponible à : <http://www.hmsoinfo.gov.uk/hmso/document/Acts1996/1996031.htm#1> ; voir : Yaman Aknediz, Recent Developments on UK and US Defamation Law concerning the Internet, <http://www.argia.fr/lij/english/ArticleJuin96-1.html>.

[349] Section 223 (47 USC 223) amended by the telecommunication Act of 1996.

[350] Jérôme Tournier, « Internet censure à domicile », *le Monde*, supplément multimédia, 19 février 1996, p.28.

[351] Xavier Milliard, « Cyberpatrol, censure à la carte », *Planète Internet* mai 1996 n°8 p.88.

Ces logiciels de contrôle ne doivent pas être considérés comme une solution définitive et satisfaisante au problème du contrôle de l'information disponible sur l'Internet.

Les fournisseurs d'accès y voient le moyen de s'exonérer de leurs responsabilités en les rejetant sur leurs utilisateurs.

Cependant, le recours à ces logiciels soulève plusieurs questions.

Il s'agit avant tout de logiciels de contrôle parental, pour permettre aux parents de surveiller ce à quoi accèdent leurs enfants. Un adulte responsable n'a pas besoin de tels logiciels. Si certains sites lui déplaisent, il lui suffit de ne pas y accéder. Rappelons que, notamment sur le Web et Usenet, l'utilisateur choisit son information, il ne la subit pas.

Les parents risquent en pratique de reporter le choix des sites à consulter sur les entreprises qui fournissent ces logiciels, c'est-à-dire de s'en remettre au choix d'une entreprise commerciale, qui peut être située dans un pays dont les conceptions culturelles sont différentes. En outre, dans une société démocratique et pluraliste, il n'existe pas une, mais plusieurs conceptions culturelles.

Ces logiciels de filtrage sont d'ailleurs le produit d'une tradition américaine de la transmission des valeurs qui ne correspond pas nécessairement à nos traditions républicaines et laïques[352].

A l'occasion de la discussion de l'amendement Fillon, qui impose justement à tous les fournisseurs d'accès français d'inclure dans leurs services la fourniture de tels logiciels, Mme Pourtaud, sénateur socialiste soulignait que :

« Nous ne sommes pas favorables à l'utilisation de "puces antiviolence" ou de logiciels de contrôle, fut-il parental. Cela aboutit à se donner bonne conscience et à déresponsabiliser les éditeurs, les fabricants de programmes et les programmateurs de télévision. Ce n'est absolument pas la bonne méthode, d'autant que rien ne garantit l'efficacité de ces dispositifs.[353] »

« Censés responsabiliser les parents, ils risquent, au contraire, de les conduire à suivre à la lettre, dépendants et assistés, le contrôle moral d'une société extérieure.[354] »

En outre la norme PICS suppose que tous les sites fassent l'objet d'un classement en fonction de ladite norme. Or la question de savoir qui va se charger d'effectuer cette classification n'est pas résolue : les éditeurs de sites, les associations, les fournisseurs de logiciels ?

Enfin, dernière constatation pratique : les enfants, même jeunes, maîtrisent généralement mieux que leurs parents les nouvelles technologies et sauront vite trouver le moyen de contourner ce type de censure.

Si les logiciels de filtrage peuvent être utiles dans le cas de jeunes enfants, les parents et les éducateurs doivent rester responsables de la protection de leurs enfants et de leur formation quant aux informations disponibles sur les réseaux.

Le filtrage des sites

La plainte de l'UEJF et l'amendement Fillon reposaient sur la thèse qu'il existe des possibilités techniques de bloquer l'accès à certains services Internet. En réalité, le filtrage des sites est très difficile et peut toujours être contourné d'une manière ou d'une autre par un internaute déterminé à le faire.

A la suite de l'amendement Fillon, l'Association des utilisateurs d'Internet a effectué une présentation des méthodes de filtrage actuellement connues dont je reprends l'essentiel de l'exposé [355]:

---

[352] Emmanuel Parody, « la trahison des clercs », *Planète Internet* n°9 juin 1996, p.16.
[353] Compte-rendu analytique des débats du Sénat, n° 94, 6 juin 1996, p.208
[354] J. Thorel, « Contrôle parental : abus dangereux », *Planète Internet* mai 1996,n° 8, p.49
[355] Voir l'analyse de l'amendement Fillon de l'AUI, disponible à : <http://www.aui.fr/Dossiers/Amend-fillon/analyse-amend.html>.

Le filtrage peut être effectué au niveau des adresses ou au niveau des services.

« 1. Filtrage d'adresse

Un point d'Internet est référencé par une adresse IP. C'est l'équivalent du "numéro de téléphone" du serveur, numéro auquel peut être associé un ou plusieurs noms. Il est donc tentant, pour interdire l'accès à un site précis, de croire qu'il suffit d'interdire l'accès à cette adresse au niveau des équipements de télécommunication (routeurs), ou au niveau du logiciel qui associe noms et adresses (DNS).

- Filtrage d'adresse au niveau des routeurs :

Une telle solution pose de nombreux problèmes techniques, ci-dessous détaillés, mais surtout un problème de fond. En effet, une adresse correspond à un ordinateur hébergeant le plus souvent de nombreux services, dont il est peu probable qu'ils soient tous reconnus comme illégaux en France. En filtrant l'un de ces services via l'adresse de l'ordinateur qui l'héberge, on va donc aussi interdire l'accès à tous les services proposés sur cet ordinateur, dont personne ne peut prévoir l'importance ou la légalité.

Les problèmes techniques autrement soulevés par cette solution sont, pour les plus importants :

Une telle technique est très facilement contournable par "re-routage". Il existe des "relais" publics permettant de se connecter à un site ainsi interdit, et il est certain que ces relais vont être de plus en plus nombreux, dans tous les pays du monde, soit pour contourner la censure, soit simplement pour des raisons techniques. Il existe même des relais permettant de recevoir par courrier électronique (dont il est légalement difficile d'imposer le filtrage) le contenu d'une page, quelle qu'elle soit.

Une impossibilité de configurer plus d'un certain nombre d'adresses "interdites", ce nombre dépendant du matériel utilisé. Si on peut prévoir une évolution de ces matériels, il est pourtant difficile de contraindre via une loi tous les fournisseurs d'accès à changer leur matériel.

Enfin un ralentissement important de tout le réseau. Chaque routeur devant traiter des milliers d'informations par seconde, le temps de traitement sera très long si chaque paquet d'information traité doit être analysé pour vérifier le numéro du correspondant dans une longue liste.

- Filtrage d'adresse au niveau du DNS :

En pratique, le résultat sera identique au cas précédent, hormis en ce qui concerne les limitations physiques du matériel.

2. Filtrage de services au niveau du fournisseur d'accès

Si un filtrage par adresse n'est ni possible techniquement, ni souhaitable pour éviter une censure de sites légaux, il va de soi d'envisager un filtrage logiciel, au niveau du fournisseur d'accès, de certains services directement. On pourrait par exemple interdire l'accès à un site Web en filtrant sur le serveur du fournisseur d'accès les appels à un nom de page Web (URL). Cette méthode permet un filtrage plus "fin" que le filtrage d'adresses : on pourra interdire l'accès à <http://www.xxx.com/photos/> sans pour autant interdire tous les services fournis par l'ordinateur répondant au nom <www.xxx.com>.

Le meilleur exemple qui démontre l'"inapplicabilité" pratique d'un tel filtrage est sans doute celui de Deutsche-Telekom et WIN (Wissenschaftsnetz, réseau allemand pour la recherche, comparable au réseau national français pour l'enseignement et la technologie, RENATER). L'accès à un site canadien négationniste a été filtré pour toute l'Allemagne pendant 48 heures. Des militants libertaires américains ont alors dupliqué les sites bloqués par Deutsche-Telekom, notamment sur les sites de grandes universités américaines comme MIT,

Stanford ou Carnegie Mellon[356]. Non seulement le blocage s'est révélé totalement inefficace, mais il a fait au serveur une publicité très discutable.

Outre ce problème de fond, on peut aussi relever de nombreux problèmes techniques, qui rejoignent les problèmes constatés pour le filtrage d'adresse. Entre autres :

On aura le même problème de performance qu'avec les routeurs (probablement pire si la liste est longue) ainsi que de gestion.

Un tel filtrage est très facilement contournable par l'utilisateur, au prix d'une reconfiguration mineure des logiciels fournis par le fournisseur d'accès, mais par ailleurs largement diffusés sur Internet.

La seule façon de filtrer de manière fiable est sémantique. Il faudrait que le serveur puisse "reconnaître" la page exclue sur son contenu, et rien d'autre. Ni son adresse ni son nom ne sont des informations suffisantes si l'on ne veut pas censurer complètement l'accès à Internet. Un tel filtrage sémantique est impossible en l'état des connaissances et des techniques informatiques. »

Concernant les newsgroups, il faut savoir qu'il existe des serveurs situés à l'étranger qui donnent accès à tous les newsgroups, qu'ils soient ou non disponibles en France. Le serveur américain Zippo permet par exemple à toute personne de plus de 18 ans de s'abonner à son serveur pour 12 dollars par an et d'avoir ainsi accès à plus de 17 500 newsgroups, y compris les newsgroups controversés[357]. On peut imaginer que de tels serveurs se multiplieraient en cas de censure massive.

Le filtrage dans l'amendement Fillon

Malgré les problèmes techniques et pratiques soulevés par le filtrage, l'amendement Fillon déclaré inconstitutionnel par le Conseil constitutionnel voulait entériner le recours à cette technique pour mettre en place un contrôle de l'Internet en France.

L'article 43-1 de la loi de 1986, qui n'a pas été censuré par le Conseil, institue l'obligation pour « toute personne dont l'activité est d'offrir un service de connexion à un ou plusieurs services de communication audiovisuelle » de fournir un moyen technique de filtrage de certains services. Les services de communication audiovisuelle référencés sont ceux relevant du régime de la déclaration auprès du TGI, et non du régime de l'autorisation préalable par le CSA (loi du 30 septembre 1986).

Cette définition du fournisseur d'accès s'applique non seulement aux fournisseurs d'accès commerciaux, mais aussi aux universités, aux employeurs, aux individus, et d'une manière générale à toute personne fournissant, gratuitement ou non, un service de connexion. Elle s'applique de la même façon aux fournisseurs de connexion, aux services Minitel (France Télécom et ses filiales), et Audiotel qui devraient donc fournir également ces moyens techniques de filtrage.

Les logiciels de filtrage par l'utilisateur sont des logiciels américains et de contrôle parental. Le législateur n'a pourtant fait aucune distinction entre les différentes catégories de fournisseurs d'accès, ce logiciel doit être fournit aux personnes majeures sans enfants, aux salariés par leurs employeurs, aux universités, à leurs étudiants, etc.

Cette obligation n'est assortie d'aucune sanction en cas de non-respect compte tenu de l'annulation des autres dispositions de la loi.

---

[356] Yves Eudes, « Internet alerte aux néo-nazis », *le Monde* 12 février 1996, supplément multimédia p.27.

[357] <http://www.zippo.com> et <http://www.super.zippo.com> ; voir : « Comment consulter les newsgroups interdits », *le Monde* supplément multimédia 20 mai 1996, p;28 et « Un maillage complexe qui défie la censure », *le Monde* supplément multimédia, 12 février 1996, p.27.

Le reste du système qui a été censuré par le Conseil prévoyait que le CST devait émettre des recommandations déontologiques. Lorsqu'un site ne respectait pas les recommandations du CST, il se voyait notifier un avis en ce sens par le CST, publié au Journal officiel.

Dans la conception des rédacteurs de l'acte, l'amendement s'appliquait à tout service même localisé à l'étranger, à partir du moment où il était accessible en France.

Or soumettre les services étrangers à la loi française semblait être une atteinte à la souveraineté des autres Etats. On peut se poser également la question de savoir si un tel principe n'était pas contraire, au niveau de l'Union européenne, au principe de libre circulation des services.

Plaçons-nous dans la situation inverse et imaginons la réaction des Français si les Emirats Arabes Unis, pays connecté à l'Internet, notifiait au service de Elle[358], ou au service « Aux Vins de France »[359], que ces services n'étaient pas conformes à leur loi nationale ! On imagine également la réaction de l'Angleterre dans le contexte actuel, si notre CST national notifiait à un service de bookmakers hébergé au Royaume-Uni de se mettre en conformité avec la loi française et de respecter le monopole de la Française des jeux ! Ces exemples sont provocateurs, c'est pourtant bien à un tel résultat que l'application du texte envisagé aurait pu aboutir.

Les notifications envisagées auraient sans doute fait une contre-publicité certaine au CST et une publicité non moins certaine aux sites ainsi montrés du doigt.

Il est à parier que le résultat aurait été comme dans le cas de l'affaire Deutsche-Telekom de multiplier les sites miroirs et donc de rendre en pratique impossible le respect d'un blocage de l'accès à ces sites.

Le fournisseur d'accès était, selon le dispositif envisagé, exonéré de responsabilité pénale à deux conditions :

- qu'il fournisse un logiciel de filtrage ;
- qu'il bloque l'accès à un service ayant fait l'objet d'un avis défavorable publié au Journal officiel.

A contrario, le fournisseur d'accès était pénalement responsable s'il ne bloquait pas l'accès au dit service, ce qui semblait créer une obligation de résultat dans le filtrage à la charge des fournisseurs d'accès.

Par ailleurs le droit commun continuait de leur être applicable puisque le texte précisait qu'ils pouvaient être tenus pénalement responsables du contenu des messages « s'il est établi qu'(ils) ont, en connaissance de cause, personnellement commis l'infraction ou participé à sa commission ».

La régulation internationale

Certains soulignent que dans un contexte international comme celui de l'Internet, toute démarche nationale est illusoire et que la solution aux problèmes de contrôle posés par l'Internet doit s'effectuer à un niveau international. Lors d'un conseil informel des ministres européens chargés des télécommunications, François Fillon, ministre des Télécommunications a ainsi indiqué que la France juge souhaitable une initiative internationale concertée dans ce domaine[360].

François Fillon souhaite qu'une convention internationale soit élaborée et traite des sujets suivants :

[358] Site Web : <http://www.elle.fr>.
[359] Site Web : <http://www.mworld.fr/avf/>.
[360] Communiqué du ministère des Télécommunications du 24 avril 1996.

- principes minimaux de déontologie applicables aux services sur l'Internet ;
- détermination de la loi applicable ;
- principes de responsabilité commun des éditeurs et des services d'hébergement ;
- principes de base d'une coopération judiciaire.

Il est illusoire d'imaginer l'élaboration d'une éthique mondiale. Déjà les conceptions en matière de mœurs peuvent être fort différentes d'un pays européen à l'autre, notamment entre pays du sud et du nord de l'Europe, sans parler des divergences parfois sur des points fondamentaux qui opposent les Etats-Unis et l'Europe, et les pays occidentaux aux pays musulmans et aux pays asiatiques.

Une loi internationale qui régirait le contenu des services Internet est une vue de l'esprit.

Elle impliquerait une harmonisation des législations de tous les pays impliqués, ce qui est à l'évidence impossible. Et quelle éthique serait appliquée ? Beaucoup d'Etats considéreront l'imposition d'une éthique qui ne correspond pas à leurs valeurs culturelles comme inacceptable.

Une telle harmonisation n'est d'ailleurs même pas souhaitable. La diversité des cultures est une richesse qui doit être préservée.

En revanche, il appartient à chaque pays d'appliquer ses lois nationales aux personnes et services localisés sur son territoire, de réprimer les comportements les plus abusifs de ses propres justiciables[361].

Prenons deux exemples :

La pédophilie est réprouvée assez universellement, en tout cas dans une majorité de pays. Si chaque pays commence par poursuivre les personnes localisées sur son territoire se servant de l'Internet pour diffuser des images pédophiles, cela devrait déjà contribuer à diminuer notablement certains abus.

Plusieurs poursuites ont d'ailleurs déjà eu lieu : en France, un homme qui diffusait de tels messages a été interpellé[362], aux Etats-Unis, le FBI a arrêté plusieurs personnes en septembre 1995 à la suite d'une enquête de plus de 2 ans sur un réseau de pédophilie, en Angleterre, plusieurs procédures à l'encontre de pédophiles ont abouti à des condamnations et notamment une condamnation à 3 ans d'emprisonnement d'une personne qui avait diffusé du matériel pédophile sur l'Internet[363].

La coopération entre les polices concernées peut être renforcée et, si le service d'un pays particulier constate que l'émetteur d'une information pédophile émet depuis l'étranger, il peut dénoncer l'infraction à la police du pays concerné. Chaque pays peut désigner un service chargé de ce type d'affaires auquel les faits seraient dénoncés, à charge pour eux d'établir les procédures adéquates dans leur propre pays.

En matière de pornographie, de nombreux pays réglementent la diffusion de matériel pornographique dans un but de protection des mineurs. C'est déjà le cas dans de nombreux pays occidentaux. Dans certains pays asiatiques, des images que nous considérerions comme normales sont censurées, et les pays musulmans n'ont pas la réputation d'être larges d'esprit dans ce domaine.

La plupart des pays occidentaux ont une législation en la matière, sans doute dans une majorité de cas parfaitement applicable aux services en ligne. Aux Etats-Unis, un couple

[361] Sur l'identification des éditeurs de sites et les auteurs de messages, voir infra
[362] Dépêche AFP du 16 juillet 1996.
[363] Yaman Akdeniz, Pornography on the Internet, <http/www.argfia.fr/lij/ english/ArticleJuin11.html>, 1996.

californien qui commercialisait par l'intermédiaire d'un BBS du matériel pornographique a été poursuivi et condamné pour diffusion de matériel obscène[364].

En France, l'article 227-24 du Code pénal est applicable sans hésitation. Reste la volonté de faire respecter les dispositions de cet article.

L'Internet n'est que le reflet de notre société actuelle, il n'est ni pire ni meilleur.

Les différences culturelles entre les différents pays connectés à l'Internet persisteront. Si un site est légal dans le pays où il est localisé, il ne devrait pas être censuré.

La Chine et Singapour cherchent, tout en bénéficiant de l'accès à l'Internet, à instaurer un contrôle étroit des informations auxquelles leurs citoyens ont accès. En Chine, tout utilisateur de l'Internet doit par exemple se faire enregistrer auprès des services de police, une procédure peu envisageable dans les pays démocratiques.

On ne pourra sans doute pas empêcher les citoyens français d'avoir accès à des informations émanant de pays ayant des valeurs culturelles, religieuses, sociales différentes des nôtres. Au lieu de s'en effrayer, n'oublions pas que d'autres citoyens d'autres pays souhaiteront bénéficier de la réciproque. Le rapport de synthèse de la mission interministérielle sur l'Internet présidée par Mme Falque-Pierrotin[365] ne dit pas autre chose : « La meilleure manière de se défendre contre l'Internet, si danger il y a, est d'y être ! (…) La tradition française est celle des valeurs humanistes, respectueuses des droits et des libertés de chacun ; il importe dès lors de favoriser la reprise de celles-ci par l'Internet afin que celui-ci soit un outil de progrès et d'enrichissement plutôt qu'un synonyme de danger. »

[364] Mark Walsh, Milpitas Couple's Internet Conviction Upheld, The Recorder, 30 janvier 1996, <http://www.callaw.com/edt130b.html> ; la décision est disponible à :<http://www.callaw.com/tommy.html>.

[365] 16 mars 1996 - 16 juin 1996, disponible à <http://www.telecom.gouv.fr/francais/activ/techno/missionint.htm>.

La protection des données

Première partie

Les droits d'auteur

La protection des droits d'auteur sur l'Internet pose plusieurs difficultés. Les nouvelles technologies de l'information permettent de numériser, puis de reproduire et de diffuser des œuvres avec une grande facilité. Une œuvre numérisée peut être reproduite de nombreuses fois, sans que la qualité des copies ne soit altérée par rapport à l'original. Elle peut également être manipulée, modifiée, altérée, intégrée dans d'autres œuvres avec une grande facilité. Les auteurs et les producteurs d'œuvres culturelles craignent de ne plus recevoir la juste rémunération de leur travail.

La protection des droits d'auteur est une assurance que ne seront pas faites plus de copies que nécessaire des œuvres une fois divulguées. Les titulaires des droits d'auteur ont besoin d'un certain degré de protection contre les copies afin de pouvoir tirer un profit de la commercialisation des œuvres.

La copie privée est notamment ressentie comme un risque de pillage généralisé des œuvres, et certains voudraient même l'interdire. Pour la Chambre de commerce internationale, « la copie privée dans un environnement numérique représente une réelle menace pour les titulaires de droits et devrait être totalement soumise à un droit de reproduction sévère.[366] »

Il faudrait pouvoir instituer un système de rémunération comme cela existe pour certaines œuvres.

Dans le domaine de l'enseignement, le développement des photocopies avait ainsi pris une telle ampleur (on parle de « photocopillage ») qu'il a amené le législateur à intervenir et à mettre en place un régime de gestion collective des redevances dues pour la reproduction par reprographie des œuvres donnant lieu à droit d'auteur[367]. La publication d'un livre entraîne cession du droit de reproduction au profit du Centre français d'exploitation du droit de copie[368] qui perçoit les droits des entreprises de photocopie, des établissement scolaires et universitaires ou d'enseignement supérieur, qu'il reverse ensuite aux éditeurs à charge pour ces derniers de les reverser aux auteurs.

De même, en matière audiovisuelle, la loi du 3 juillet 1985 a institué un droit à rémunération pour copie privée reposant sur une redevance sur les cassettes vidéo vierges et instituant un système de gestion collective[369].

L'autre domaine d'action concerne la technique.

[366] Commentaires de la CCI à propos du Livre vert de la CE sur le droit d'auteur et les droits connexes dans la société de l'information, Droit de l'Informatique et des Télécoms 1995/4, p. 58.
[367] Loi n° 95-4 du 3 janvier 1995, JO du 4 janvier, p.120.
[368] CFC, 3, rue Hautefeuille, 75006 Paris.
[369] Jean Cottin, Redevance et rémunération pour la copie privée audiovisuelle, Gaz. Pal. 12 octobre 1995 p. 18.

Le tatouage électronique des œuvres

On envisage actuellement la mise en place de procédés qui permettront l'immatriculation des œuvres, leur « tatouage électronique ». Il s'agit à la fois de permettre l'identification des œuvres, ce qui permet de connaître le titulaire des droits d'auteur, et de repérer les utilisateurs. Ce tatouage permettrait de mettre en place la gestion collective des œuvres numériques. Il n'est pas certain que cela soit techniquement réaliste, sauf à réduire considérablement la liberté des auteurs de logiciels.

La CISAC[370], Confédération internationale des sociétés d'auteur et compositeurs a débuté en février 1995 un programme de ce type.

Il s'agit de normaliser toutes les œuvres afin de s'entendre sur un système de codification international type ISBN pour les livres ou ISSN pour les revues, qui soit en outre compatible avec tous les systèmes, logiciels et matériels informatiques.

Le tatouage électronique devrait être également infalsifiable.

Cependant, à partir du moment où une œuvre est numérique, il est difficile d'en empêcher les reproductions.

C'est le cas notamment des logiciels. La copie privée des logiciels est en principe interdite, seule étant autorisée la copie de sauvegarde et les reproductions nécessaires à l'utilisation normale du logiciel. En pratique, comme un logiciel se présente sous forme numérique, il est très difficile d'éviter que de telles copies soient effectuées et l'industrie du logiciel est impuissante face aux nombreuses copies pirates qui circulent.

Pour la CCI (Chambre de commerce internationale), « les moyens de faire respecter les droits de propriété intellectuelle sont une question clé à laquelle les gouvernements doivent s'intéresser.

Il est essentiel que les gouvernements éduquent le public, afin que ce dernier, lorsqu'il utilisera la nouvelle infrastructure de l'information, respecte dès le début les droits de propriété intellectuelle. Des moyens efficaces de faire appliquer ces derniers doivent être disponibles et la volonté de les mettre en œuvre doit être démontrée, afin qu'il soit clair que toute atteinte aux droits de propriété intellectuelle sera sanctionnée.

Les détenteurs de droits recourront largement à la technologie pour se protéger contre les atteintes à la propriété intellectuelle.[371] »

Il faudrait donc également mettre en place des dispositifs techniques empêchant les reproductions.

La solution des tatouages numériques et des systèmes bloquant la reproduction n'est pas sans poser un certain nombre de problèmes d'ordre technique et juridique.

Les techniques informatiques sont en constante évolution : de nouveaux langages sont créés, de nouveaux protocoles expérimentés…

Par ailleurs, la consultation des données sur l'Internet nécessite de nombreux actes de reproduction :

- propagation des messages sur Usenet ;
- consultation des serveurs Web le document peut être stocké dans la mémoire de l'ordinateur par le navigateur lors des opérations de chargement et d'affichage, il peut être

[370] site Web : <http://www.cisac.com>.

[371] CCI, Développement des technologies de l'information : déclaration de politique générale, Droit de l'Informatique et des Télécoms 1995/1, p.62.

temporairement stocké dans le disque dur de l'ordinateur par le logiciel de navigation, il peut être automatiquement stocké sur un cache[372].

La création de copies est inhérente à la technologie de l'Internet, et nécessaire pour que le système fonctionne de manière appropriée[373].

Il ne faudrait pas que la mise en place de systèmes de tatouage numérique et de blocage ne devienne un frein à l'évolution technologique et à l'innovation.

Le tatouage généralisé des œuvres et l'institution d'un système de gestion collective de rémunération des copies privée va se heurter à de nombreux obstacles et n'est pas encore opérationnel.

Du point de vue juridique, le contrôle des œuvres implique également le contrôle des utilisateurs. Il y a donc des enjeux en terme de protection de la vie privée et des libertés sur lesquels il serait bienvenu d'entamer des réflexions : les gens souhaitent-ils vraiment que l'on sache tout ce qu'ils lisent, tout ce qu'ils écoutent, tout ce qu'ils regardent ?

Le contrôle des œuvres mises en ligne

Comment aujourd'hui, en l'état des moyens disponibles, contrôler ce qui est mis sur le réseau ?

Le choix des œuvres qui sont diffusées

Lorsque l'on ne veut pas qu'une œuvre puisse être recopiée, on évite tout simplement de la mettre sur le réseau en libre accès. C'est le seul moyen de protection qui garantisse contre les reproductions non autorisées, les copies privées, les pillages en tout genre. Il ne s'agit pas d'arrêter de faire des sites Web, il s'agit d'être conscient qu'à l'heure actuelle l'Internet reste avant tout un moyen de communication des idées et de promotion.

L'état de la technique

Concernant les journaux et les livres, le papier a sans doute encore de beaux jours devant lui. Feuilleter un magazine, lire un livre confortablement installé ou l'emporter à la plage restent des méthodes de lecture plus conviviales pour la plupart des gens que la consultation d'écrans d'ordinateurs. Le jour où tout citoyen possédera son ordinateur de poche n'est pas encore arrivé.

La qualité des enregistrements de son sur l'Internet est loin d'égaler la qualité d'écoute d'un CD.

La longueur des temps de téléchargement, la faiblesse des débits, sont autant d'obstacles actuels à la consultation des données qui occupent beaucoup de mémoire.

Compter sur l'état de la technique n'est qu'une solution temporaire, compte tenu des progrès réalisés sans cesse. Il s'agit toutefois d'un élément qui peut être pris en compte.

Le contrôle de l'accès

Il s'agit de réserver l'accès d'un site aux personnes autorisées, par exemple aux personnes qui se sont abonnées préalablement. L'accès à l'œuvre n'est autorisé que moyennant paiement préalable.

---

[372] Un cache est un serveur qui stocke temporairement des documents. Au lieu de faire une requête sur le serveur qui contient les documents consultés, la requête est faite au cache. Les fournisseurs d'accès mettent en place des serveurs cache afin de diminuer les temps de consultation et l'usage de la bande passante. Il s'agit donc d'un procédé utilisé pour améliorer les transmissions de données.

[373] Norderhaug, T & Oberding, J.(1995), Copyright Infrigment on the Web, Designing a Web of Intellectual Property, Computer Networks and ISDN Systems, 27(6), p. 1037, disponible à : <http://www.ifi.uio.no/~terjen/pub/webip/950220.html>.

Plusieurs sociétés commercialisent leurs logiciels sur l'Internet en laissant l'acheteur potentiel le tester. Si l'utilisateur veut acheter le logiciel après l'avoir testé, un code lui est envoyé pour lui donner accès à la version intégrale du logiciel.

Les avertissements

Sur la page d'accueil du serveur il peut être utile d'insérer une mise en garde sur la protection du site et de ses éléments par le droit d'auteur. Des précisions pourront être données aux utilisateurs : modalités des liens hypertextes, autorisations préalables pour les références inline d'images, courrier électronique de l'administrateur du site, modalité de citation des articles mis en ligne, mises en garde diverses.

La mise en place de tels avertissement ne garantit pas que les droits d'auteur seront respectés, mais elle permet d'informer les usagers qui n'ont pas toujours conscience que le fait qu'une donnée soit en libre accès ne signifie pas que l'on est autorisé à en faire tout ce que l'on veut. Ces avertissements peuvent donc avoir une fonction pédagogique importante. Même si le service est en français, une traduction de ces avertissements en plusieurs langues peut être utile, notamment si le site comporte des données graphiques ou musicales.

L'Internet comme outil de promotion

Une œuvre numérisée ne remplace pas nécessairement l'œuvre réelle. La photographie d'un tableau, d'une sculpture ne remplace pas la possession de l'œuvre. L'Internet peut servir dans cette perspective à présenter les œuvres.

Concernant les photographies, on peut jouer sur la résolution et la définition des œuvres diffusées. Par exemple, une image en basse définition sera moins facile à exploiter. On peut par exemple présenter des catalogues en ligne sans craindre le pillage direct, car si l'utilisateur veut une photo de qualité, il sera obligé de la commander.

La valeur ajoutée apportée par le site

Les services offerts en ligne peuvent être conçus comme des compléments des services offerts hors réseau au lieu d'être considérés comme concurrents.

Par exemple, certains journaux mettent en place sur leur site une base de données de leurs articles sur laquelle on peut effectuer une recherche en ligne par mot clé.

Des fabricants de logiciels permettent à leurs clients de télécharger directement les mises à jour des versions achetées sur l'Internet

Plutôt que de vouloir à tout prix adapter la technologie pour qu'elle puisse se calquer sur les modèles actuels, il faudrait sans doute réfléchir à une nouvelle économie qui prenne en compte les spécificités des réseaux informatiques.

L'objectif des droits d'auteur est d'assurer une juste rémunération du créateur, tout en préservant le droit du public d'accéder aux œuvres et la diffusion des idées.

L'Internet est aujourd'hui un outil de communication, de promotion et de diffusion de l'information. Les producteurs attendent des autoroutes de l'information qu'elles leur permettent de commercialiser leurs œuvres, qu'elles véhiculent une sorte de télévision interactive, avec jeux et vidéos à la demande. Peut-être que ces deux manières d'utiliser les techniques d'information ne sont pas compatibles et que les réseaux serviront à tout autre chose que ce qui avait été prévu au départ.

Au lieu de considérer l'Internet uniquement comme une menace, les auteurs pourraient comprendre qu'ils possèdent là un moyen de communication direct et nouveau avec leur public.

Il s'agit d'imaginer les nouvelles utilisations qui pourraient être faites des moyens de communication offerts par l'Internet et d'inventer les nouveaux services du futur, plutôt que de vouloir à tout prix rester sur ses acquis et tenter d'empêcher des évolutions inéluctables.

Deuxième partie

Les systèmes et données informatiques

L'informatique ne sert pas qu'à transférer et traiter des données, elle peut être le vecteur de fraudes en tous genres. C'est ce que l'on appelle la fraude ou criminalité informatique.

Sont concernés, en premier lieu, les accès non autorisés dans les ordinateurs des autres, que ce soit par malveillance, par défi, ou par jeu.

La fraude informatique vise, en second lieu, les altérations, dégradations, manipulations de données en tous genres : modifications des données, introductions de virus (programmes informatiques capables de se reproduire qui peuvent être conçus pour effacer ou altérer les données des systèmes dans lesquels ils ont été introduits), sabotages, destructions de documents.

Elle recouvre, enfin, les interceptions non autorisées.

La fraude informatique peut être le fait de personnes extérieures, de tiers, mais également de personnes internes à une organisation, un groupement, comme les salariés.

Les statistiques sur la criminalité informatique montrent que ce phénomène est en constante augmentation. Le total des fraudes informatiques est estimé en France à 1,4 milliards de dollars.

L'Internet n'est évidemment pas épargné par la délinquance informatique.

Sur un réseau comme l'Internet, ouvert, reliant des millions d'ordinateurs, la tentation est très forte pour ceux que l'on surnomme les « pirates » ou « crackers » de pénétrer illégalement dans les systèmes des autres, d'intercepter les communications qui ne leur sont pas destinées. S'il faut croire le journaliste Jean Guisnel, les services de renseignements ne sont d'ailleurs par en reste et l'Internet serait largement utilisé pour l'espionnage économique[374].

D'un point de vue juridique, il existe en France depuis une loi du 5 janvier 1988 dite loi « Godfrain », un arsenal de textes qui ont évidemment vocation à s'appliquer, le fait que l'ordinateur pénétré soit relié à l'Internet, que la communication interceptée ou les données modifiées aient transité par un service de communication Internet ne modifiant pas la nature de l'infraction.

Les dispositions prévues ont pour objet soit de protéger la confidentialité, soit de protéger les données elles-mêmes.

[374] Jean Guisnel, Guerres dans le cyberespace, services secrets et Internet, éditions la Découverte, 1995.

La protection de la confidentialité

Les intrusions

L'intrusion dans un système informatique est prévue par l'article 323-1 alinéa 1 du Code pénal qui précise 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 100 000 francs d'amende. »

Un système de traitement automatisé de données est un système informatique.

L'intrusion, c'est le simple fait d'accéder de manière non autorisée, de pénétrer dans le système, mais également le maintien dans le système suite à cet accès. Une personne qui se serait immiscée par erreur dans un système mais s'y serait maintenue de manière consciente rentre ainsi dans le cadre de l'incrimination.

Les interceptions[375]

L'article 226-15 du Code pénal réprime l'atteinte au secret des communications ainsi que l'installation d'appareils conçus pour réaliser de telles interceptions.

Les atteintes au secret des correspondances réalisées par une personne dépositaire de l'autorité publique dans l'exercice de ses fonctions, de même que de telles atteintes commises par les exploitants de réseaux de télécommunications, les fournisseurs de services de télécommunications sont réprimées par l'article 432-9 du Code pénal.

La protection des données

L'intrusion ayant occasionné des altérations

Lorsqu'une intrusion ou un maintien illicite dans un système a occasionné la suppression, la modification des données contenues dans le système ou une altération du fonctionnement du contenu de ce système, les peines prévues en cas d'intrusion sont aggravées : elles sont portées à 2 ans d'emprisonnement et 200 000 francs d'amende (article 323-1 alinéa 2 du Code pénal).

L'atteinte au système

L'article 323-3 du Code pénal dispose que :

« Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de 3 ans d'emprisonnement et de 300 000 francs d'amende. » Les termes généraux utilisés par la loi permettent de sanctionner les altérations diverses telles que la mise en place de bombes logiques ou l'introduction de virus.

L'atteinte aux données

L'article 323-3 du Code pénal prévoit que :

« Le fait d'introduire frauduleusement des données dans un système de traitement automatisé de données ou de supprimer ou de modifier frauduleusement les données qu'il contient est puni de 3 ans d'emprisonnement et de 300 000 francs d'amende. »

[375] Voir supra

Le texte sanctionne les altérations volontaires de données, ainsi que les manipulations d'informations, les données fausses introduites sciemment dans un fichier, la modification ou la suppression malveillantes de données sans qu'il ne soit porté atteinte au système informatique lui-même.

La falsification de documents numériques

L'incrimination de faux et usage de faux ne s'applique plus seulement aux altérations de documents écrits, mais aussi aux altérations accomplies « par quelque moyen que ce soit, dans tout autre support d'expression de la pensée » qui ont pour objet ou qui peuvent avoir pour effet d'établir la preuve d'un droit ou d'un fait ayant des conséquences juridiques (article 441-1 du Code pénal).[376]

Le faux et l'usage de faux sont punis de 3 ans d'emprisonnement et de 300 000 francs d'amende.

La répression internationale de la fraude informatique

La répression de la fraude informatique réalisée par le biais de l'Internet pose, en raison du caractère transfrontière de ce réseau, divers problèmes.

Les infractions seront souvent internationales. Par exemple, le site Internet de l'Ecole polytechnique a fait l'objet d'intrusions par un pirate localisé en Israël[377] : l'infraction est réalisée sur des ordinateurs situés sur le territoire français, par un délinquant situé à l'étranger.

Or, il convient que le mode de présentation de la preuve électronique soit le même entre le pays où elle aura été recueillie et le pays où l'infraction sera jugée. Cette compatibilité exige des choix technologiques similaires et des accords internationaux.

Ensuite, pour que les poursuites puissent s'exercer, il ne suffit pas que les pays concernés prévoient et punissent les mêmes faits, il est également nécessaire de mettre en place des instruments d'entraide adaptés à la criminalité informatique, qui présente la particularité de nécessiter des informations et des réactions rapides[378].

Pour prendre en compte les aspects spécifiques de la criminalité informatique, le Comité des ministres du Conseil de l'Europe a adopté le 11 septembre 1995 une recommandation relative aux problèmes de procédure pénale liés à la technologie de l'information[379].

La recommandation vise à adapter, compléter et organiser les systèmes juridiques existants. Il s'agit de mettre à jour et de compléter les pouvoirs d'investigation pour tenir compte des exigences spécifiques des enquêtes en matière de délinquance informatique, et de développer la coopération technique et juridique. Il est donc recommandé aux Etats membres de s'inspirer, lorsqu'ils révisent leurs législations et pratiques internes, des principes posés par la recommandation.

Les différentes dimensions de la fraude informatique sont donc appréhendées par le droit.

Cependant en la matière, il est préférable d'agir à titre préventif pour assurer, dans la mesure du possible, la sécurité des systèmes informatiques. Les mesures à prendre sont connues des techniciens même si elles ne sont pas toujours appliquées : coupe-feus, codes d'accès en tous

[376] Voir infra
[377] Erich Inciyan et Annie Kahn, « Le site Internet de Polytechnique a été fermé à la suite d'intrusions », *le Monde* 4 juin 1996, p.13.
[378] Pierre Novaro, La procédure pénale en matière informatique, Lamy droit de l'informatique, Bulletins d'actualité décembre 1995, (H).
[379] Recommandation n° R (95) 13, disponible à :<http://www2.echo.lu/legal/en/crime/crime.html>.

genre, formation et sensibilisation du personnel aux problèmes de sécurité, mise en place de procédures.

La responsabilité du serveur

Le responsable d'un serveur sur l'Internet doit prendre des mesures pour préserver la sécurité de son système, car le fait que ses ordinateurs reliés au réseau fassent l'objet d'une intrusion peut lui causer un préjudice grave.

En outre, il ne risque pas seulement d'être une victime du piratage informatique, il pourrait voir sa responsabilité engagée pour ne pas avoir suffisamment veillé à la protection des données qu'il traite.

Par exemple, l'article 226-17 du Code pénal précise que :

« 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 empêcher qu'elles ne soient déformées, endommagées ou communiquées à des tiers non autorisés est puni de 5 ans d'emprisonnement et de 2 millions de francs d'amende. »

La divulgation à un tiers non autorisé, même par négligence ou par imprudence, d'informations nominatives susceptibles de porter atteinte à la considération ou à l'intimité de la vie privée d'une personne est également un délit pénal prévu et réprimé par l'article 226-22 du Code pénal :

« Le fait, par toute personne qui a recueilli, à l'occasion de leur enregistrement, de leur classement, de leur transmission ou d'une autre forme de traitement, des informations nominatives dont la divulgation aurait pour effet de porter atteinte à la considération de l'intéressé ou à l'intimité de sa vie privée, de porter, sans autorisation de l'intéressé, ces informations à la connaissance d'un tiers qui n'a pas qualité pour les recevoir est puni d'un an d'emprisonnement et de 100 000 francs d'amende.

La divulgation prévue à l'alinéa précédent est punie de 50 000 francs d'amende lorsqu'elle a été commise par imprudence ou par négligence. »

La gérante d'un serveur télématique a ainsi été condamnée pour avoir laissé divulguer le numéro de téléphone d'une personne sur un service télématique pornographique. Pour sa défense, la responsable du serveur invoquait la force majeure trouvant son origine dans des micro-coupures d'électricité, susceptible de fausser les verrous informatiques qui filtrent normalement les chiffres correspondant à des numéros de téléphone ou à des adresses. Le juge pénal a écarté cet argument au motif que ces micro-coupures n'étaient ni imprévisibles, ni irrésistibles[380].

Les éditeurs de services, s'ils font héberger leur site par une entreprise tierce, devraient veiller à faire insérer dans le contrat d'hébergement des clauses relatives aux précautions prises et moyens mis en œuvre par le serveur pour assurer la sécurité du site et assurer la confidentialité des données nominatives éventuellement recueillies et traitées. Ces moyens techniques pourraient par exemple être récapitulés dans un cahier des charges. L'importance des précautions prises peut varier en fonction de la personne de l'éditeur et de l'objet du service.

Il est certain que les sites gouvernementaux ou de grandes sociétés risquent d'être davantage la cible de pirates qui chercheraient à modifier le contenu du site pour ridiculiser l'organisme ou la société visée, que des sites moins populaires.

[380] TGI de Briey, 15 septembre 1992, Aff. Costel c/Castellvi et Sériot, Droit de l'Informatique et des Télécoms 1994/3 p.34.

Ainsi, le site officiel du ministère de la Justice américain a été piraté par des personnes qui ont remplacé le contenu habituel du site par des slogans et images obscènes et des liens vers des sites critiquant ou ridiculisant Bill Clinton ou le candidat républicain Bob Dole[381].

Si des incidents surviennent alors que les mesures de sécurité annoncées n'ont pas été prises par le serveur, la responsabilité de ce dernier pourrait être engagée.

[381] Yves Eudes, « Les pirates provos s'attaquent au Web », *le Monde*, supplément multimédia, 26 août 1996, p.26.

Troisième partie
les données personnelles

Un nombre toujours croissant de données personnelles sont collectées et traitées par les ordinateurs. Nos faits et gestes quotidiens sont enregistrés dans des machines :

- cartes à mémoire, comme les cartes bleues, dont chaque utilisation est enregistrée dans la mémoire d'un ordinateur ;
- auto-commutateurs téléphoniques dans les hôtels, les entreprises qui permettent d'enregistrer les coordonnées des appels téléphoniques ;
- vidéo-surveillance dans le métro, dans la rue, sur les lieux de travail, dans les magasins ;
- mises en place de profils types dans le secteur de la consommation en fonction des habitudes de consommation.

Toutes ces pratiques ont une incidence sur les libertés individuelles.

Les citoyens ne sont pas toujours informés des conséquences de ces techniques comme :

- la durée de conservation par les banques des traces des opérations effectuées par les cartes bleues ;
- la durée de conservation des factures téléphoniques dans les hôtels ;
- la localisation possible des utilisateurs de téléphones portables et cellulaires ;
- le devenir des images filmées par les caméras de vidéo-surveillance.

« Autant de données qui, de plus en plus, enserrent les citoyens dans leur liberté d'aller et venir, de communiquer (…) dans un carcan technique. Ces innovations sont souvent annoncées à grand bruit comme sécuritaires. Mais sait-on que le nombre de hold-up n'a en rien diminué dans les banques depuis la présence de caméras même si celles-ci facilitent l'arrestation de malfaiteurs ? (…)

Tous ces systèmes présentent avantages et inconvénients pour les utilisateurs, même si ces derniers sont souvent informés des premiers et beaucoup moins des seconds. Il n'y a manifestement pas symétrie de l'information. C'est un problème important : peut-on assurer la sécurité en mettant tout citoyen sous contrôle ? Peut-on admettre que des mesures de prime abord protectrices, puissent être utilisées comme dénonciatrices de faits et gestes relevant de la vie privée ?[382] »

La menace suivante pour notre vie privée, c'est l'interconnexion des fichiers, aujourd'hui interdite en France, mais que certains voudraient autoriser au nom de la chasse aux fraudeurs[383] : MM. Gérard Léonard et Charles de Courson ont remis au Premier ministre le 9 mai 1996, un rapport préconisant pour chasser les fraudeurs de recouper l'ensemble des fichiers informatiques du fisc et des organismes sociaux grâce à l'attribution à chaque personne d'un numéro d'identification générale.

---

[382] Franck Sérusclat, Le citoyen et le droit au respect de sa vie privée, Les nouvelles techniques d'information et de communication : l'homme cybernétique ? Rapport de l'Office parlementaire d'évaluation des choix scientifiques et technologiques, Sénat n° 232, p.239 et 242.

[383] Fraude et pratiques abusives : Rapport "Léonard-de Courson", Cahiers Lamy droit de l'informatique, juin 1996 (C), p.17.

« Big Brother a les moyens d'exister », nous avertit-on[384].

L'Internet, ensemble de réseaux et d'ordinateurs interconnectés, n'échappe pas à ces possibilités de surveillance et de collecte des données. Sans que l'on en soit toujours conscient, chaque connexion laisse des traces.

Les forums de discussion

Il faut savoir que toutes les contributions dans les forums de discussion peuvent être archivées dans des bases de données librement accessibles et dans lesquelles des recherches par nom peuvent être effectuées. Le moteur de recherche Altavista[385] garde les messages pendant un mois, celui de Dejanews[386] archive les messages sur des périodes beaucoup plus longues.

Sur le Web[387]

Chaque connexion effectuée sur un site Web laisse au minimum les informations suivantes : heure de la connexion, nom de la page requise, l'adresse IP de la machine à partir de laquelle la connexion est effectuée.

Toutes ces informations font l'objet d'une surveillance et d'une maintenance normale des sites.

Mais la surveillance peut aller au-delà. Avec l'équipement approprié, il est éventuellement possible d'obtenir les adresses de courrier électronique de l'utilisateur, le temps passé sur chaque page, le serveur à partir duquel l'utilisateur est venu.

Certains logiciels de navigation contiennent ce que l'on appelle des « cookies », qui stockent dans le disque dur de l'ordinateur de l'utilisateur les informations sur les sites visités. Chaque fois que l'on retourne sur un site, les « cookies » permettent de savoir si le site a déjà été visité auparavant[388].

En elles-mêmes, toutes ces données ne servent à rien. Mais elles peuvent être recoupées analysées, triées par les logiciels de mesure d'audience et servir à dresser un profil détaillé des activités des utilisateurs sur le Web sans que celui-ci en ait conscience.

Ces mesures d'audience permettent de mieux connaître la fréquentation des sites, d'évaluer le comportement des internautes et d'affiner le choix de la publicité que les annonceurs peuvent faire figurer sur les sites. Mais les risques de dérapages, que les informations collectées par certains serveurs soient revendues (par exemple, que les informations collectées sur un site d'information médicale soit cédées à une assurance), que ces mesures servent à dresser des profils des internautes sont aussi réels[389].

Les sites faisant directement du commerce électronique, de l'offre de transaction à distance sont évidemment en mesure d'enregistrer et de conserver les données concernant les transactions effectuées.

Certains intermédiaires peuvent avoir accès à un grand nombre d'informations sur les activités de leurs clients, leurs goûts : services en ligne comme Compuserve, AOL, tous les organismes qui servent d'intermédiaire entre le client et le commerçant pour les opérations de paiement.

Enfin, certains sites font remplir à leurs visiteurs des questionnaires avant de les laisser accéder aux contenu du service.

---

[384] Jean Guisnel, « Big Brother a les moyens d'exister », *Libération* cahier multimédia, 19 janvier 1996.
[385] <http://www.altavista.digital.com>.
[386] <http://www.dejanews.com>.
[387] Voir la page : "Who's watching you and What are You telling them" du Center for Democracy and Technology, <http://www.cdt.org>, Privacy Demonstration Page.
[388] Sur les cookies, voir : Jack Rodgers, That's the Way the Magic Cookie Crumbles, <http://www.bravado.net/rodgers/InterNetNews.html> et les spécifications de Netscape, <http://home.netscape.com/newsref/std/cookie_spec.html>.
[389] Nicole Penicaut, « La pub sur la piste des internautes », *Libération*, cahier multimédia, 17 mai 1996.

Ainsi, quelle que soit la manière dont l'information est obtenue, l'utilisation de l'Internet laisse de nombreuses informations personnelles derrière soi. Une grande partie de cette information peut rester inexploitée dans la mémoire des ordinateurs. Elle peut aussi servir à dresser des profils, voire à surveiller les activités des personnes.

Une enquête réalisée par le Georgia Institute of Technology[390] montre que si les internautes reconnaissent le besoin légitime des concepteurs de sites Web de collecter des informations relatives à l'audience de leurs sites pour les améliorer et les vendre aux publicitaires, en revanche, ils s'opposent à ce que les informations obtenues soient revendues à d'autres entreprises et apprécient de pouvoir visiter les sites de manière anonyme.

Sur l'Internet, même si de nombreuses données sont disséminées, l'informatique peut servir à regrouper ces informations et à les traiter logiquement.

La collecte et la gestion des données personnelles soulèvent des inquiétudes quant à la défense des libertés et de la vie privée des citoyens.

La France s'est dotée dès 1978 d'une loi relative aux traitement d'informations à caractère personnel : la Loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés[391]. L'objectif de cette loi est énoncé à l'article 1 :

« 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. »

Cette loi a institué une autorité administrative indépendante, la CNIL, Commission nationale de l'informatique et des libertés, chargée de veiller à la protection des données personnelles.

Cette loi s'applique aux informations qui seraient collectées sur l'Internet par les entreprises françaises.

D'autres pays, notamment européens, disposent de législations nationales spécifiques en la matière. Mais le niveau de protection des personnes à l'égard des traitements de données à caractère personnel peut varier fortement d'un Etat à l'autre. Considérant que ces différences peuvent constituer un obstacle au développement d'activités à l'échelle communautaire et fausser la concurrence, alors que les flux transfrontières de données sont amenés à se multiplier, les institutions communautaires ont adopté le 24 octobre 1995 une directive relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données[392].

Cette directive a pour ambition d'établir un haut niveau de protection des personnes tout en permettant la libre circulation des données d'un Etat à l'autre[393].

Les Etats doivent se mettre en conformité en modifiant leur législation interne dans un délai de 3 ans.

Il est important de connaître d'ores et déjà les dispositions à prendre ou à envisager pour être en conformité avec les principes posés par la directive.

---

[390] Fifth GVU WWW User Survey, conduite du 10 avril au 10 juin 1996 disponible à : <http://www.cc.gatech.edu/gvu/user_surveys/survey-04-1996/>.

[391] Loi n° 78-17, modifiée par la loi n° 88-227 du 11 mars 1988 et la loi n°92-1336 du 16 décembre 1992.

[392] Directive n° 95/46/CE, JOCE n° L281 23 novembre 1995, p.31.

[393] Considérants 2 et 3.

Présentation de la réglementation relative à la collecte et aux traitements des informations nominatives

Ne seront pas évoqués dans le cadre de cette étude les traitements concernant des domaines sensibles tels que la santé[394], la justice ou la défense. Dans ces hypothèses particulières, des procédures d'autorisation et des dispositions spécifiques sont prévues par la législation.

La loi française est en grande partie déjà conforme à la directive européenne dans laquelle on retrouve l'essentiel du système en vigueur en France : champ d'application, droits essentiels, principes d'application[395]. Je n'examinerai plus en détail les dispositions de la directive que dans les cas où il y a des points de divergence avec la loi informatique et libertés.

Les traitements concernés

Sont concernés les traitements automatisés d'informations nominatives. Le traitement automatisé fait référence aux traitements informatiques.

Pour la CNIL, une donnée nominative au sens de la loi, c'est une donnée qui permet l'identification de la personne physique, même indirectement.

Par exemple, sont considérées comme données indirectement nominatives : un numéro de compte bancaire, de carte bancaire, de téléphone, d'abonné, une photographie permettant l'identification de la personne, et relèvent de la loi informatique et libertés les situations suivantes :

- utilisation d'automates d'appel, de commutateurs téléphoniques ;
- utilisation de mailings ;
- fichier de marketing direct ;
- fichier de clients, même s'il s'agit de sociétés dès lors que les fichiers intègrent les coordonnées de personnes physiques ;
- établissement de statistiques utilisant des informations sur les personnes, mise en place et exploitation de messageries ;
- bases de données incluant des informations nominatives.

A partir du moment où le numéro de téléphone est considéré comme une donnée qui peut servir à l'identification de la personne, une adresse de courrier électronique doit également être estimée comme une information nominative au sens de la loi. De nombreuses adresses e-mail sont d'ailleurs composées directement du nom de la personne.

Comme cet aperçu l'aura montré, le champ d'application de la loi informatique et liberté est en réalité très vaste et concerne toutes les données qui peuvent servir à l'identification des personnes. De nombreuses applications que l'on peut mettre en place sur l'Internet vont constituer des traitements de données personnelles rentrant dans le champ d'application de la loi.

Il en est ainsi :

- des listes de diffusion ;
- des formulaires en tous genres que l'on fait remplir en ligne par les internautes ;

[394] Une loi n° 94-548 du 1er juillet 1994 (JO du 2 juillet) a prévu une réglementation particulière pour les traitements de données nominatives ayant pour fin la recherche dans le domaine de la santé. Sur cette loi, voir Nathalie Mallet-Poujol, La loi du 1er juillet 1994 relative au traitement de données nominatives ayant pour fin la recherche dans le domaine de la santé : contraindre ou convaincre ? Droit de l'Informatique et des Télécoms 1995/1, p.17.

[395] Jean Frayssinet, La directive du 24 octobre 1995, Cahiers Lamy droit de l'informatique, mars 1996, supplément.

- des applications permettant l'enregistrement de télétransactions ;
- des moteurs de recherche dès lors que des recherches par nom sont possibles.

Les serveurs hébergeant des sites Web enregistrent tous des informations relatives à la fréquentation du site. La simple mise en place d'un site Web constitue-t-il un traitement automatisé de données ?

Tout dépend de l'utilisation faite de ces statistiques.

Les statistiques de fréquentation des pages, le type de logiciel et d'ordinateur ne sont pas des données nominatives. L'adresse IP à partir de laquelle est faite la connexion peut être une donnée nominative si la machine est individuelle, c'est-à-dire attribuée à un seul utilisateur.

L'établissement de statistiques ne rentre dans la champ d'application de la loi que lorsque les données étudiées permettent l'identification des personnes.

Ce sera le cas si les données collectées incluent l'adresse e-mail.

Les données recueillies peuvent également servir à l'établissement de profils. Les données elles-mêmes ne sont pas personnelles, mais un rapprochement est effectué qui va leur donner ce caractère. Ce sera notamment le cas lorsque le serveur enregistre les précédentes visites de l'internaute grâce au « cookie » intégré dans le logiciel de navigation. Si l'on étudie la fréquentation de la même personne on va être amené à connaître ses goûts et ses habitudes, ses centres d'intérêt.

L'établissement de profils est appelé par la CNIL « segmentation comportementale ». Il s'agit de construire à partir de l'observation statistique d'une population, des classes d'individus (segments) en fonction des comportements analysés. Cette méthode permet de cibler les actions de prospection et de marketing auprès de la clientèle d'après les attentes supposées des intéressés.

La CNIL s'est penchée sur ces méthodes[396].

Elle considère que l'on ne saurait faire grief à une entreprise de chercher à caractériser sa clientèle et de procéder à des tris en fonction de variables pertinentes pour orienter sa stratégie et son action commerciale, mais rappelle que l'utilisation des méthodes de segmentation comportementale doit respecter les dispositions relatives à la protection des données personnelles[397]. Pour la CNIL, les informations nominatives ne se limitent pas à l'identité des personnes, elles englobent les données servant à la qualifier.

L'établissement de profils relève donc de la loi informatique et liberté.

La collecte des informations

Quelles données peuvent être collectées ?

Certaines informations sont considérées comme trop sensibles pour être recueillies en l'absence d'accord express de la personne concernée. Il s'agit des informations faisant apparaître même indirectement les origines raciales, les opinions politiques, philosophiques ou religieuses, les appartenances syndicales, les mœurs, notamment sexuelles (article 31 de la loi et article 8-1 de la directive).

L'accord exprès doit être entendu au sens d'accord écrit des intéressés[398].

[396] Délibération n° 93032 du 6 avril 1993.
[397] Sylvie Lepany, La CNIL et la segmentation comportementale, Droit de l'Informatique et des Télécoms 1994/1, p.75.
[398] CNIL, 7e rapport, p.78.

Comment sont collectées les informations ?

Le principe de loyauté

La loi pose un principe général de loyauté et indique que la collecte de données opérée par tout moyen frauduleux, déloyal ou illicite est interdite (article 25 de la loi).

Il s'agit d'une sorte d'exigence de transparence.

Il a par exemple été jugé que la collecte d'informations réalisée à l'insu des intéressés constituait une manœuvre déloyale dans la mesure où la personne concernée n'avait pas eu la possibilité de faire jouer son droit d'opposition à la collecte[399].

Les entreprises éviteront par exemple de collecter les adresses de courrier électronique à l'insu des personnes visitant leur site Web. La mise en place d'outils pour traiter les informations recueillies par les « cookies » peut constituer un moyen déloyal de collecte.

Les personnes auprès desquelles sont recueillies les données nominatives doivent être informées (article 27 de la loi) :

- du caractère obligatoire ou facultatif des réponses ;
- des conséquences à leur égard d'un défaut de réponse ;
- des personnes physiques ou morales destinataires des informations ;
- de l'existence d'un droit d'accès et de rectification.

Si lesdites informations sont recueillies au moyen de formulaires en ligne, les pages du service devront afficher un avertissement relatif à ces informations.

La notice explicative de la CNIL donne à titre d'exemple : « Les informations figurant dans nos fichiers clients peuvent donner lieu à l'exercice du droit d'accès et de rectification selon les dispositions de la loi du 6 janvier 1978. Notre société est seule destinataire des informations que vous lui communiquez. »

Les cessions de fichiers

Si une cession du fichier est envisagée, les personnes auprès desquelles ces informations sont collectées doivent en être informées afin d'être en mesure de s'y opposer. La CNIL recommande l'emploi de la formule suivante qu'il conviendra évidemment d'adapter aux formulaires en ligne : « Par notre intermédiaire, vous pouvez être amené à recevoir des propositions d'autres entreprises. Si vous ne le souhaitez pas, il suffit de nous écrire (…) ou de cocher la case suivante (…) ».

Informations lorsque les données n'ont pas été collectées auprès de la personne concernée

Ce droit prévu par l'article 11 de la directive va plus loin que ce qui est exigé par la loi française. La personne doit être informée de l'identité du responsable du traitement et des finalités poursuivies dès l'enregistrement des données ou au plus tard lors de la première communication des données à un tiers. Elle doit également être informée d'un droit d'accès et de rectification, de la catégorie des données concernées et des destinataires des données lorsque ces informations supplémentaires « sont nécessaires pour assurer à l'égard de la personne concernée un traitement loyal des données ».

Cette nouvelle obligation qui apparaît importante doit être notamment prise en compte en cas de cession des données à un tiers ou de collecte de données disséminées sur l'Internet ou de traitement de données statistiques pour dresser des profils de comportement et de consommation des internautes.

---

[399] Rennes, 24 juin 1986, Expertises n° 91, janvier 1987.

Cette obligation pourrait en pratique imposer d'afficher sur la page d'accueil du service Web cette information lorsque les données recueillies lors des consultations du site sont utilisées par l'éditeur du site pour établir des profils de consommation et surtout lorsqu'elles sont revendues à des tiers.

Quant à l'information des personnes sur lesquelles des données ont été collectées sur l'Internet, on pourrait imaginer qu'elle puisse se faire par courrier électronique.

L'exploitation des fichiers

Droit d'opposition

La loi pose le principe que « toute personne physique a le droit de s'opposer, pour des raisons légitimes, à ce que des informations nominatives la concernant fassent l'objet d'un traitement (article 26 de la loi) ».

La directive reconnaît le droit de s'opposer, sur demande et gratuitement, au traitement envisagé à des fins de prospection.

Aujourd'hui, les personnes qui souhaitent être retirées des fichiers d'adresses utilisées par les entreprises pour leur prospection commerciale ont 3 possibilités :

- liste orange de France Télécom, qui regroupe les abonnés qui refusent que leurs coordonnées soient utilisées aux fins de prospection commerciale qui sont donc retirés des listes d'abonnés commercialisées par France Télécom ;
- liste Safran comprenant la liste des personnes qui ne souhaitent pas être démarchées par télex ou télécopie également gérée par France Télécom[400] ;
- liste Robinson mise en place par la profession du marketing direct[401] et mentionnant les personnes souhaitant, pour recevoir moins de courrier publicitaire, être rayées des fichiers de sollicitations commerciales.

Les professionnels du marketing direct se sont également dotés d'un code de déontologie concernant la protection des données à caractère personnel[402].

La nouvelle loi sur les télécommunications a prévu la mise en place d'un annuaire universel géré par une entité indépendante à la fois du ministère des Télécommunications et des opérateurs de téléphonie[403]. L'article L33-4 précise que « la publication des listes d'abonnés ou d'utilisateurs est libre, sous réserve de la protection des droits des personnes concernées ».

Parmi les droits garantis figure celui d'interdire que les informations nominatives concernant une personne soient utilisées dans des opérations commerciales.

Aujourd'hui, de nouveaux types de fichiers apparaissent qui ne concernent plus les numéros de télécopies ou adresses postales, mais les courriers électroniques et sont utilisés pour l'envoi de mailings. L'envoi de courrier électronique publicitaire non sollicité est contraire aux règles de la Netiquette, un principe qui ne suffit pas à décourager certaines entreprises de procéder ainsi. Il faudra sans doute un jour intégrer les adresses électroniques dans les données que les intéressés peuvent choisir d'exclure d'utilisation à des fins de prospection commerciale.

---

[400] Article 10 de la loi n° 89-1008 du 31 décembre 1989.
[401] Liste tenue par l'Union française du marketing direct, 60, rue de la Boétie, 75 008 Paris.
[402] Voir Herbert Maisl, Marketing direct et données personnelles, définition d'une déontologie, Droit de l'Informatique et des Télécoms 1995/1, p.71.
[403] Article L35-4 du Code des postes et télécommunications.

Dans un système décentralisé comme l'Internet, la mise en place de fichiers centraux pourrait être aléatoire et difficile à mettre en œuvre car les annuaires de courrier électronique peuvent être réalisés n'importe où, et pas nécessairement en France.

Par exemple, il existe un annuaire d'adresses électroniques sur l'Internet, le Four 11[404] géré par une société californienne. Le service ne doit pas être utilisé pour accéder à de grandes quantités d'adresses e-mail et donc pour télécharger l'annuaire à des fins commerciales[405].

Rien ne garantit que cette politique sera toujours respectée par cette société américaine et rien n'empêche d'autres entreprises de réaliser de tels annuaires aux fins de commercialisation des adresses collectées.

La directive instaure un droit nouveau, non prévu dans la loi française : le droit d'être informé avant que des données à caractère personnel ne soient pour la première fois communiquées à des tiers ou utilisées pour le compte de tiers à des fins de prospection commerciale et de se voir expressément offrir le droit de s'opposer, gratuitement, à ladite communication ou utilisation (article 14 de la directive).

Cette obligation pourrait poser des problèmes pratiques de mise en œuvre car elle implique une information préalable sur ce droit d'opposition directe.

Droit à l'oubli

Les données recueillies ne doivent pas être indéfiniment archivées et ne doivent pas être conservées au-delà de la durée prévue lors de la déclaration du traitement (article 26 de la loi).

Par exemple, les renseignements concernant les abonnés d'un périodique ne peuvent pas être conservés pendant plus d'un an après l'expiration de l'abonnement[406].

L'obligation de sécurité

La personne responsable d'un fichier informatique nominatif doit prendre toutes les précautions utiles pour préserver la sécurité et la confidentialité des informations et notamment empêcher qu'elles ne soient divulguées à des tiers non autorisés (article 29 de la loi). Le même type d'obligation est prévu par la directive : le responsable du traitement doit mettre en œuvre « les mesures techniques et d'organisation appropriées pour protéger les données à caractère personnel contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisés, notamment lorsque le traitement comporte des transmissions de données dans un réseau »(article 17 de la directive).

La négligence dans la mise en œuvre de cette obligation de sécurité peut engager la responsabilité pénale du responsable du traitement[407].

La finalité du traitement

La finalité du traitement doit être respectée

Il s'agit d'un principe important. Les données doivent être collectées pour des finalités déterminées, explicites et légitimes, et ne peuvent pas être traitées ultérieurement de manière incompatible avec ces finalités. Elles doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et traitées ultérieurement (article 6 b) et c) de la directive).

---

[404] Site Web : <http://www.four11.com>.
[405] Bruno Giussani, « Composez le 411 », *Planète Internet* n°4, décembre 1995, p.38.
[406] Norme simplifiée n° 25- délibération n° 81-117 du 1er décembre 1981.
[407] Voir supra

Chaque fichier est créé dans un but particulier : fichier de clients, paie du personnel, etc. Il ne peut pas être utilisé à d'autres fins. Par exemple, on ne peut pas céder un fichier client à une société tierce si cela n'a pas été indiqué dans la déclaration et si les personnes concernées n'ont pas été informées de cette possibilité.

Droit d'accès et de rectification

Toute personne justifiant de son identité a le droit d'interroger la personne responsable d'un fichier informatique en vue de savoir si le fichier inclut des renseignements la concernant et obtenir communication de ces informations. Si elle constate que les informations la concernant sont inexactes ou que leur conservation est interdite, elle peut demander que ces informations soient modifiées et si cette demande est justifiée, le détenteur du fichier devra y procéder (articles 34, 35 et 36 de la loi).

L'article L33-4 du CPT au sujet de la publication des listes d'abonnés ou d'utilisateurs des réseaux ou services de communication prévoit que figure parmi les droits garantis le droit de pouvoir obtenir communication desdites informations nominatives et exiger qu'elles soient rectifiées, complétées, clarifiées, mises à jour ou effacées, dans des conditions prévues aux articles 35 et 36.

En cas de problème pour exercer ce droit d'accès et de rectification, la personne fichée peut saisir la CNIL.

La déclaration du traitement automatisé de données

Tous les traitements mis en place par les entreprises du secteur privé doivent faire l'objet d'une déclaration préalable auprès de la CNIL. Le traitement ne peut en principe être mis en œuvre qu'à réception du récépissé de la CNIL. En pratique, compte tenu des délais de traitement des dossiers, il n'est pas toujours aisé de respecter cette obligation et beaucoup de traitements sont en réalité mis en œuvre dès l'envoi du dossier de déclaration.

La mise en œuvre des traitements du secteur public est subordonnée à la publication d'un acte réglementaire pris après avis de la CNIL portant création du traitement.

La directive[408] prévoit une simple notification du traitement qui doit faire apparaître :

- l'identification du responsable du traitement ;
- les finalités de celui-ci ;
- la description des personnes et des données concernées ;
- les destinataires ;
- les transferts vers un pays tiers ;
- les mesures de sécurité.

Cependant, les traitements susceptibles de présenter des risques particuliers au regard des droits et libertés des personnes concernées font l'objet d'un contrôle préalable (article 20 de la directive).

Lorsque la directive sera transposée en droit français, un assouplissement du régime des déclarations et autorisations pourra être prévu.

En attendant, le dispositif actuel continue de s'appliquer.

[408] Article 19.

Secteur privé

La CNIL a édité un formulaire type (Cerfa n° 99001) de « déclaration d'un traitement automatisé d'informations nominatives » qu'il suffit de remplir en suivant les instructions données dans la notice explicative accompagnant le formulaire.

On peut se procurer ce formulaire :

- auprès des préfectures ;
- auprès des Chambres de commerce et d'industrie ;
- auprès de la CNIL :
  21, rue Saint-Guillaume
  75340 Paris Cedex 07
  tél : 01 53 73 22 22

La CNIL peut également faire parvenir ce formulaire par correspondance sur simple demande.

On peut enfin le commander par Minitel en quelques minutes sur le 36 15 code CNIL.

Pour les fichiers les plus courants et qui ne comportent pas de risque d'atteinte à la vie privée ou aux libertés, la CNIL a établi un certain nombre de normes simplifiées.

Si le traitement envisagé correspond à une de ces normes, une déclaration dite simplifiée est établie : en pratique, seuls les renseignements de la première page du formulaire sont à fournir.

Des normes simplifiées existent par exemple pour les fichiers de clients[409], d'abonnés à un périodique de presse[410], de clients d'entreprises de vente par correspondance[411], de paie des personnels[412], de listes d'adresses ayant pour objet l'envoi d'informations[413]. La notice explicative de la CNIL comprend un tableau des normes simplifiées qui permet de vérifier si le traitement envisagé correspond à une de ces normes.

Si le fichier considéré ne rentre pas dans le cadre d'une norme simplifiée, il faut fournir les annexes demandées dans le formulaire, ce qui est nettement plus fastidieux.

Malheureusement, concernant l'Internet, beaucoup de traitements couramment pratiqués, faute d'avoir fait déjà l'objet de normes simplifiées ou de rentrer dans le cadre des normes simplifiées existantes, devront faire l'objet d'une déclaration ordinaire.

Par exemple, la mise en place d'une simple liste de diffusion ne correspond pas au cas de la norme relative aux listes d'adresses ayant pour objet l'envoi d'information et devrait faire l'objet d'une déclaration normale. Autre exemple, la norme simplifiée correspondant à la vente par correspondance concerne les entreprises dont l'objet social inclus la vente par correspondance.

Une fois le formulaire rempli avec les annexes éventuelles, il faut envoyer le tout à la CNIL, en 3 exemplaires par lettre recommandée avec accusé de réception.

La CNIL adresse ensuite un récépissé de déclaration, et le déclarant peut alors mettre en œuvre son fichier.

---

[409] Norme simplifiée n°11 concernant les traitements automatisés d'informations nominatives relatifs à la gestion des fichiers de clients, délibération n°80-21 du 24 juin 1980.
[410] Norme simplifiée n°25, délibération n°81-117 du 1er décembre 1981.
[411] Norme simplifiée n°17, délibération n°81-16 du 17 février 1981.
[412] Norme simplifiée n°28, délibération n°85-38 du 18 juin 1985.
[413] Norme simplifiée n° 15, délibération n°80-32 du 21 octobre 1980.

Secteur public

Les traitements automatisés d'informations nominatives opérés pour le compte de l'Etat, d'un établissement public ou d'une collectivité territoriale ou d'une personne morale de droit privé gérant un service public sont autorisés par une loi ou un acte réglementaire pris après avis motivé de la CNIL. Si l'avis de la CNIL est défavorable, il ne peut être passé outre que par décret pris sur avis conforme du Conseil d'Etat (article 15 de la loi). Ce système est évidemment assez lourd.

Le formulaire de la CNIL sert dans ce cas à présenter la demande d'avis. Un dossier complet avec toutes les annexes demandées doit être remis à la CNIL, qui a un délai de 2 mois, renouvelable une fois pour notifier son avis. En cas de silence au bout de ces délais, l'avis est réputé favorable. L'acte réglementaire doit ensuite être publié.

Des normes simplifiées pour les traitements les plus courants existent également pour les fichiers du secteur public.

Les sanctions

La loi informatique et libertés a prévu, en cas de non-respect de ses dispositions, différentes sanctions pénales. Certes, bien souvent, la CNIL préférera inviter le détenteur du fichier à régulariser sa situation, mais il lui arrive aussi de transmettre certaines affaires aux tribunaux.

La loi a prévu les infractions suivantes définies comme des « atteintes au droit de la personne résultant des fichiers ou des traitements informatiques » :

- l'omission de la déclaration préalable constitue le délit de création de fichier clandestin, 3 ans d'emprisonnement et 300 000 francs d'amende (article 226-16 du Code pénal) ;
- manquement à la sécurité, 5 ans d'emprisonnement et 2 millions de francs d'amende (article 226-17 du Code pénal) ;
- collecte frauduleuse, déloyale ou illicite, 5 ans d'emprisonnement et 2 millions de francs d'amende (article 226-18 du Code pénal) ;
- collecte d'informations sensibles, 5 ans d'emprisonnement et 2 millions de francs d'amende (article 226-19 du Code pénal) ;
- conservation des informations au-delà de la date prescrite, 5 ans d'emprisonnement et 2 millions de francs d'amende (article 226-20 du Code pénal) ;
- délit de détournement de finalité d'informations nominatives, 5 ans d'emprisonnement et 2 millions de francs d'amende (article 226-21 du Code pénal) ;
- délit de divulgation illicite d'informations nominatives, un an d'emprisonnement et 100 000 francs d'amende (article 226-22 du Code pénal) ;
- la non-information des personnes interrogées, l'entrave au droit d'accès et de communication, l'entrave au droit de rectification sont punies des peines prévues pour les contraventions de 5^{e} classe (10 000 francs d'amende)[414].

Les flux internationaux de données

L'article 25 de la directive contient des dispositions spécifiques relatives aux transfert de données vers des pays tiers (non membres de l'Union européenne).

[414] Décret n° 81-1142 du 23 décembre 1981, JO du 26 décembre.

Ce transfert ne peut avoir lieu que si le pays tiers assure un niveau de protection adéquat. Sinon le transfert est interdit, sauf certaines exceptions énumérées à l'article 26 de la directive, dont le consentement de la personne concernée et le cas du transfert nécessaire à l'exécution d'un contrat entre la personne concernée et le responsable du traitement.

Le respect de ce principe sur un réseau comme l'Internet où il y a nécessairement des pays connectés qui n'assurent pas un niveau de protection adéquat au sens de la directive va se révéler difficile.

Notamment, les Etats-Unis ne sont pas considérés comme un pays tiers disposant d'un niveau de protection adéquat. L'usage des fichiers des sociétés privées n'y fait pas l'objet d'une réglementation. Le Privacy Act de 1974 concerne les traitements informatiques de données dans le secteur public[415].

Malgré les risques que font courir les technologies de l'information à la vie privée[416], l'administration américaine n'entend pas adopter de réglementation spécifique et souhaite continuer à appliquer les principes suivis jusqu'ici, à savoir :

- adoption de codes de conduite par les professions concernées ;
- recours aux dispositions contractuelles.

Les optiques américaines et européennes diffèrent donc sensiblement[417].

La CNIL a été saisie d'une demande concernant la mise en place sur l'Internet d'annuaires professionnels de chercheurs de l'Institut de physique nucléaire d'Orsay et du Centre national du calcul parallèle des sciences de la terre.

L'annuaire comprend les renseignements suivant : sexe, nom et prénoms, lieu de travail et service d'affectation, numéros de téléphone, télécopie et adresse de courrier électronique, mots-clés caractérisant l'emploi occupé et les thèmes de recherche.

La CNIL a émis un avis favorable pour la mise en place de ces annuaires[418], tout en posant des conditions particulières :

- obtention de l'accord exprès des chercheurs concernés ;
- affichage sur l'écran de l'ordinateur de la personne se connectant à l'annuaire d'un avis rappelant les droits, garanties et protections dont bénéficient les chercheurs en vertu des réglementations françaises et européennes ainsi que la mention de l'interdiction de capturer ces informations pour enrichir des bases de données à des fins commerciales ou publicitaires, avec un lien sur la loi informatique et libertés et des dispositions du Code pénal.

Or, les conditions posées par la CNIL ne résultent pas des nécessités de la loi[419]. Les informations traitées sont des informations professionnelles qui ne sont donc pas sensibles et échappent à la vie privée.

Deux raisons semblent expliquer cette position de la CNIL.

D'une part, la CNIL considère que l'Internet compte tenu de sa « nature particulière » présente des « risques inhérents ».

D'autre part, la CNIL semble anticiper l'intégration de la directive dans notre législation puisque cette dernière interdit le transfert d'informations nominatives vers des pays n'assurant pas un niveau de protection adéquat au sens européen.

---

[415] O. Hance, Business et Droit d'Internet, Best Of Editions 1996, p. 120.

[416] Sur la situation aux Etats-Unis, voir : Oscar H. Gandy, Jr., Legitimate Business Interest. No end in sight?, article préparé pour le Chigago Legal Forum's Symposium sur « The Law of Cyberspace », 3 et 4 novembre 1995, <http://www-law.lib.uchicago.edu/forum/96vol.htm>.

[417] Alain Bailliart, Internet et les flux transfrontières de données, les Petites Affiches, 22 mai 1996, n° 62, p.13.

[418] Délibérations 95-132 et 95-131 du 7 novembre 1995, Gaz. Pal. 27 janvier 1996, p. 36.

[419] Alain Bensoussan (sous la direction de), Internet aspects juridiques, éditions Hermès 1996, p.97.

Cette position stricte de la CNIL va sans doute poser des problèmes pratiques d'application.

Toute diffusion d'annuaire professionnel nécessiterait selon cette doctrine d'obtenir l'accord préalable de toutes les personnes enregistrées dans l'annuaire. Un consentement est exprès et ne peut pas résulter du simple silence. Pourtant on voit apparaître des annuaires de journalistes, d'avocats, etc. Ce type d'annuaires professionnels ne semble pas présenter de risques particuliers pour la vie privée et peuvent s'avérer fort utiles. Une information auprès des personnes inscrites dans l'annuaire devrait être suffisante pour leur permettre d'exercer leur droit d'opposition.

Les bases de données de noms de domaine qui sont indispensables, car elles permettent de retrouver les coordonnées des administrateurs de sites, comportent des données nominatives. Ces données, même si elles sont d'ordre professionnel, devraient en application de la doctrine adoptée par la CNIL nécessiter le consentement exprès des personnes mentionnées.

On peut citer également le cas des listes de diffusion qui permettent par l'utilisation d'une commande adéquate auprès du serveur gestionnaire d'obtenir les adresses e-mail des abonnés à ladite liste. Va-t-on devoir avant de s'inscrire dans une liste de diffusion envoyer une lettre écrite à l'administrateur du serveur ?

La position adoptée par la CNIL semble trop restrictive. En outre, notre législation française et européenne risque de se révéler en pratique impuissante à empêcher la constitution de fichiers dans des pays n'ayant pas le même degré de protection quant au traitement des données personnelles.

La loi française est applicable si le traitement est effectué par un établissement localisé en France (article 4 de la directive).

Le droit français est également applicable en cas de collecte de données réalisée en France à destination de l'étranger[420].

Avec l'Internet, il est possible de réaliser depuis l'étranger des collectes de données concernant des citoyens français : les données peuvent par exemple être disséminées par les internautes lorsqu'ils se connectent à des sites Web hébergés sur des serveurs étrangers ou lorsqu'ils envoient dans les forums de discussion des messages.

Dans ces hypothèses, la donnée est collectée hors de France. Or, la loi applicable en cas de collecte de données réalisée à l'étranger à destination de la France est en principe la loi étrangère[421].

Il est donc aisé de collecter, stocker et traiter des données depuis un pays ayant un niveau plus faible de protection des données sans contrevenir aux dispositions concernant l'exportation de données vers des pays tiers. La directive vise en effet le lieu de localisation du responsable du traitement et le lieu de localisation du moyen utilisé à des fins de traitement mais pas la collecte et le traitement de données hors frontière pourtant possible avec l'Internet.

Le traitement pourrait être ensuite cédé puis réimporté en France ou en Europe. Ce type de situations ne semble pas couvert par la directive. La directive traite de l'exportation de données vers des pays tiers mais pas de l'importation.

Face aux défis posés par les flux transfrontières de données nominatives sur les réseaux informatiques, la directive semble déjà dépassée.

---

[420] Lamy informatique 1996, n°748.
[421] Lamy informatique n°753.

Quatrième partie
la cryptographie

Introduction à la cryptographie : définition, fonctionnement, applications

Définition

La cryptographie, ou chiffrement, est le processus de transcription d'une information intelligible en une information inintelligible par l'application de conventions secrètes dont l'effet est réversible. La loi française définit les prestations de cryptologie comme :

« Toutes prestations visant à transformer à l'aide de conventions secrètes des informations ou signaux clairs en informations ou signaux inintelligibles pour des tiers, ou à réaliser l'opération inverse, grâce à des moyens matériels ou logiciels conçus à cet effet »[422].

La stéganographie[423] est une technique qui permet de communiquer, de manière non apparente, des messages cachés dans d'autres messages. Les logiciels existant actuellement permettent de modifier d'une manière indétectable par l'homme, mais compréhensible par l'ordinateur, un fichier numérique de son ou d'image. En présence d'un message crypté, on se rend compte qu'il a été chiffré alors qu'il n'est pas possible de détecter et de prouver qu'un message a été codé par un procédé de stéganographie. La stéganographie constitue également un moyen de transcription d'une information intelligible en une information inintelligible par l'application de conventions secrètes et elle est soumise à ce titre à la réglementation en matière de cryptographie.

Dans le contexte d'une société où les échanges d'informations numériques se développent, il est indispensable de pouvoir bénéficier de systèmes sécurisés pour protéger les données à caractère personnel ou confidentiel, assurer la sécurité des transactions financières et commerciales, passer des contrats en l'absence de support papier.

Pour réaliser ces objectifs, la cryptographie s'avère être un outil indispensable.

Il existe deux grands types de cryptographie :

- la cryptographie symétrique : la même clé (le code secret) est utilisée pour crypter et décrypter l'information. Le problème de cette méthode est qu'il faut trouver le moyen de transmettre de manière sécurisée la clé à son correspondant ;
- la cryptographie asymétrique : ce n'est pas la même clé qui crypte et qui décrypte les messages. L'utilisateur possède une clé privée et une clé publique. Il distribue sa clé publique et garde secrète sa clé privée. Dans ce type d'application, tout le monde peut lui écrire en utilisant la clé publique, mais seul l'utilisateur destinataire pourra décrypter et

[422] Article 28 de la loi 90-1170 du 29 décembre 1990 modifée.
[423] Sur la stéganographie, voir : Neil F. Johnson, Steganography, <http://adams.patriot.net/~johnson/html/neil/sec/steg.htm>.

donc lire le message avec sa clé privée. La cryptographie permet ici d'assurer la confidentialité des données transitant sur un réseau : les données sont uniquement portées à la connaissance des personnes autorisées.

Une autre paire de clés sera utilisée pour s'assurer de l'identité de l'émetteur d'un message : c'est la question de l'authentification. L'utilisateur crypte avec sa clé privée son message. Tout le monde peut décrypter le message avec la clé publique correspondant à l'expéditeur ainsi identifié.

Fonctionnement

Les méthodes de cryptage à clés asymétriques reposent sur des calculs mathémathiques sophistiqués utilisant des nombres premiers (nombres qui ne sont divisibles que par 1 et par eux-mêmes) gérés par des algorithmes (suite d'opérations nécessaires à l'accomplissement d'une opération). Il est facile de multiplier deux nombres premiers par exemple 127 et 997 et de trouver 126 619. Mais il est plus difficile de factoriser c'est-à-dire de retrouver 127 et 997 à partir de 126 619.

C'est sur ce principe mathématique que repose la cryptographie asymétrique.

Le premier système de cryptographie à clé publique a été proposé en 1978 par Ronald Rivest, Adi Shamir et Leonard Adleman, trois chercheurs du MIT, une université américaine, qui ont donné leur nom au système baptisé RSA[424]. C'est sur cette méthode RSA que sont fondés de nombreux logiciels de chiffrement et la plupart des logiciels de paiement sécurisé comme celui de Netscape et de Digicash.

Pour vérifier l'intégrité du message transmis, le caractère exact et complet des données envoyées, on utilise une fonction mathématique qui associe une valeur calculée au message. Lorsque le destinataire reçoit le message, il calcule sa propre valeur et la compare avec celle qui lui a été envoyée : si les deux valeurs sont identiques, on est assuré que les documents n'ont pas été modifiés.

La combinaison de procédés d'authentification de l'expéditeur et de vérification de l'intégrité de son message permet la création de véritables signatures électroniques qui s'avèrent en pratique plus difficilement falsifiables que nos procédés de paraphes et signatures manuscrites.

Enfin, la cryptographie permet de garantir la « non-répudiation », c'est-à-dire que l'émetteur ou le destinataire de la communication ne peuvent ensuite pas nier l'envoi ou la réception, ni le contenu de la communication.

La technique informatique permet d'élaborer des outils générant des clés et utilisant les systèmes de cryptographie de manière transparente pour l'utilisateur.

Le plus célèbre des procédés de cryptage, et un des plus sûrs d'après les spécialistes, devenu un standard de fait sur l'Internet où il est facile de se le procurer, est le logiciel PGP (Pretty Good Privacy), basé sur le système RSA, inventé par l'Américain Phil Zimmerman[425].

Pour que le système soit fiable, il est d'autant plus nécessaire que les clés de cryptage utilisées soient suffisament sûres, que les falsifications et atteintes ne soient pas physiquement décelables.

Avec les méthodes de codage actuelles, la sûreté d'une clé dépend de sa longueur.

Mais plus la clé est longue, plus la transaction ou la communication va être lente, en raison du temps nécessaire au logiciel pour faire les calculs. Ce qui est gagné en sécurité est donc perdu en rapidité et en convivialité.

---

[424] A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, In : Communication of the ACM, February 1978, p.120.

[425] « Comment PGP protège les messages », *Libération*, cahier multimédia, 19 janvier 1996, p.VIII ; Stéphane Bortzmeyer, L'utilisation du chiffrement en France, <http://www.cnam.fr/Network/Crypto/>.

Pour décrypter un document sans posséder la clé, il est nécessaire de disposer d'ordinateurs capables d'effectuer un très grand nombre d'opérations par seconde. La fiabilité d'un système dépend de la puissance de calcul nécessaire à mettre en œuvre pour casser le code. La dépense nécessaire pour casser le code doit être disproportionnée à la valeur de l'information protégée.

Aujourd'hui, une clé d'une longueur de 1024 bits nécessiterait plusieurs milliards d'années de calcul d'ordinateur pour être cassée.

Cependant, ce système dépend de l'état de la technique, qui évolue très rapidement.

Un algorithme jugé incassable aujourd'hui ne le sera peut-être plus dans quelques années. Même si le code est incassable, la conception du logiciel peut présenter des failles qui peuvent être exploitées pour trouver les messages chiffrés sans avoir à faire des calculs massifs. Ce type de problème est en tout cas arrivé dans une des versions du programme sécurisé de Netscape[426].

Applications

Les applications de la cryptographie dans le cadre des réseaux informatiques sont variées :

- commerce électronique ;
- protection du secret médical, du secret professionnel ;
- protection de la confidentialité des correspondances ;
- protection de la vie privée ;
- protection des traitements d'informations nominatives, des bases de données, contre les intrusions, les divulgations à des tiers non autorisés ;
- protection contre la fraude informatique ;
- transmission sécurisée des données sensibles à travers les réseaux internationaux ;
- preuve informatique ;
- identification et authentification ;
- protection contre l'espionnage industriel.

Pour la CNIL, « la sécurité des données est donc, pour la protection de la vie privée et des libertés, la première des exigences. Les techniques de certification et d'authentification, de contrôle de l'intégrité et de cryptage des informations issues de la voix et de l'image primitives doivent être développées »[427]. Face aux menaces que fait peser l'informatique sur notre vie privée[428], l'usage de la cryptographie pour assurer la confidentialité apparaît comme un juste retour de balancier.

La cryptographie est également indispensable au développement du commerce électronique. La cryptographie permet de sécuriser les transactions financières et la plupart des systèmes de paiement électronique actuellement envisagés utilisent les techniques de chiffrement[429].

Dans le cadre des réseaux ouverts, les communications sont facilement interceptées et le secret des correspondances n'est plus garanti[430]. La cryptographie permet de pallier à cet inconvénient. Des données sensibles peuvent être communiquées sans craindre les indiscrétions.

---

[426] Steven Levy, Wisecrackers, Wired magazine, March 1996, p.128.
[427] Voix, Image et Protection des données personnelles, rapport de la CNIL, Documentation française 1996, p.49
[428] Voir supra
[429] Voir infra
[430] Voir supra

Si l'on crypte les messages avec des algorithmes puissants, le contenu des informations cryptées devient indéchiffrable pour tous, y compris pour l'Etat. Or la cryptographie, procédé d'origine militaire, est considérée comme un enjeu de sécurité intérieure et extérieure par un certain nombre de gouvernements.

En France, les moyens de cryptologie ont été classés jusqu'à la loi du 29 décembre 1990 sur la réglementation des télécommunications parmi les matériels de guerre. La réglementation actuelle, même si elle a été assouplie, reste lourde avec une surveillance étroite de l'Etat sur tout utilisateur d'un procédé de chiffrement.

Aux Etats-Unis, son utilisation y est libre à l'intérieur des Etats-Unis. Mais les produits de cryptographie sont classés dans la catégorie des munitions et leur exportation nécessite l'autorisation du département d'Etat (State Department) et de la National Security Agency (NSA), conformément aux règles prévues par l'ITAR, International Traffic In Arm Regulation[431].

La divulgation ou le transfert de données techniques à une personne étrangère, même si elle réside sur le territoire américain est considérée comme une exportation[432].

La France est cependant le seul pays du bloc occidental à interdire le libre usage de la cryptographie sur son territoire.

La législation française ou la suspicion d'un Etat

Analyse de la législation française

En France, la fourniture, l'exportation et même la simple utilisation de méthodes de cryptage sont réglementées par l'article 28 de la loi du 29 décembre 1990 sur la réglementation des télécommunications[433], récemment modifiée par l'article 17 de la loi du 26 juillet 1996 sur la réglementation des télécommunications[434].

Selon les cas, une déclaration ou une demande d'autorisation préalable doit être effectuée auprès des services du Premier ministre.

La loi du 26 juillet 1996 a introduit des cas où l'usage de la cryptographie peut être libre, et où les formalités de déclaration et d'autorisation sont allégées.

Cependant, un examen des nouvelles dispositions et de leurs implications pratiques montre qu'en réalité, le système qui existe depuis 1990 n'est pas bouleversé dans ses fondements.[435]

Avant d'examiner les nouveaux cas introduits par la loi du 26 juillet 1996, il convient d'examiner le régime de droit commun des demandes d'autorisation et des déclarations et la manière dont il est appliqué par l'administration. Cette autorisation est nécessaire aussi bien pour la fourniture, l'exportation et la simple utilisation de moyens de cryptographie permettant d'assurer des fonctions de confidentialité. La loi du 26 juillet 1996 a ajouté à cette liste l'importation de pays n'appartenant pas à la Communauté européenne et la précision sui-

[431] Category XIII (B) (1) of the Munitions List of ITAR, International Traffic In Arm Regulation, 22 CFR §§120-130. Sur le droit américain, voir l'étude préparée pour le gouvernement américain : "Review and analysis of US laws, regulations, and case laws pertaining to the use of commercial encryption products for voice and data communications", January 1994, disponible à : <ftp://ftp.wimsey.com/pub/crypto/Doc/laws>.

[432] ITAR, article 120.17.

[433] Article 28 de la loi du 29 décembre 1990, modifée par la loi n° 91-648 du 11 juillet 1991(JO du 13 juillet 1991).

[434] Voir supra

[435] Frédérique Olivier et Eric Barby, Des réseaux aux autoroutes de l'Information : Révolution technique ? Révolution Juridique ? 1- de l'utilisation des réseaux, JCP éd. E, I, 3926, n°17.

vante : « L'autorisation peut être subordonnée à l'obligation pour le fournisseur de communiquer l'identité de l'acquéreur ».

Les conditions dans lesquelles sont souscrites les déclarations et accordées les autorisations sont définies par décret. Les dossiers sont instruits par le Service central de la sécurité des systèmes d'information (SCSSI), service rattaché au Secrétaire général de la Défense nationale (SGDN).

Les critères des décisions de la SCSSI ne sont pas publics. En pratique, une demande d'autorisation déclenche une véritable enquête policière.

Les autorisations ne sont accordées qu'à certaines conditions : le système ne doit pas permettre à l'utilisateur de générer ses propres clés privées.

En outre, soit le SCSSI doit pouvoir être en mesure de casser, de déchiffrer, en cas de nécessité[436], soit un exemplaire des clés privées doit pouvoir être livré en cas de besoin ou être remises à l'administration[437].

La préparation et la défense d'un dossier de demande d'autorisation nécessite plusieurs semaines de travail d'un ingénieur qualifié.

Le décret du 28 décembre 1992[438] pris en application de la loi du 29 décembre 1990 précisait qu'un dossier en deux parties administratives et techniques était à fournir. La partie technique comportait une description complète du procédé de cryptographie, avec une description détaillée des fonctions et mécanismes de sécurité[439].

Les autorisations et déclarations préalables

Cette déclaration préalable doit être fournie pour la fourniture, l'importation d'un pays n'appartenant pas à la Communauté européenne et l'exportation de procédés qui ne permettent pas d'assurer des fonctions de confidentialité.

Il s'agit notamment des procédés qui permettent d'authentifier les communications ou d'assurer l'intégrité du message transmis, c'est-à-dire de générer des signatures électroniques. Rentrent dans cette catégorie les procédés de protection des mots de passe, codes d'accès et d'authentification, ainsi que les techniques de codage permettant de détecter les altérations portant atteinte à l'intégrité des données[440]. Cependant, les fonctionnalités de cryptage ne doivent pas permettre de chiffrer d'autres informations que les données nécessaires au contrôle d'accès, ni aucune autre information que celle nécessaire à l'authentification ou au contrôle d'intégrité des données elles-mêmes.

Or, les logiciels de cryptage permettent généralement d'assurer à la fois des fonctions de confidentialité et d'authentification.

Par exemple, un logiciel comme PGP peut être utilisé aux fins d'authentification, mais également pour chiffrer des données elles-mêmes.

La procédure de déclaration est également effectuée auprès du SCSSI.

La procédure de déclaration bien que qualifiée de « simple » par certains[441] ne consiste pas en une simple formalité administrative, type dépôt légal, mais suppose, un mois au moins avant la première livraison ou utilisation, le dépôt d'un dossier détaillé, avec une partie technique comportant une description complète du procédé de cryptographie et de son mode d'exploitation, y compris de la gestion des conventions secrètes[442].

---

[436] Stéphane Bortzmeyer, « Pour la libéralisation du chiffrement en France », *le Monde*, 27 janvier 1995.
[437] Jérôme Thorel, « Parcours du combattant pour un coffre-fort », *Planète Internet* n°8 mai 1996, p.40.
[438] Décret n° 92-1358, JO du 30 décembre 1992.
[439] Article 1er 2 b) de l'arrêté du 28 décembre 1992, JO du 30 décembre 1992.
[440] Voir article 2 de l'arrêté du 28 décembre 1992, préc.
[441] Chantal Arens, Le nouveau régime de la cryptologie, Juris-PTT 1993/2, p.22.
[442] décret n°92-1358 du 28 décembre 1992, titre 1er.

Certains considèrent que c'est par un abus de langage que l'on dit que le cryptage est interdit en France[443].

Il est exact que la cryptographie n'est pas à proprement parler interdite. Mais en pratique, certains logiciels, comme PGP, que vous pouvez vous procurez sur l'Internet et que l'on peut utiliser librement dans d'autres pays de l'Union européenne, n'obtiendront jamais l'autorisation du SCSSI. Vous pouvez toujours effectivement déposer un dossier de demande d'autorisation.

Même des industries de pointe qui souhaitent pouvoir communiquer de manière sécurisée avec leurs filiales étrangères seraient victimes de la position rigide du SCSSI.

Ainsi, PGP ne peut pas être utilisé, même pour authentifier une signature, au motif que le « logiciel PGP constitue un seul et même moyen de cryptologie, malgré les différentes options accessibles »[444].

Le régime de « liberté »

Désormais, l'utilisation de procédés de cryptographie à des fins d'authentification et d'intégrité est libre. Il y a toutefois une précision, importante : le procédé de cryptographie ne doit pas permettre d'assurer des fonctions de confidentialité.

En pratique, les logiciels de cryptographie devront être bridés. L'utilisation de PGP, même limitée aux fonctions de signature de ce logiciel reste exclue.

Les « tiers de confiance »

L'usage de la cryptographie pour assurer la confidentialité est libre, à condition que les conventions secrètes soient gérées selon les procédures et par un organisme agréé. L'instauration de ce que l'on appelle les « tiers de confiance » est la principale innovation de la loi.

Le tiers de confiance est un organisme auquel l'utilisateur confie sa clé privée de cryptage et qui en cas de nécessité remet ladite clé à l'autorité judiciaire ou à la police. Les Anglo-saxons désignent ce système sous le terme de « key-escrow » ou de « GAK » pour Government Access to Keys (Accès du gouvernement aux clés).

Dans le système imaginé par le législateur français, le tiers de confiance ne se limite pas à être le dépositaire des clés privées, il en assure la gestion pour le compte de l'utilisateur.

L'organisme passe un contrat avec l'utilisateur et lui transmet les clés à utiliser pour chiffrer son information. Le tiers de confiance devient le garant de la fiabilité des moyens de cryptographie utilisés.

L'utilisateur n'est donc pas autorisé à utiliser des logiciels qui lui permettent de générer lui-même sa clé privée.

Qui seront ces organismes ?

Ils devront être agréés par le Premier ministre.

L'agrément précise les moyens ou prestations qu'ils peuvent utiliser ou fournir, c'est-à-dire qu'en tout état de cause, seuls les logiciels de chiffrement qui auront reçu l'aval des services du gouvernement seront autorisés.

Un décret d'application précisera les conditions dans lesquelles ces organismes seront désignés ou agréés.

---

[443] Frédérique Olivier et Eric Barby, Des réseaux aux autoroutes de l'Information : Révolution Technique ? Révolution Juridique ? 1- de l'utilisation des réseaux, JCP éd. E, I, 3926, n°17.

[444] Stéphane Bortzmeyer, « Pour la libéralisation du chiffrement en France », *le Monde,* 27 janvier 1995.

Il semblerait néanmoins que les organismes qui assureront le rôle de ces tiers de confiance seront des sociétés privées ayant de bons rapports avec le ministère de la Défense. Le nom du Groupement des cartes bancaires a été également évoqué[445].

L'activité de tiers de confiance sera donc une activité commerciale, et l'utilisateur devra payer pour pouvoir obtenir le droit d'utiliser ce système.

Quel degré de confiance pourra-t-on accorder à une société commerciale pour respecter le secret médical, le secret professionnel des professions judiciaires comme les avocats, les secrets industriels ?

Le contrôle de la confidentialité échappe totalement à l'utilisateur et repose sur le tiers de confiance. En outre cette approche pose le problème de la responsabilité du tiers de confiance.

A la différence de logiciels développés à partir de systèmes connus comme RSA, les algorithmes des logiciels de chiffrement fournis par les tiers de confiance seront des algorithmes propriétaires, qui ne sont connus que du tiers de confiance (et évidemment du SCSSI). Il ne sera donc pas possible à des clients d'apprécier le degré de fiabilité du logiciel de cryptage, d'évaluer le risque qu'il soit cassé par un professionnel du chiffre.

Comment les tiers de confiance assureront la sécurité du système contre les intrusions extérieures et les faiblesses humaines ? Comment être sûr que vos clés ne seront pas remises à un concurrent qui fait de l'espionnage industriel par un employé indélicat ?

Comment prouver qu'il y a eu fraude ou défaillance ?

La communication des clés

Les conventions secrètes doivent être remises aux autorités judiciaires ou mises en œuvre selon leur demande, dans les cas prévus par la loi du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications[446](interceptions autorisées), et les enquêtes menées dans le cadre du régime prévu par le Code de procédure pénale[447].

La loi précise que « lorsque ces organismes remettent les conventions secrètes qu'ils gèrent dans le cadre des enquêtes menées (dans le cadre des dispositions du Code de procédure pénale), suite aux réquisitions du procureur de la République, ils informent les utilisateurs de cette remise ».

Cette disposition est un peu obscure.

Signifie-t-elle que l'utilisateur ne peut être averti que ses clés ont été remises aux autorités que dans le cas des enquêtes menées suite à une réquisition du procureur, ce qui exclut les cas où un officier de police judiciaire procède d'office à une enquête, ou que le tiers de confiance ne doit remettre ses clés que dans le cadre d'une enquête menée sous le régime du Code de procédure pénale sur réquisition du procureur ?

Cette réserve concernant les « demandes faites sur réquisition du procureur » ne figure pas dans l'alinéa précédent relatif aux cas dans lesquels le tiers de confiance remet ses clés aux autorités, ce qui semble exclure la seconde solution.

La loi du10 juillet 1991 a fixé un cadre précis aux interceptions de télécommunications[448]. Le dispositif ne devrait pas être détourné pour permettre à un officier de police judiciaire réalisant une enquête d'office, de se faire communiquer les clés par le tiers de confiance pour intercepter des communications, sans aucun contrôle d'un magistrat ou de la CNCIS (Commission nationale de contôle des interceptions de sécurité).

---

[445] Jérôme Thorel, « Les serruriers prennent forme », *Planète Internet*, n°10 juillet/ août 1996, p.16
[446] Voir supra,
[447] Articles 53 à 78.
[448] Voir supra

La remise des clés dans le cadre des dispositions du Code de procédure pénale devrait être réservée aux cas où les autorités judiciaires ont besoin de décrypter un fichier local et non des communications chiffrées. Cependant, on imagine mal le tiers de confiance, dont l'activité dépend de l'agrément de l'administration, refuser de coopérer avec les services de police et de leur donner les clés dès que cette dernière invoquera les besoins d'une enquête.

Les formalités simplifiées

Le décret qui fixera les conditions dans lesquelles sont souscrites les déclarations et accordées les autorisations prévoira :

a) un régime simplifié de déclaration ou d'autorisation pour certains types de moyens ou de prestations ou pour certaines catégories d'utilisateurs. Cette disposition pourrait concerner par exemple les banques qui bénéficient déjà d'autorisations pour assurer la sécurité de leurs transactions financières, ou encore les services de l'Etat comme l'armée ou la police ;

b) la substitution de la déclaration à l'autorisation pour les opérations portant sur des moyens ou des prestations de cryptologie, dont les caractéristiques techniques ou les conditions d'utilisation, tout en justifiant, au regard des intérêts susmentionnés, un suivi particulier, n'exigent pas l'autorisation préalable de ces opérations ;

c) la dispense de toute formalité préalable pour les opérations portant sur des moyens ou des prestations de cryptologie, dont les caractéristique techniques ou les conditions d'utilisation sont telles que ces opérations ne sont pas susceptibles de porter atteinte aux intérêts mentionnés au deuxième alinéa.

Les intérêts auxquels ces textes font référence sont les intérêts de la Défense nationale et de la sécurité intérieure et extérieure de l'Etat.

Il sera intéressant de connaître les procédés de cryptographie « dont les caractéristiques techniques ou les conditions d'utilisation sont telles que ces opérations ne sont pas susceptibles de porter atteinte aux intérêts » précités, c'est-à-dire les procédés de chiffrement aisément cassables par les services de renseignement français.

Les sanctions

Outre l'application du Code des douanes, le fait de fournir, d'importer de pays n'appartenant pas à la Communauté européenne ou d'exporter un moyen ou une prestation de cryptologie sans autorisation préalable ou en dehors des conditions de l'autorisation est puni de 6 mois d'emprisonnement et de 200 000 francs d'amende.

Les peines sont aggravées par loi du 26 juillet 1996 puisque les peines de prison encourues passent de 3 à 6 mois et que l'importation d'un pays n'appartenant pas à la Communauté européenne est désormais passible de sanctions pénales, ce qui n'était pas le cas auparavant.

Cette nouvelle incrimination ne va pas manquer de poser certains problèmes d'application. On peut télécharger sur l'Internet des logiciels incorporant des fonctionnalités de cryptage qui n'ont pas été autorisés en France, mais qui peuvent être utilisés et fournis dans d'autres pays. Or les sites qui proposent ces logiciels peuvent être indifféremment situés dans des pays de l'Union européenne, comme la Suède, ou dans des pays n'appartenant pas à l'Union, comme la Norvège.

En pratique, rien ne distinguera le logiciel téléchargé d'un site norvégien de celui téléchargé d'un site suédois.

Les douanes vont-elles contrôler les ordinateurs portables des citoyens étrangers non résidents de la Communauté en voyage d'affaires ou touristique pour vérifier qu'ils ne comportent pas de logiciel incorporant des procédés de chiffrement non autorisés en France, comme certaines versions de Netscape ? C'est évidemment irréaliste.

Le simple usage de procédés de cryptographie sans autorisation devrait comme par le passé être passible d'une contravention qui serait fixée par les décrets d'application.

Les autres sanctions

La loi crée également le délit d'exercice illégal d'une activité de tiers de confiance :

« Le fait de gérer, pour le compte d'autrui, des conventions secrètes de moyens ou de prestations de cryptologie permettant d'assurer des fonctions de confidentialité sans avoir obtenu l'agrément est puni de 2 ans d'emprisonnement et de 300 000 francs d'amende ».

Enfin, « le fait de fournir, d'importer de pays n'appartenant pas à la Communauté européenne, d'exporter un moyen ou une prestation de cryptologie en vue de faciliter la préparation ou la commission d'un crime ou d'un délit est puni de 3 ans d'emprisonnement et de 500 000 francs d'amende ».

Quelle responsabilité encourt le tiers de confiance qui transmettrait une clé privée à un tiers non autorisé ?

Le texte prévoit que le tiers de confiance est soumis au secret professionnel. Les dispositions de l'article 226-13 du Code pénal qui précisent que « la révélation d'une information à caractère secret par une personne qui en est dépositaire soit par Etat ou par profession, soit en raison d'une fonction ou d'une mission temporaire, est punie d'un an d'emprisonnement et de 100 000 francs d'amende », pourront donc être invoquées.

En revanche, l'article 432-9 sur l'atteinte au secret des correspondances qui punit de 3 ans d'emprisonnement le fait par une personne dépositaire de l'autorité publique, l'exploitant d'un réseau de télécommunications ou le fournisseur d'un service de télécommunications, agissant dans l'exercice de ses fonctions d'« ordonner, de commettre ou de faciliter, hors les cas prévus par la loi, l'interception ou le détournement des correspondances », ne semble pas applicable, sauf à considérer que le tiers de confiance est dépositaire de l'autorité publique ou chargé d'une mission de service public.

On voit en comparant ces deux dispositions que la question du risque de divulgation des clés privées ou d'un usage frauduleux par le tiers de confiance n'a pas été prise en considération.

Le fournisseur d'accès encourt des peines plus graves (s'il facilite l'interception de correspondances) que le tiers de confiance qui divulgue une clé qu'il gère pour le compte d'un client.

Malgré les allégements annoncés, la cryptographie reste en France très sévèrement réglementée. Les peines sont aggravées et de nouvelles infractions sont créées.

Quant aux deux cas où l'on est « libre » d'utiliser des procédés de cryptographie, ils ne doivent pas faire illusion, il s'agit d'une liberté très encadrée.

Pour l'authentification, des logiciels spécialement bridés devront être développés pour les utilisateurs français. Pour prendre une analogie, c'est comme si on demandait aux constructeurs d'automobiles de faire une voiture qui ne dépasserait pas 50km/heure ou ne roulerait pas plus de 100 km, uniquement pour la France.

Les tiers de confiance sont une institution artificielle qui ne correspond à aucune nécessité technique. Il s'agit d'un système lourd qui va entraîner formalités et coûts pour les entreprises ou personnes qui voudraient l'utiliser tout en n'étant pas satisfaisant.

Il ne faut pas confondre les tiers de confiance avec les tiers certificateurs. Le tiers de confiance est celui qui est dépositaire ou qui gère des clés privées de cryptage, celles qui permettent d'assurer la confidentialité et l'authentification des données. Le tiers certificateur est dépositaire de la clé publique, celle qui sert aux correspondants pour crypter les messages qui vous sont adressés (confidentialité) ou décrypter un message crypté avec la clé privé(fonction de signature).

Le réseau de tiers certificateur ou de « notaire électronique » permet de certifier l'identité et les pouvoirs de la personne à qui appartient une clé publique. Son existence est le corollaire du système de la crytographie asymétrique et il apparaît souhaitable pour le développement des échanges dématérialisés de mettre en place un réseau de tiers certificateur.

En revanche, la clé privée reste en possession de l'utilisateur.

La cryptographie n'est plus réservée aux seuls militaires, ses applications civiles sont aujourd'hui indispensables au développement des réseaux. L'article 28 modifié de la loi fait lui-même référence à « la protection des informations et le développement des communications et des transactions sécurisées ».

Quelles sont les raisons invoquées par les Etats en général et le gouvernement français en particulier pour justifier de leurs craintes vis-à-vis des systèmes de chiffrement ?

La justification de la réglementation

Il ne s'agit pas moins que de « préserver les intérêts de la Défense nationale et de la sécurité intérieure ou extérieure de l'Etat » (article 28 alinéa 2 de la loi).

Pour les Etats, une protection trop forte de l'information porte atteinte à leur sécurité et profite au crime organisé. Les procédés de cryptage inviolables peuvent entraver l'application de la loi, être utilisés par des gouvernements ou d'autres organisations hostiles pour cacher des informations subversives et constituent à ce titre une menace potentielle pour l'ordre public et la sécurité nationale[449].

L'Etat invoque le fait qu'il doit avoir accès à certains types d'informations pour pouvoir contrer les réseaux terroristes, la mafia, les narco-trafiquants, le blanchiment de l'argent sale et d'autres types d'activités illégales[450].

Pour le Français Joël de Rosnay, « il n'est pas concevable qu'une personne privée dispose de moyens quasi-militaires »[451] et pour l'Américain James Kallstrom, agent du FBI, « nous ne voulons pas créer de sanctuaire pour les criminels » ou encore « un cryptage inviolable aurait pour seul effet d'assurer l'impunité aux criminels »[452].

Témoigne de cette défiance des Etats vis-à-vis de la cryptographie le point V (Use of Encryption) de la recommandation du 11 septembre 1995 du Comité du conseil de l'Europe relative aux problèmes de procédure pénale liés à la technologie de l'information :

« Des mesures pour minimiser les effets négatifs de l'utilisation de la cryptographie dans l'investigation des crimes et délits doivent être envisagées, sans préjudicier à son usage légitime plus qu'il n'est nécessaire »[453].

Les Etats craindraient-ils que ne se réalisent les prédictions des « crypto-anarchistes », militants purs et durs d'une généralisation et d'une liberté totale de la cryptographie ?

« La technologie informatique est sur le point de fournir aux individus et aux groupes la possibilité de communiquer et d'interagir les uns avec les autres d'une manière totalement anonyme (…)

Ces développements vont complètement modifier la nature de la réglementation étatique, la possibilité de taxer et de contrôler les interactions économiques, la possibilité de garder l'information secrète, et affectera même la notion de confiance et de réputation (…)

[449] Livre vert de la Commission européenne, La sécurité des systèmes d'information, DG XIII 4/1994, points 4.2.5.1 et 5.1.3.
[450] Jean Guisnel, Guerres dans le cyberespace, éditions la Découverte, p. 31 et s. 69 et s.
[451] Joël de Rosnay, « Non au codage invulnérable sur l'Internet », *Libération*, 31 mars 1995.
[452] Entretien croisé avec Phil Zimmerman, « Vie privée, vie cryptée », *Libération*, cahier multimédia, 23 février 1996.
[453] Recommandation n°R(95) 13, disponible à : <http://www2.echo.lu/legal/en/crime/crime.html>.

Bien évidemment, l'Etat cherchera à ralentir ou à stopper la diffusion de cette technologie, invoquant les impératifs de sécurité nationale, l'utilisation de la technologie par les trafiquants de drogue et la fraude fiscale, et la crainte de la désintégration sociale. Nombre de ces inquiétudes seront fondées ; la crypto-anarchie permettra le libre commerce de secrets nationaux et la commercialisation de produits illicites et volés. Un marché informatique anonyme rendra même possible l'émergence de marchés exécrables d'assassinats et d'extorsions. Divers éléments criminels et étrangers seront des utilisateurs actifs du CryptoNet. Mais cela n'empêchera pas la progression de la crypto-anarchie.[454] »

Cette position est évidemment extrémiste. Mais la mafia, les trafiquants de drogue ou d'armes, les espions, les fraudeurs du fisc n'ont pas attendu la cryptographie pour prospérer.

A côté de la lutte contre la mafia, la drogue, le terrorisme, la petite et moyenne délinquance est également au cœur des préoccupations gouvernementales. L'usage de la cryptographie peut empêcher l'application de la loi et la réalisation des interceptions légales.

Le développement des réseaux informatiques voit émerger de nouvelles préoccupations : la sécurité informatique, la protection des données, la preuve. La cryptographie, même si elle n'est pas la solution à tous ces problèmes en représente néanmoins un pivot essentiel et indispensable.

Critique de la réglementation

L'utilisation de la cryptographie par le crime organisé

Il s'agit de l'argument majeur invoqué pour fonder les restrictions apportées ou envisagées à la cryptographie. Or, il serait naïf de croire que l'on peut empêcher le crime organisé de se procurer les solutions de cryptage existantes ou de développer des mécanismes propres.

Il existe une contradiction manifeste dans la loi française entre les peines encourues pour la fourniture de procédés de cryptologie non autorisée (jusqu'à 6 mois de prison) et les objectifs annoncés de préservation de la sécurité intérieure ou extérieure de l'Etat. Les terroristes et autres trafiquants encourent des peines autrement plus graves, et ne seront pas dissuadés, quelle que soit la réglementation adoptée, de se procurer des moyens de crypter, y compris par les méthodes dites « traditionnelles ». La nouvelle infraction créée par la loi lorsque les procédés de cryptage sont utilisés, fournis, importés ou exportés en vue de faciliter la préparation ou la commission d'un crime ou d'un délit avec une peine pouvant aller jusqu'à 3 ans de prison ne change pas le raisonnement pour des criminels qui risquent des peines beaucoup plus longues.

« Une législation restrictive a des conséquences plus fortes sur l'utilisateur respectueux de la loi que sur les autres »[455].

Concernant les tiers de confiance, « Imagine-t-on sérieusement que la mafia ou un réseau de pédophilie utilisera un logiciel de cryptage fourni par un "centre de confiance" ? Le système projeté risque bien de n'être mis en œuvre que par des citoyens honnêtes, dont les autorités n'auront justement jamais besoin de décrypter les messages »[456].

---

[454] extraits de "The Crypto Anarchist Manifesto" par Timothy C.May disponible à : <http://www.quadralay.com/Crypto/crypto-anarchist.html > ; sur le sujet voir : Jean Guisnel, Guerres dans le cyberespace, éditions la Découverte, p.57.

[455] Livre vert, préc., point 4.2.5.2 p.53

[456] Paul Vidonne, « Pour une vraie liberté de crypter », *le Monde*, 15 mai 1996.

Pour le cryptographe Ross Anderson, les criminels utilisent plutôt la stéganographie pour camoufler leurs messages[457].

L'argument tiré de la grande criminalité organisée n'est pas convaincant. Il peut justifier des restrictions à l'exportation, ou concernant des procédés utilisés à des fins militaires, mais pas une législation unique dans les pays occidentaux qui soumet même l'utilisation de la cryptographie à des fins privées, légitimes et internes soit à une autorisation préalable, soit à une obligation de passer par des tiers de confiance.

Pour la CCI, « la limitation de l'utilisation du chiffrement pour cette raison est sujette à caution, car les auteurs d'actes délictueux ne se sentiront pas obligés de se plier aux règlements applicables à la communauté économique »[458].

Un autre problème est qu'un code cassable par les services gouvernementaux est également cassable par les services secrets étrangers, les organisations criminelles, les espions industriels ou encore les pirates informatiques. Ainsi, un message crypté avec la version à 40 bits du logiciel serveur de Netscape, seule version autorisée à l'exportation des Etats-Unis et à la fourniture en France, a été cassé en une semaine par un informaticien français, Damien Doligez.

Pour Jean Guisnel, « les services secrets avaient pris l'habitude, depuis des années, de violer l'intimité des citoyens sans même en demander l'autorisation au pouvoir judiciaire. Les pédophiles et autres narco-trafiquants ont bon dos : c'est la société entière que ces agences veulent pouvoir contrôler »[459].

Le cauchemar décrit dans le livre, *1984,* de Georges Orwell, serait-il déjà une réalité ? :

« Naturellement, il n'y avait pas de moyen de savoir si, à un moment donné on était surveillé. Combien de fois, et suivant quel plan, la police de la pensée se branchait-elle sur une ligne individuelle quelconque, personne ne pouvait le savoir. On pouvait même imaginer qu'elle surveillait tout le monde, constamment. Mais de toute façon elle pouvait mettre une prise sur votre ligne chaque fois qu'elle le désirait »[460].

L'Etat est donc soucieux de se préserver la possibilité d'« écouter » ce qui se passe sur les réseaux.

Cependant, les bénéfices que l'on peut tirer d'un usage plus généralisé de la cryptographie sont supérieurs aux inconvénients que cet usage peut générer[461].

L'exception française

Cette constatation revient comme un leitmotiv dans toutes les études sur la cryptographie : la France possède la législation la plus restrictive sur le sujet des pays de l'Union européenne et des pays occidentaux en général. Dans certains pays comme le Danemark, l'Autriche, la Finlande, il n'existe aucune législation spécifique à la cryptographie qui est donc utilisée librement. Beaucoup de pays parmi lesquels on peut citer les Etats-Unis, le Canada, l'Allemagne, la Grande-Bretagne, la Hollande, L'Espagne, la Suède ont des règles restreignant la libre exportation des procédés de cryptographie, mais leur usage interne est libre[462].

---

[457] Intervention à la conférence du 25 septembre 1995 sur la cryptographie organisée par l'EPIC, voir : <http://www.netpress.fr/crypto/>.

[458] Prise de position de la CCI sur une politique internationale du chiffrement, Droit de l'Informatique et des télécoms 1994/2 p.70.

[459] Préc., p.32.

[460] Extrait de *1984,* éditions Gallimard pour la traduction de l'anglais.

[461] Cryptography's Role in Securing the Information Society, Rapport du National Research Council, 30 mai 1996, disponible à : <http://www2.nas.edu/cstbweb>.

[462] Bert-Jaap Koops, Crypto Law Survey, Université de Tilburg et Eindhoven, Pays-Bas, <http://cwis.kub.nl/~frw/people/koops/lawsurvy.htm>, Sept. 1996 ; Sylvain André,Data encryption and the Law, <http://www.cnam.fr/Network/Crypto/survey.html>, décembre 1994 ; Identification and analysis of foreign laws and regulations pertaining to the use of commercial encrytion products for voice and data communications, January 1994, une étude préparée pour le gouvernement américain, disponible à : <ftp://ftp.wimsey.com/pub/crypto/Doc/laws>.

Seule la Belgique connaîtrait une réglementation applicable à l'utilisation de la cryptographie, d'après une loi du 21 décembre 1994[463].

On relèvera que certains des pays ne réglementant pas l'usage interne de la cryptographie sont confrontés au problème du terrorisme. Il ne semble pas que la possibilité d'user la cryptographie a induit un taux de criminalité plus élevé qu'ailleurs.

Le développement des réseaux informatiques va de pair avec la nécessité de pouvoir communiquer de manière sécurisée et confidentielle. En matière de commerce électronique, des standards internationaux vont émerger et seront *de facto* adoptés par la majorité des utilisateurs[464]. La France risque de se retrouver à l'écart du mouvement et des innovations en cours et du flux des affaires.

La lourdeur de la procédure française, le risque que les autorisations nécessaires soient refusées ou trop longues à obtenir, la nécessité aujourd'hui d'assurer des fonctions de tiers de confiance si une entreprise veut pouvoir fournir des logiciels de chiffrement, ne peut qu'entraver l'investissement des entreprises françaises dans ce secteur pourtant vital, entreprises qui se tourneront ensuite logiquement vers les produits disponibles des entreprises étrangères.

Les entreprises américaines, qui ont déjà l'avantage de bénéficier d'une législation interne beaucoup plus favorable qu'en France, font actuellement pression auprès du gouvernement pour obtenir un assouplissement des règles à l'exportation des produits de cryptographie. Le motif invoqué est que cela gêne la compétitivité des entreprises américaines. Or, les produits américains représenteraient déjà 75% des produits disponibles sur le marché mondial du logiciel selon le département du commerce américain[465]. Concernant le marché du logiciel de sécurité, la compétition avec les entreprises de l'Europe de l'ouest serait plus serrée. Déjà, les règles de l'ITAR ont été récemment assouplies pour permettre aux Américains de voyager, sous certaines conditions, avec des produits de cryptographie[466].

Les initiatives en vue d'obtenir d'autres assouplissements se multiplient : plusieurs projets de lois ont été déposés en ce sens, comme le « Promotion of Commerce On-Line in the Digital Era (pro-Code) Act du sénateur Conrad Burns[467] ou le projet du sénateur Patrick Leahy qui prévoit la diminution des contrôles à l'exportation en transférant le pouvoir d'autoriser les exportations du NSA au ministère du Commerce et une levée des contrôles concernant les logiciels de cryptage « généralement disponibles »[468]. Le National Research Council a rendu public le 30 mai 1996, un rapport sur la politique américaine en matière de cryptographie qui recommande que les contrôles à l'exportation soient allégés sans être totalement éliminés[469].

Même si les règles à l'exportation américaines sont modifiées, la France ne sera pas obligée d'autoriser l'importation desdits produits, au risque de maintenir et d'aggraver son retard en ce qui concerne l'Internet.

Les dernières versions des logiciels de Netscape et de Microsoft intègrent des fonctions de cryptage qui permettent notamment de mettre en place des procédures de paiement sécurisées.

Aujourd'hui, pour mettre en place un serveur de paiement sécurisé avec ces logiciels, il faut une autorisation. Cette autorisation restera nécessaire demain puisqu'il ne s'agit pas de logiciels gérés par les tiers de confiance sauf s'ils rentrent dans les catégories à déclaration simplifiées qui seront définies par décret. Lorsque les sociétés américaines obtiendront

---

[463] O. Hance, Business et Droit d'Internet, Best Of Editions 1996, p. 175.

[464] Toward Enabling Secure Electronic Commerce : The need for a revised US cryptographic policy, by CommerceNet Network Services Working Group, <http://www.commerce.net >.

[465] A study of the International market for computer software with encryption, redacted copy prepared by the US Department of Commerce and The National Security Agency, disponible à :<http://www.epic.org/crypto>.

[466] Federal Register Notice (61FR6111) du 16 février 1996, Bureau of Political Military Affairs 22 CFR Parts 123 et 126, disponible à : <http://washofc.epic.org/crypto/export_controls/personal.html>.

[467] Disponible à : <http://washofc.epic.org/crypto/legislation/pro_code.html>.

[468] Disponible à :<http://www.epic.org/crypto/export_controls/>.

[469] Cryptography's Role in Securing the Information Society, disponible à : <http://www2.nas.edu/cstbweb>.

l'autorisation d'exporter des logiciels intégrant des fonctions de cryptage avec des clés plus longues, donc plus sûres, pourra-t-on réellement continuer à empêcher l'utilisation de ces logiciels en France ?

La position adoptée par le gouvernement en la matière entrave, dans un secteur clé, la créativité des entreprises françaises. En outre, cette réglementation fait peser sur les entreprises une charge qui n'existe pas chez nos partenaires européens, et donc constitue une distorsion de la concurrence en leur défaveur. Les entreprises françaises ont également besoin de la cryptographie pour se protéger des pirates et de l'espionnage industriel. La préservation de la sécurité intérieure ne rimerait donc pas toujours avec préservation des intérêts nationaux.

Les tiers de défiance

La France est le premier pays du monde a avoir adopté une loi prévoyant la mise en place d'un système de tiers de confiance.

Pourtant ce système n'est pas une solution satisfaisante.

Toute la sécurité des procédés de cryptographie modernes repose sur la clé secrète. Cette clé devrait donc être conservée dans un environnement sécurisé. L'idée même de déposer sa clé chez un tiers est antinomique avec la conception de la méthode à clé asymétrique.

Le système prévu par la loi ne garantit aucunement contre les interceptions abusives qui pourraient être effectuées par l'administration. Il ne garantit pas non plus la sécurité des données contre l'espionnage industriel, les indiscrétions de tout ordre d'origine humaine.

Comment les clés privées sont-elles transmises à l'utilisateur ? Toute la technique de la cryptographie double clé a justement été imaginée pour résoudre les problèmes liés à la communication des clés.

En résumé, peut-on faire reposer la confidentialité et la protection des données sur un tiers que l'on ne contrôle pas ?

Plusieurs Etats, dont le Danemark, les Pays-Bas, l'Allemagne avaient envisagé des projets de loi prévoyant la mise en place de tels systèmes. Le projet hollandais a notamment été très critiqué[470].

La Commission européenne envisage également de créer des services européens de tiers de confiance et a mis en place un groupe de travail d'experts, le Senior Officers Group for Information System Security (SOG-IS).

Aux Etats-Unis, le gouvernement a tenté d'imposer un système de tiers de confiance, dans lequel il aurait fourni les procédés de cryptographie. Ce projet connu sous le nom de « Clipper Chip »[471] a donné lieu à une levée de boucliers et a dû être abandonné.

L'administration américaine n'a néanmoins pas abandonné son idée de « key-escrow » et d'autres projets sont à l'étude.

Aussi bien les organisations de défense des libertés sur les réseaux comme l'AUI (Association des utilisateurs d'Internet), l'EFF (Electronic Frontier Fondation) ou l'EPIC (Electronic Privacy Information Center), que l'IAB (Internet Architecture Board), l'IESG (Internet Engineering Steering Group)[472] que les entreprises[473] sont hostiles à tous ces projets de « key-escrow ».

---

[470] O. Hance, Business et Droit d'Internet, Best Of Editions 1996, p. 175.

[471] Sur le "Clipper Chip" voir les archives de l'EFF <http://www.eff.org/> et de l'Epic <http://www.epic.org/crypto/> ; EFF Statement on and Analysis of Digital Telephony Act, <http://www.eff.org/pub/Privacy/Digital_Telephony_FBI/digtel94_passage_statement.eff>, October 8, 1994 ; USA, Statement of the US council for international business on liabilities issues and the US administrations's encryption initiatives, November 2, 1994, Droit de l'Informatique et des Télécoms, 1994/4 p.99.

[472] IAB and IESG statement on cryptography technology and the Internet, 24 juillet 1996.

[473] Toward Enabling Secure Electronic Commerce : The need for a revised US cryptographic policy, by CommerceNet Network Services Working Group, <http://www.commerce.net>.

Le rapport du National Research Council préconise quant à lui l'absence de restriction sur l'usage de la cryptographie à l'intérieur des Etats-Unis, au motif que l'obligation d'utiliser des procédés de cryptage avec tiers de confiance soulève des questions d'ordre technique et constitutionnel[474].

Les échanges internationaux

Le système des tiers de confiance est en outre inadapté aux échanges internationaux. Un réseau de tiers de confiance ne peut être que national. La mise en place d'un réseau international ou même seulement européen de tiers de confiance n'est pas réaliste. L'existence des tiers de confiance est justifiée par des impératifs de sécurité nationale et de Défense, un domaine où précisément les Etats refuseront d'abandonner toute parcelle de souveraineté nationale.

La loi française précise que les organismes « doivent exercer leurs activités agréées sur le territoire national ».

Dès lors comment peut-on communiquer avec des correspondants étrangers avec un tel procédé ?

Les deux correspondants doivent utiliser le même logiciel de chiffrement ou des logiciels compatibles. Les logiciels de chiffrement devront donc au préalable être vendus à l'étranger. On voit mal pourquoi les particuliers et surtout les entreprises étrangères se rendraient acquéreurs d'un système qui sera soupçonné d'avoir été affaibli par les services du renseignement français. On les imagine encore moins demander à des entreprises étrangères, dont l'activité en matière de chiffrement sera contrôlée par le gouvernement français, de leur fournir leurs clés privées de chiffrement.

Il apparaît indispensable qu'un équilibre puisse être trouvé entre les intérêts des gouvernements qui doivent assurer le maintien de la sécurité et de l'ordre public et les intérêts privés des entreprises et des utilisateurs qui ont besoin de disposer de systèmes de cryptage sûrs, faciles d'accès et abordables.

Des réflexions doivent être engagées pour explorer d'autres solutions que celle du tiers de confiance. Par exemple l'obligation de communiquer les systèmes et clés de cryptage à la requête de l'autorité judiciaire[475], faire de l'usage de la cryptographie en vue de dissimuler un crime ou un délit une circonstance aggravante (c'est un délit autonome dans la loi). L'article 434-4 du Code pénal punit déjà d'une peine de 3 ans d'emprisonnement et de 300 000 francs d'amende, le fait, en vue de faire obstacle à la manifestation de la vérité, c'est-à-dire en vue de faire obstacle à l'action de la justice, « de détruire, soustraire, receler ou altérer un document public ou privé ou un objet de nature à faciliter la découverte d'un crime ou d'un délit, la recherche des preuves ou la condamnation des coupables ».

On ne peut pas fonder une loi sur le postulat que tous les citoyens sont des délinquants en puissance, en invoquant la lutte contre les grands criminels et les terroristes, alors que, quel que soit le système adopté, il ne sera pas respecté par ces derniers. En attendant qu'une solution satisfaisante puisse éventuellement être trouvée au niveau européen et international, le régime de la cryptographie en France doit être assoupli de manière significative et la liberté de crypter avec le moyen de son choix reconnu à l'utilisateur.

Si les entreprises et les usagers des réseaux réclament le droit de crypter, ce n'est pas dans le but de frauder le fisc, ou de se lancer dans le trafic de drogue, c'est pour pouvoir assurer la

[474] Cryptography's Role in Securing the Information Society, recommandation n°1, disponible à : <http://www2.nas.edu/cstbweb>.
[475] Paul Vidonne, « Pour une vraie liberté de crypter », *le Monde,* 15 mai 1996.

sécurité de l’information qui circule, quelle qu'en soit la nature, et donc se protéger contre les malveillances et les indiscrétions qui pourraient être commises par de vrais délinquants.

Le commerce électronique

Les entreprises ne pouvaient se désintéresser de ce formidable outil de développement des échanges que représente l'Internet. L'ouverture de l'Internet au grand public, sa croissance extraordinaire, le développement du World Wide Web qui permet la mise en place d'applications multimédia ont joué un rôle de catalyseur.

Le commerce sur l'Internet est déjà une réalité. De plus en plus d'entreprises offrent leurs produits à la vente directe sur l'Internet. Les meilleures ventes sont réalisées par les CD-Rom, les CD-Audio, les livres et le matériel informatique. La mise en place d'un serveur Web devient un outil de marketing.

Selon une étude réalisée par Médiangles, et publiée en mai 1996, au cours des 6 derniers mois, 17% des utilisateurs ont effectivement réalisé une transaction électronique pour un montant moyen de 1 630 F. La majorité serait prête à effectuer leurs réservations, leurs opérations bancaires ou commandes de produits sur l'Internet[476].

En Asie également, le commerce électronique sur l'Internet suscite l'engouement. En juillet 1996, une société de Hong-Kong, Telecom IMS'Netvigator service annonçait le lancement du premier supermarché virtuel en ligne[477].

Le commerce électronique ne suppose pas nécessairement un échange en temps réel et une interactivité. Des partenaires, au lieu de communiquer par les moyens traditionnels, utilisent le courrier électronique. Il s'agit en pratique d'un usage très répandu dans certaines branches professionnelles. Or, le courrier électronique n'est pas interactif, les échanges se font en temps différé. Un contrat conclu par courrier électronique est pourtant bien une manifestation du commerce électronique.

Si l'on se connecte sur le service d'une entreprise qui n'est pas en accès libre et qui nécessite un abonnement ou un paiement, l'envoi préalable d'un mot de passe et d'un identifiant est effectué par télécopie ou par courrier électronique. Une commande de produit sur un serveur Web fait généralement l'objet d'une confirmation par courrier électronique.

La commande de billets de trains sur Minitel est une forme de commerce électronique bien que l'on n'ait pas recours à un réseau international de télécommunications[478].

Pour les Américains, inventeurs du concept[479], le commerce électronique c'est l'utilisation de toutes les technologies de l'information pour développer le commerce des entreprises, le passage de l'utilisation d'applications informatiques coûteuses et sophistiquées pour les échanges par un petit nombre d'entreprises à l'utilisation de nouvelles techniques de com-

[476] « Quand Médiangles s'empêtre dans le comptage des internautes français », *Planète Internet* n° 9 juin 1996, p.13.
[477] South China Morning Post, Cahier Cybertech, 19 juillet 1996, p.1.
[478] « La France à l'avant-garde du commerce électronique », *le Monde*, supplément multimédia, 30 septembre 1995, p.VII.
[479] Thierry Piette-Coudol, Convention cadre pour le commerce électronique, Cybernews, Volume II n°II, Hiver 1996, <http://www.droit.umontreal.ca/CRDP/Cybernews/>.

munication par les petites et moyennes entreprises. Le commerce électronique inclut également la collecte et le tri d'une masse toujours plus grande d'informations. Dans ce deuxième aspect, le commerce électronique se définit par rapport à l'objet sur lequel il porte : le bien immatériel[480].

Le commerce électronique diffère du commerce traditionnel par la manière dont l'information est échangée et traitée. Il y a une modification du support de l'échange, mais pas de la nature juridique du rapport qui reste un contrat.

Ce contrat du commerce électronique est un type de contrat à distance, entre partenaires qui ne sont pas en présence simultanée l'un de l'autre.

Une proposition de directive de la Commission européenne sur la protection des consommateurs en matière de contrats négociés à distance[481] définit le contrat négocié à distance comme :

« Tout contrat concernant un produit ou un service conclu après sollicitation par le fournisseur sans présence physique simultanée du fournisseur et du consommateur et en utilisant une technique de communication à distance pour la transmission de la sollicitation de contracter et de la commande. »

Selon l'article 14 de l'arrêté du 3 décembre 1987 relatif à l'information du consommateur sur les prix :

« Constitue une technique de communication à distance (…) toute technique permettant au consommateur, hors des lieux habituels de réception de la clientèle, de commander un produit ou de demander la réalisation d'un service. Sont notamment considérés comme technique de communication à distance la télématique, le téléphone, la vidéotransmission, la voie postale et la distribution d'imprimés. »

La proposition de directive inclut dans les techniques de communication à distance le visiophone, le vidéotexte, le courrier électronique, le télécopieur, la télévision.

Le juriste n'est pas projeté de l'ère du contrat écrit entre personnes présentes à l'ère du contrat immatériel à distance. L'évolution des techniques de commercialisation s'est faite progressivement, et certaines questions soulevées par le commerce électronique comme le problème de la preuve, sont déjà débattues par les juristes depuis des années.

Traditionnellement, un échange s'effectue par un contrat direct et personnel. La présence simultanée des deux contractants est la base de l'engagement.

Il est des hypothèses où ce contact direct et personnel n'existe pas : recours à un mandataire, contrats qualifiés de contrats entre absents dont le cas le plus fréquent est le contrat par correspondance.

Du fait de l'absence de contact direct et simultané dans le contrat par correspondance, certaines questions juridiques n'ont pas manqué de se poser : identification du cocontractant, moment et lieu de formation du contrat.

Le développement des techniques de commercialisation à distance a également contribué à l'émergence d'un régime spécifique d'information et de protection des consommateurs ainsi sollicités.

Le contrat par correspondance faisait classiquement appel aux échanges par voie postale.

Avec l'apparition du Minitel et l'utilisation des nouveaux médias, une deuxième donnée vient se superposer à la problématique du contrat entre absents : l'absence du support papier. Cela concerne d'abord l'offre du commerçant, puis la commande.

---

[480] Putting the Information Infrastructure to Work : A Report of the Information Infrastructure Task Force's Committee on Applications and Technology, Electronic Commerce and the NII, Draft for public comment, 1994, disponible à : <http://iitfcat.nist.gov:94/doc/Electronic_Commerce.html>.

[481] Proposition n°92/C 156/5, JOCE n° C 156/4 du 23 juin 1992.

L'étape suivante est le recours à un système de paiement électronique. Le paiement s'effectue par des moyens classiques comme le chèque, puis l'usage de la carte de crédit se développe. La télétransmission de factures fait son apparition, puis aujourd'hui le porte-monnaie électronique.

Avec l'Internet, les techniques de communication à distance sont utilisées au maximum de leur potentialités et la transaction peut être entièrement dématérialisée jusque dans son processus de livraison.

C'est déjà le cas pour les logiciels que l'on peut se procurer sur l'Internet par téléchargement sans recours au moindre support matériel. Sont évidemment concernés par cette dématérialisation totale tous les biens immatériels.

Les livres à télécharger font leur apparition, des journaux électroniques se créent, de la musique peut être diffusée sous forme de fichiers informatiques.

Les techniques et les matériels actuels ne permettent pas encore de télécharger des films entiers. Mais ce n'est qu'une question de temps avant que de telles possibilités relèvent de la réalité. Demain, les progrès techniques devraient permettre le perfectionnement de ces techniques, l'amélioration du confort d'écoute, de lecture ou de visualisation, et leur banalisation.

On passe d'un support papier à un support électronique, mais les questions juridiques soulevées par le contrat à distance restent identiques : formation du contrat entre absents, lois spécifiques en droit de la consommation. Ces questions seront examinées dans une première partie : « Le contrat à distance ».

Le fait que le contrat électronique se forme, se paie, voire s'exécute sans support matériel pose un problème majeur au niveau de la preuve, dans un système juridique marqué par la prééminence de l'écrit. Ce sera le thème de la deuxième partie : « Remplacer l'écrit : aspects juridiques ».

L'Internet est un réseau ouvert et non sécurisé. De nombreuses solutions sont en cours de mise en place actuellement en vue de proposer des systèmes de paiement sécurisés. J'examinerai ces techniques dans une troisième partie : « Le paiement électronique ».

L'Internet étant un réseau mondial, se posent également des questions de droit international qui seront analysées dans le chapitre suivant. Parmi les aspects internationaux figure la question de la TVA. Je donnerai un aperçu de la question fiscale dans la dernière partie : « TVA et commerce électronique ».

Première partie

Le contrat à distance

La formation du contrat à distance

Le contrat peut se définir comme un acte juridique formé par l'accord de deux ou plusieurs volontés individuelles[482]. La caractéristique essentielle du contrat est l'accord de volonté des parties qui détermine librement les effets du rapport de droit établi : c'est le principe dit de l'autonomie de la volonté.

La conclusion du contrat peut se réaliser de manière instantanée, ce qui est le cas habituel des contrats conclus entre présents. Dans le cas du contrat à distance, la manifestation de la volonté de chaque partie est exprimée successivement, une partie faisant une offre que l'autre accepte postérieurement.

Plusieurs questions se posent alors pour le juriste. En voici les principales .

L'offre

L'offre se définit comme une déclaration unilatérale de volonté adressée par une personne à une autre, et par laquelle l'offrant propose à autrui la conclusion d'un contrat.

Cette offre peut se faire sous n'importe quelle forme. Les entreprises de vente par correspondance offrent leurs produits à la vente sur catalogue papier.

Le commerçant peut aujourd'hui utiliser les moyens offerts par l'Internet, comme support de ses offres : mise en ligne de catalogues électroniques sur un service Web, annonces postées dans les forums de discussion par exemple.

Dans toutes ces hypothèses, l'offre est adressée à une personne indéterminée. Elle contient une proposition de contracter permanente et générale[483].

La jurisprudence a posé le principe que « l'offre faite au public lie le pollicitant (l'offrant) dans les mêmes conditions que l'offre faite à une personne déterminée »[484].

L'offre doit contenir tous les éléments nécessaires afin qu'une simple adhésion du destinataire suffise pour former le contrat. Dans le cas de la vente, il suffit que soient indiqués la chose et le prix : le contrat de vente est formé dès l'accord sur ces deux points[485].

---

[482] Weill et Terré, Les obligations, Dalloz, 4e édition, n°23 et suivants, article 1101 du Code civil.
[483] Francis Delbarre, Offre de produits et services, Gaz. Pal. n° spécial sur la vente à distance, 25 février 1996, p. 6.
[484] Civ. 3e 28 novembre 1968, Bull. Civ., III, n°507.
[485] Articles 1582 et 1583 du Code civil.

Juridiquement, l'offrant est lié si une acceptation est intervenue pendant le délai de validité de l'offre. Le contrat est formé et une personne ou une société qui rétracte tardivement une offre sans motif légitime peut engager sa responsabilité civile[486].

Dans les ventes par correspondance, une fois le support de vente distribué, le vendeur ne sait pas si son offre aura le succès escompté et si les stocks qu'il a prévu suffiront à satisfaire à la demande des clients ou bien s'il se retrouvera avec des surplus. La difficulté pour le commerçant est d'ajuster la validité du support de vente par rapport à l'offre qu'il est en mesure de satisfaire. L'administration admet que les entreprises de vente par correspondance éditant un catalogue annuel ou saisonnier limitent leurs offres aux articles disponibles en stock, en utilisant par exemple la mention « jusqu'à épuisement des stocks ».

L'avantage des nouvelles techniques de communication est qu'elles permettent de connaître la disponibilité d'un article[487]. Une mise à jour du catalogue électronique en ligne peut être effectuée rapidement.

L'offre peut être faite avec réserves, expresse ou tacite, comme celles d'usage ou impliquées par la nature du contrat.

Cependant si ces réserves sont trop générales, il n'y a plus offre mais invitation à entrer en pourparlers.

Dans l'hypothèse où une entreprise utilise un service Internet à seule fin de présentation de ses produits et services et non comme support de vente à distance, pourrait-elle voir sa responsabilité contractuelle engagée en raison des informations fournies sur son site ?

En d'autres termes, l'entreprise pourrait-elle récuser la valeur contractuelle des informations données au public sur son service ?

Une jurisprudence s'est élaborée sur la valeur contractuelle des documents publicitaires.

La jurisprudence considère aujourd'hui que lorsqu'ils sont suffisamment précis et détaillés, les documents publicitaires lient celui qui les réalise ou les utilise, même s'ils précisent qu'ils n'ont pas valeur contractuelle[488].

Un service Internet n'est rien d'autre qu'une nouvelle forme de support pour les offres et la publicité commerciales. Les informations figurant sur un service en ligne, par exemple un site Web, pouvant porter notamment sur les prix ou les caractéristiques techniques des produits de l'entreprise ont valeur de document contractuel.

L'acceptation

L'acceptation marque le moment où se forme le contrat et naît l'engagement contractuel. Aucune forme particulière n'est requise pour la validité du contrat : c'est le principe dit du consensualisme.

Il y a des exceptions à ce principe, la validité de certains contrats étant subordonnée à l'accomplissement d'une formalité particulière. C'est le cas notamment des contrats exigeant l'intervention d'un notaire : donations, contrats de mariage, transferts de biens immobiliers. Même si la profession notariale commence à réfléchir aux conséquences pour l'exercice professionnel de l'irruption des nouvelles techniques de communication[489], la signature des actes notariés à distance n'est pas encore d'actualité.

Les contrats couramment conclus sur l'Internet sont des contrats de la vie commerciale couverts par le principe du consensualisme.

---

[486] Com. 29 juin 1993, Bull.Civ., IV, n°271.

[487] Francis Sérusclat, Le citoyen consommateur, les nouvelles techniques d'information et de communication : l'homme cybernétique ? Rapport de l'Office parlementaire d'évaluation des choix scientifiques et technologiques, Sénat n° 232, p. 207.

[488] Ghestin, Traité de droit civil, Le contrat : formation, LGDJ, 2e édition, n°304 et suivants.

[489] Voir Alain Gobin, Pour une problématique notariale des autoroutes de l'information, JCP éd. N 1995, 3567.

L'acceptation doit être expresse, la jurisprudence ayant posé comme principe que le silence ne vaut pas acceptation. Il en va autrement lorsque l'offre est faite dans l'intérêt exclusif du destinataire et lorsque les parties sont en relation d'affaires. Les usages peuvent également faire obligation au destinataire d'une offre d'exprimer positivement un refus. Par exemple, en matière bancaire, le défaut de contestation après un délai d'un mois des avis d'opéré vaut acceptation des opérations figurant sur l'avis.

La pratique dite des envois forcés, par laquelle des expéditeurs tentent de forcer le consentement des destinataires, en leur faisant parvenir des objets sans demande préalable de ces derniers, accompagnés d'une correspondance indiquant que l'objet peut-être accepté contre versement d'un prix fixé ou renvoyé à son expéditeur est, en plus d'être dépourvue d'effet juridique par l'application du droit commun, sanctionnée pénalement[490], pour dissuader les abus commis par certaines entreprises. Les peines encourues sont notamment une amende de 10 000 francs pour les particuliers et de 50 000 francs pour les personnes morales. Autant d'amendes peuvent être prononcées qu'il y a eu d'envois, s'agissant de contraventions.

Ce texte pourrait-il être appliqué à des envois forcés réalisés par voie électronique ?

Une réponse positive semble pouvoir être apportée : la notion d'objet a été étendue par la jurisprudence à des documents dépourvus de toute valeur mais représentatifs d'un droit tels qu'une carte d'abonnement à une revue[491]. La notion de correspondance accompagnant l'envoi a elle aussi été interprétée largement par les tribunaux[492].

Les modalités d'acceptation d'une offre peuvent être variées, aucune condition de forme n'est imposée par la loi.

C'est cette liberté dans l'expression du consentement à un contrat qui est utilisée dans la pratique dite du contrat « Shrink Wrap License ».

Le fait de déchirer l'emballage de la disquette support d'un logiciel après avoir lu les dispositions du contrat de licence figurant sur la disquette matérialise l'acceptation de l'acheteur[493].

L'entreprise doit imaginer des modes d'expression du consentement adaptés à l'Internet.

Dans certains cas, l'entreprise préfère avoir recours au moyen classique du bon de commande signé, que l'on peut trouver en ligne et qu'il faudra imprimer avant de l'adresser au commerçant. C'est notamment le procédé utilisé par le NIC-France, qui refuse même les demandes d'enregistrement de noms de domaine adressées par télécopie et impose le recours à l'envoi par la poste.

L'entreprise proposant la commande de produits ou services directement sur l'Internet devra veiller à ce que le processus de prise de commande ne laisse planer aucune ambiguïté sur la volonté du contractant.

Pour la CNIL, l'interactivité présente l'inconvénient d'affaiblir la notion de consentement éclairé :

« Dans cette nouvelle relation, marquée par la convivialité, l'attrait du jeu, le désir d'en savoir plus, que devient véritablement le consentement du sujet, qui suppose un minimum de recul, une information préalable et complète, puis un temps de réflexion. »[494]

Le fait qu'une commande puisse être réalisée par la simple activation d'un lien hypertexte pourrait être considéré comme insuffisant : faire défiler des pages d'écran et naviguer d'un service à un autre sans but nécessairement précis est une pratique courante de la part des

[490] Article R 635-2 du Code pénal.
[491] Crim. 14 avril 1972, Gaz. Pal. 1972.1.601.
[492] Francis Delbarre, Aspects spécifiques, Gaz. Pal. N° spécial sur la vente à distance, 25 février 1993, p.51.
[493] Sur ce contrat, voir : Yves Wehrli et F. Bloch, Portraits de contrats, Expertises octobre 1993, n°165, p. 337.
[494] Voix, image et protection des données, Rapport de la CNIL, Documentation française 1996, p. 50.

internautes baptisée « surfer » ou « butiner ». On ne devrait pas pouvoir se retrouver engagé dans un contrat par simple inadvertance.

L'entreprise qui adresserait des objets commandés ainsi pourrait risquer de se voir reprocher de faire des envois forcés.

La manifestation de l'acceptation peut résulter par exemple de l'accomplissement des démarches nécessaires pour effectuer un paiement.

Certaines commandes nécessitent une confirmation par courrier électronique.

Par exemple, pour enregistrer un nom de domaine auprès de la société Network Solutions Inc., il faut remplir un formulaire en ligne. Un courrier électronique est adressé, auquel il devra être répondu par le même moyen pour confirmer l'opération.

Une autre méthode est l'envoi d'un mot de passe et d'un identifiant par courrier électronique au client potentiel qui valide ensuite les opérations effectuées sur le site de l'offrant en fournissant mot de passe et identifiant.

Un auteur explique qu'il n'y a aucun obstacle en droit français à ce que l'acceptation s'exécute par « cliquage », la saisie de données puis le « cliquage » constituant l'acceptation[495].

Cependant, la confirmation de la commande par courrier électronique correspond à une nécessité pratique et juridique : il faut bien vérifier que l'acceptation correspond à une volonté réelle et qu'elle n'est pas le fait d'une personne qui utilise la boîte aux lettres d'une autre. Sinon n'importe quelle personne disposant d'un accès à l'Internet pourrait effectuer des commandes en utilisant les coordonnées de tiers.

Le droit et la technique laissent tout loisir au commerçant pour organiser comme il l'entend la formation d'un contrat conclu sur l'Internet. L'entreprise devra néanmoins veiller à prendre un minimum de précautions pour s'assurer de l'authenticité de l'engagement de son client.

Dans la pratique actuelle cette vérification s'effectue souvent au niveau du paiement, qui conditionne la livraison par le vendeur, soit par une procédure d'échange de courrier électronique telle que décrite ci-dessus.

Cette question de l'authenticité de l'engagement du contractant m'amène au problème de la vérification de l'identité des intervenants.

L'identification des parties au contrat

Dans les rapports traditionnels, l'identité des parties est établie par les contacts directs. Le cas échéant, une pièce d'identité, l'extrait K-bis d'une société, peuvent être fournis. Par hypothèse, ce moyen de contrôle échappe à l'entreprise qui vend par correspondance et il en est de même sur l'Internet.

En droit, cette impossibilité de contrôler l'identité du client pose la question de la vérification de sa capacité juridique. Le problème se pose notamment pour les mineurs et les personnes morales.

Le contrat à distance avec un mineur[496]

Le mineur ne peut pas en principe agir juridiquement sans l'intermédiaire d'un représentant légal, généralement ses parents[497]. Il s'agit d'une mesure de protection du mineur. Cependant, la jurisprudence admet que le mineur peut valablement accomplir certains actes de la

[495] Olivier Itéanu, Internet et le Droit, Aspects juridiques du commerce électronique, éditions Eyrolles 1996, p. 86.
[496] Léon Azancot, Formation du contrat, problèmes posés par les mineurs, Gaz. Pal. n°spécial sur la vente à distance, 25 février 1993,p.31.
[497] Article 1124 du Code civil.

vie courante. Les articles 389-3 (administration légale) et 450 (tutelle) du Code civil visent d'ailleurs expressément les cas où la loi ou l'usage autorise les mineurs à agir eux-mêmes.

Les décisions semblent fondées sur l'importance du bien vendu. Par exemple, l'achat d'un vélomoteur[498] a été considéré comme un acte de la vie courante que le mineur pouvait accomplir seul.

Cette notion d'acte de la vie courante devrait couvrir tous les biens de consommation courante, tels que logiciels et jeux, que l'on peut se procurer sur l'Internet. D'autres décisions ont recours à la notion de mandat tacite : le mineur est considéré comme le mandataire de ses parents[499].

Il a par exemple été jugé que le vendeur par correspondance de biens de faible valeur destinés aux enfants peut invoquer, en cas de commande passée par un mineur, un mandat apparent, tacite et oral des parents de celui-ci[500].

Les parents ne sont pas tenus des obligations nées des contrats passés par leurs enfants mineurs[501]. Le recours à la théorie du mandat tacite permet à l'entreprise de vente à distance d'avoir un recours direct contre les parents du mineur *a priori* plus solvables.

La question de la vérification de l'âge du cocontractant va également se poser pour l'entreprise qui vend à distance du matériel à caractère pornographique. L'article 227-24 du Code pénal punit de 3 ans d'emprisonnement et de 500 000 francs d'amende le fait de fabriquer, transporter, diffuser par quelque moyen que ce soit et quel qu'en soit le support un message à caractère violent ou pornographique ou d'en faire commerce lorsque ce message est susceptible d'être vu par un mineur.

Le pouvoir d'engager son entreprise

Dans le cas d'une commande effectuée par un employé de l'entreprise destinataire de l'offre, la question de savoir si elle émane bien d'une personne habilitée à engager l'entreprise peut se poser. Le pouvoir d'obliger l'entreprise appartient aux dirigeants légaux, qui peuvent déléguer leurs pouvoirs à certains employés. On a recours à la notion de mandat apparent : le commerçant peut légitimement croire aux pouvoirs de son cocontractant. La jurisprudence considère que la vente est valablement formée, dans la mesure où le vendeur n'a pu raisonnablement douter de l'habilitation de celui qui effectue la commande[502].

Dans une affaire où le préposé d'une société avait réservé par télex une chambre d'hôtel, la société a été considérée comme contractuellement engagée bien que le préposé n'était autorisé à utiliser le télex que pour la prospection de la clientèle : elle avait la possibilité de vérifier l'authenticité des messages émis, dont copie était conservée, et de demander l'annulation de réservations faites en son nom par une personne autorisée à utiliser son télex[503].

Le moment et le lieu de la formation du contrat

Le contrat à distance pose le problème théorique de la détermination du moment et du lieu de sa formation.

La détermination de la date du contrat peut avoir des incidences pratiques.

Une fois le contrat formé par l'acceptation, l'offre ne peut plus être rétractée, l'offrant est lié. La date de formation marque également le pont de départ des effets du contrat : c'est à cette date que la propriété, et le risque de perte sont transférés à l'acheteur.

---

[498] Rennes 19 novembre 1980, JurisData n°80220.
[499] L'article 1990 du Code civil prévoit expressément la possibilité pour le mineur d'agir en qualité de mandataire.
[500] TI Nîmes 29 juin 1982, D 1983.13.
[501] Civ. 1re 21 juin 1997, Bull.Civ. I, p. 225.
[502] Léon Azancot, Formation du contrat, Gaz. Pal. n°spécial sur la vente à distance, 25 février 1993, p28.
[503] Com. 13 mai 1986, n°84-12.791.

Le lieu de formation du contrat peut avoir des conséquences sur la loi applicable en droit international privé[504].

Concernant le moment de formation du contrat, deux choix sont possibles : le contrat est formé lors de l'émission de l'acceptation ou il n'est formé qu'au moment où l'entreprise reçoit et prend connaissance de l'acceptation de son client.

Dans un arrêt en date du 7 janvier 1981, la Cour de cassation a posé le principe que faute de stipulation contraire, l'offre était destinée à devenir parfaite, non pas par la réception par son auteur de l'acceptation de son destinataire, mais par l'émission par celui-ci de son acceptation[505].

Si l'on transpose cette solution à l'Internet, le contrat doit-il être considéré comme conclu dès la validation du bouton informatique apparaissant à l'écran ?

Certaines entreprises choisissent de recourir à un système de confirmation par courrier électronique, en vue de s'assurer de la réalité de la volonté du client.

Ces échanges, ces confirmations font partie du processus mis en place pour exprimer la manifestation de l'acceptation du client. Le contrat serait formé lors de l'émission du courrier électronique de confirmation.

La solution est fluctuante, puisqu'elle va dépendre de la procédure mise en œuvre. En outre, elle pose un problème de preuve quant à la date exacte de l'envoi d'un courrier ou de la validation d'une page écran. Toutes ces questions peuvent sembler abstraites. Le commerçant aura cependant intérêt pour éviter tout conflit, à s'assurer de la fiabilité de son système et à fixer conventionnellement, en l'incluant dans son offre, le moment choisit pour la formation du contrat.

Les règles du contrat à distance

Le contrat conclu avec un consommateur

Le régime particulier de protection des consommateurs élaboré pour les contrats à distance est applicable au commerce électronique[506], qui n'est qu'une technique particulière de ce type de commercialisation.

Ce régime spécifique n'est applicable que si le cocontractant est un consommateur, c'est-à-dire un non-professionnel. En matière de commerce sur l'Internet, certains produits pourront indifféremment être achetés par des consommateurs ou par des professionnels. C'est par exemple le cas des logiciels. L'entreprise devra en tenir compte. Il a d'ailleurs été jugé que les obligations en matière de produits ou de services offerts à des consommateurs s'appliquent même si le fournisseur s'adresse le plus souvent à des utilisateurs professionnels, dès lors que les produits ou services sont également offerts à des consommateurs ou peuvent être achetés par eux[507].

La sollicitation du consommateur

Une loi du 23 juin 1989[508] réglemente la technique du marketing téléphonique :

[504] Voir Infra
[505] Bull.Civ. IV, n°14.
[506] Isabelle Pottier, Le commerce électronique sur Internet, Gaz. Pal. 4 avril 1996, p.27.
[507] Crim. 15 juin 1987, Bull. Crim., p. 678.
[508] Article 2 bis de la loi n°89-421, modifiant la loi n°72-1137 du 22 décembre 1972.

« A la suite d'un démarchage par téléphone ou par tout moyen technique assimilable, le professionnel doit adresser au consommateur une confirmation de l'offre qu'il a faite. Le consommateur n'est engagé que par sa signature. »

La réglementation en matière de démarchage à domicile[509] est appliquée au marketing téléphonique : remise d'un écrit comportant des mentions obligatoires lors de la conclusion du contrat, faculté de renonciation dans un délai de 7 jours à compter de la commande ou de l'engagement d'achat, interdiction de recevoir du client une contrepartie quelconque avant l'expiration du délai de réflexion. Les infractions aux règles relatives au démarchage sont punies d'une peine d'emprisonnement d'un mois à un an et/ou d'une amende de 1 000 à 20 000 francs. Le moment de la formation du contrat est retardé jusqu'à ce que le consommateur ait signé une acceptation écrite. Ce dispositif est-il applicable aux échanges sur l'Internet ?

Des auteurs estiment qu'une télécopie ou un télex constituent un « moyen technique assimilable » au téléphone[510]. La loi sur le démarchage téléphonique semble donc pouvoir s'appliquer aux offres et prestations transmises par courrier électronique, ou un autre moyen de télécommunication. Il faut également pour que le dispositif prévu par la loi de 1989 s'applique qu'il y ait démarchage. Il n'y a pas démarchage si le client est à l'initiative de la commande. Ce sera notamment le cas lorsqu'elle est effectuée par l'intermédiaire d'un site Web. Certaines entreprises pratiquent le mailing massif de courrier électronique à des fins publicitaires, pratique désignée sous le terme de « spamming ».

Si une commande est effectuée suite à l'envoi d'un tel courrier, il y a démarchage et la loi de 1989 devrait être respectée par l'émetteur du message publicitaire[511].

Cette pratique est en outre contraire aux règles de la Netiquette[512].

On peut imaginer aussi un vendeur communiquant avec ses clients par une méthode comme l'IRC, qui permet l'échange de messages en temps réel : il y aurait dans une telle situation démarchage.

En revanche, si une commande est effectuée à la suite d'une annonce parue dans un forum de discussion, il n'y a pas démarchage : la lecture d'un forum est un acte volontaire.

L'information du consommateur

La réglementation du droit de la consommation concernant les contrats à distance s'applique au commerce électronique.

Le législateur considère le catalogue ou tout autre support de la vente à distance comme un lieu de vente au sens de la réglementation[513].

Identification de l'entreprise émettrice de l'offre

L'article 121-18 du Code de la consommation prévoit que « dans toute offre de vente d'un bien ou de fourniture d'une prestation de services qui est faite à distance à un consommateur, le professionnel est tenu d'indiquer le nom de son entreprise, ses coordonnées téléphoniques ainsi que l'adresse de son siège, et si elle est différente, celle du responsable de l'offre ».

Information du consommateur sur les caractéristiques du produit

L'entreprise doit mettre le consommateur en mesure de connaître « les caractéristiques essentielles du bien ou du service » (article L111-1 du Code de la consommation).

---

[509] Articles L121-23 et suivants du Code de la consommation.
[510] France. Delbarre, Offre de produits et services, Gaz. Pal. n° spécial sur la vente à distance, 25 février 1996, p. 11 ; Lamy droit économique 1996, n°2677.
[511] O. Hance, Business et Droit d'Internet, Best Of Editions 1996, p. 135.
[512] Voir supra
[513] Danielle Marsal, La Vision du praticien, Gaz. Pal. n° spécial sur la vente à distance, 25 février 1996, p 15.

Une disproportion trop grande entre l'objet présenté et la réalité pourrait constituer le délit de publicité trompeuse[514]. Cela peut être délicat à mettre en œuvre pour la diffusion d'un catalogue sur un service Web, où la page affichée va varier en fonction de l'ordinateur, du logiciel et de l'écran utilisés par le client. Les photographies et dessins pourront être complétés par des indications sur la dimension et la couleur exactes des produits.

Information sur les prix

L'article 14 d'un arrêté du 3 décembre 1987 prévoit que « le prix de tout produit ou de toute prestation de service proposés au consommateur selon une technique de communication à distance doit être indiqué de façon précise au consommateur, par tout moyen faisant preuve, avant la conclusion du contrat ».

Une circulaire du 19 juillet 1988 prévoit que les professionnels ont toute latitude dans le choix du procédé approprié à cette fonction. Tout procédé d'information publique comme un site Web peut être utilisé à cette fin.

Le prix doit être indiqué en monnaie française et toutes taxes comprises. Les frais de livraison doivent être inclus dans le prix de vente, ou leur montant doit être indiqué en sus.

Les manquements aux obligations d'information sont sanctionnés par une contravention de 5e classe (10 000 francs par infraction).

Conditions de vente

L'indication de la date limite à laquelle le professionnel s'engage à livrer le bien ou à exécuter la prestation est obligatoire lorsque le prix excède 3 000 francs[515].

Les conditions de vente, notamment en ce qui concerne la responsabilité contractuelle, les conditions particulières, les garanties, les modalités de paiement devraient être portées à la connaissance du consommateur de la manière la plus claire et la plus précise possible[516].

Le délai de rétractation

« Pour toutes les opérations de vente à distance, l'acheteur d'un produit dispose d'un délai de 7 jours francs à compter de la livraison de sa commande pour faire retour de ce produit au vendeur pour échange ou remboursement, sans pénalités à l'exception des frais de retour. »[517]

Ce droit est discrétionnaire, le client n'a pas à en donner la motivation. Il n'est pas applicable aux prestations de services, mais ne comporte aucune exception, même dans l'hypothèse où seraient concernés des produits périssables. L'exercice de ce droit pourrait être susceptible de soulever des difficultés dans d'autres hypothèses. Notamment, ce droit de retour est-il justifié dans le cas de biens numérisés, qui peuvent être téléchargés, comme les logiciels, les enregistrements audio et vidéo, les articles de journaux téléchargés à l'unité ? De tels biens, s'ils sont livrés sous forme numérique, sont reproductibles à volonté. Un consommateur de mauvaise foi ne serait-il pas tenté d'en tirer parti pour invoquer son droit de rétractation tout en conservant une copie du bien obtenu ?

Il n'est pas inintéressant de relever qu'un projet de directive [518] prévoit que le droit de rétractation n'est pas octroyé au consommateur sauf accord contraire, dans certains cas spécifiques, et notamment aux produits immédiatement reproductibles[519].

---

[514] Voir supra

[515] Article L114-1 du Code de la consommation.

[516] France. Delbarre, Gaz. Pal. n° spécial sur la vente à distance, 25 février 1996, p 6.

[517] Article L121-16 du Code de la consommation.

[518] Proposition de directive du 21 mai 1992 "concernant la protection des consommateurs en matière de contrats négociés à distance", COM(92) 11, JOCE 92 C156, modifiée plusieurs fois. Le Conseil a adopté une position commune le 29 juin 1995.

[519] Article 11-4 de la proposition, préc.

On relèvera également que dans le projet de directive le droit de rétractation est étendu aux services.

Cependant cette proposition n'a pas encore été adoptée et ne peut pas être invoquée par une entreprise qui offre ses produits ou services en France. Le refus d'échanger ou de rembourser un produit retourné par l'acheteur constitue une contravention de 5e classe (10 000 francs d'amende).

Les réglementations spécifiques

L'offre à distance de certains produits ou activités fait l'objet d'une réglementation spécifique qui concerne également le commerce électronique[520]. L'entreprise doit présenter ses produits et services en appliquant et adaptant, le cas échéant, la réglementation existante. Le fait que le support utilisé soit l'Internet ne change pas ce principe.

Par exemple, les pharmaciens n'ont pas le droit de vendre à distance des médicaments ou d'autres marchandises dont il font le commerce[521]. Or, il est possible de commander sur l'Internet par correspondance des médicaments. Ainsi, il est possible d'acheter par correspondance de la mélatonine, une substance qui n'a pas eu d'autorisation de mise sur le marché en France mais est en vente libre dans d'autres pays[522].

Cependant, l'interdiction de l'envoi par correspondance des médicaments peut s'avérer contraire au principe de libre circulation des marchandises. Concernant une affaire qui opposait un consommateur allemand, qui avait commandé à une pharmacie strasbourgeoise l'envoi par la poste d'un médicament vendu en France, à la douane allemande, la Cour de justice de la Communauté européenne a précisé que :

« Est incompatible avec les articles 30 et 36 du traité CEE une disposition nationale qui interdit l'importation, par un particulier, pour ses besoins personnels, de médicaments autorisés dans l'Etat membre d'importation, délivrés dans cet Etat sans prescription médicale et achetés dans une pharmacie d'un autre Etat membre »[523].

[520] Voir Olivier Itéanu, Internet et le Droit, éditions Eyrolles, 1996, p.96 et suivantes.
[521] Article L589 du Code de la santé publique.
[522] Marc Salama, « J'ai acheté ma dose sur le Net », *Planète Internet* n° 9 juin 1996, p.34.
[523] CJCE 7 mars 1989, aff. 215/87, Rec. CJCE, p. 617.

Deuxième partie

Remplacer l'écrit ; aspects juridiques

La recevabilité de la preuve informatique

La preuve est un élément déterminant dans une relation contractuelle. Elle permet de prévenir et de régler les contestations ultérieures. La loi réglemente la manière dont on peut apporter la preuve de l'engagement d'une autre partie.

L'exigence d'un écrit pour la preuve

Le droit de la preuve est marqué par le principe de la prééminence de l'écrit. L'écrit représente la preuve légale parfaite. Même si le contrat est valablement formé sans écrit du seul fait de l'échange des consentements des parties, la nécessité pour les parties de se ménager la preuve de leur contrat impose en réalité le recours à un écrit. L'écrit au sens traditionnel, c'est le titre original, acte sous seing privé ou acte authentique (acte passé devant notaire) revêtu d'une signature manuscrite et matérialisé dans un document papier.

Le principe est posé par l'article 1341 du Code civil complété par un décret du 15 juillet 1980 : un acte écrit est exigé pour toute convention dont l'objet vaut plus de 5 000 francs. En outre, lorsqu'un écrit a été rédigé, on ne peut apporter la preuve contraire que par un autre écrit, la preuve par témoins est irrecevable.

Ce principe de la preuve écrite comporte néanmoins un certain nombre d'exceptions qui permettent de s'affranchir de cette exigence qui ne manquerait pas autrement d'être un obstacle juridique certain au développement du commerce électronique. En effet, lorsqu'une transaction s'effectue à travers un réseau informatique, il est évident que les parties n'échangent aucun écrit signé : l'écrit (au sens de document papier écrit à l'encre) impose des contraintes physiques de déplacement incompatibles avec le commerce électronique.

Les exceptions à l'exigence d'un écrit

En matière commerciale

En application de l'article 109 du Code de commerce, le contrat peut être prouvé par tous moyens en matière commerciale. Ce principe est important car il concerne toutes les relations entre entreprises. Dans les actes dits mixtes passés entre un commerçant et un particulier, la preuve est libre pour le particulier contre le commerçant.

En matière civile (contrat entre particuliers, ou preuve du contrat pour le commerçant contre le particulier), les exceptions suivantes sont admises :

En matière civile

La valeur du bien est inférieure à 5 000 francs

La loi impose un écrit pour les conventions dont l'objet a une valeur supérieure à 5 000 francs. En dessous de ce seuil, la preuve est libre.

Le principe est important car en matière de distribution et de consommation courante, qui constitue l'essentiel de la vente à distance aux particuliers, la majorité des transactions n'excède pas ce montant.

Le commencement de preuve par écrit

Cette exception résulte de l'article 1347 du Code civil qui précise que :

« On appelle ainsi tout acte par écrit qui est émané de celui contre lequel la demande est formée, ou de celui qu'il représente, et qui rend vraisemblable le fait allégué. »

Par exemple, une copie carbone[524] ou une photocopie[525] peut valoir commencement de preuve par écrit.

Le texte est interprété largement par la jurisprudence. La Cour de cassation a admis qu'il importait peu que l'acte ne soit ni écrit, ni signé par celui à qui on l'opposait, pourvu qu'il soit son œuvre intellectuelle[526]. Cependant, il ne s'agit que d'un début de preuve qui devra être complété par d'autres éléments.

Il serait donc possible d'admettre comme commencement de preuve par écrit un tirage papier de documents numériques[527], à condition de disposer d'éléments complémentaires et que le document invoqué émane de l'autre partie.

L'impossibilité d'établir un écrit

Aux termes de l'article 1348 du Code civil, la règle de l'écrit reçoit exception lorsque l'une des parties s'est trouvée dans l'impossibilité de se procurer une preuve écrite. La loi vise deux types d'impossibilités : l'impossibilité morale, qui va concerner notamment les relations familiales et l'impossibilité matérielle.

Plusieurs auteurs estiment que la notion d'« impossibilité matérielle » ouvre la voie à l'admission de la preuve informatique. Le juge peut considérer qu'il y a eu impossibilité de rédiger un écrit chaque fois qu'il se trouvera en présence d'un procédé de transmission de données dématérialisées[528]. L'impossibilité résulte de l'état de la technique[529].

Aucune décision de jurisprudence n'est encore venue infirmer ou confirmer ce raisonnement qui ne fait pas l'unanimité chez les juristes[530].

La perte de l'original

La règle de l'écrit reçoit aussi exception « lorsqu'une partie ou le dépositaire n'a pas conservé le titre original et présente une copie qui en est la reproduction fidèle mais aussi durable. Est réputée durable toute reproduction indélébile de l'original qui entraîne une modification irréversible du support[531] ».

---

[524] Civ. 1re 27 mai 1986, Bull.Civ.I, n° 141.
[525] Civ.1re 14 février 1995, JCP éd. G, II, 22 402, note Chartier.
[526] Civ.1re 7 juillet 1955, D 1955.737.
[527] Lamy informatique 1996, n° 2403.
[528] Françoise Chamoux, La loi du 12 juillet 1980 : une ouverture sur de nouveaux moyens de preuve, JCP éd. G 1981, II, 13 491, n° 21.
[529] Alain Bensoussan, Contributions théoriques au droit de la preuve dans le domaine informatique : aspects techniques et solutions juridiques, Gaz. Pal. 1991, 2, p. 361.
[530] Pour un avis opposé, voir Claude Lucas de Leyssac, Le droit fondamental de la preuve, l'informatique et la télématique, Petites Affiches, 29 mai 1996, p.3.
[531] Article 1348 alinéa 2 du Code civil.

Un enregistrement numérique pourrait-il être considéré comme un copie ? Avec la technique numérique, la notion d'original n'existe plus puisque la copie est indissociable du document original.

En outre, il faut que le juge puisse être certain que le document n'a pas été modifié à son insu. Or les procédés de reproduction utilisés ne permettent pas de déceler un montage qui aurait été fait[532]. Enfin, pour qu'il y ait copie, il faut qu'il y ait eu un original qui n'existe plus[533].

Le texte semble donc exclure la preuve par le contenu des mémoires d'un ordinateur[534].

Les conventions sur la preuve

Les dispositions relatives à la preuve ne sont pas d'ordre public. Il est donc possible pour les parties de prévoir dans un contrat les questions relatives à l'admissibilité et la valeur probante de documents numériques.

Un arrêt de la Cour de cassation du 2 mai 1989 a ainsi consacré la validité d'une convention sur la preuve à propos d'un paiement électronique[535]. Cette jurisprudence a été confirmée dans un arrêt du 8 novembre 1989[536] :

« En statuant ainsi, alors que la société Crédicas invoquait l'existence dans le contrat, d'une clause déterminant le procédé de preuve de l'ordre de paiement et que, pour les droits dont les parties ont la libre disposition, ces conventions relatives à la preuve sont licites, le tribunal a violé les textes susvisés. »

Une convention sur la preuve peut être conclue entre un professionnel et un consommateur. Par exemple, les conditions générales de fonctionnement de la carte bleue de la BNP (Banque nationale de Paris) [537] prévoient que :

« Les enregistrements des appareils automatiques ou leur reproduction sur un support automatique constituent la preuve des opérations effectuées au moyen de la carte et la justification de leur imputation au compte sur lequel cette carte fonctionne ».

Toutefois, dans le cadre d'une convention conclue avec un consommateur, l'entreprise devra veiller à ce que les dispositions sur la preuve ne puissent pas être qualifiées d'abusives.

En effet, l'article L132-1 du Code de la consommation répute non écrites les clauses qualifiées d'abusives dans les contrats conclus entre professionnels et non-professionnels. La clause est abusive si elle a « 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 ».

Le Code de la consommation comporte une annexe avec une liste indicative et non exhaustive de clauses qui peuvent être regardées comme abusives. En cas de litige concernant une telle clause, le demandeur n'est pas dispensé d'apporter la preuve du caractère abusif de la clause. Parmi les clauses énumérées dans l'annexe figurent les clauses ayant pour objet ou pour effet de « supprimer ou d'entraver l'exercice d'actions en justice ou des voies de recours par le consommateur, notamment (…) en limitant indûment les moyens de preuve à la disposition du consommateur ou en imposant à celui-ci une charge de preuve qui, en vertu du droit applicable, devrait revenir normalement à une autre partie au contrat ».

Concernant cette fois les clauses insérées par les émetteurs de cartes dans leurs contrats, la Commission des clauses abusives recommande que soient éliminées des contrats « porteur » proposés par ces émetteurs, les clauses ayant pour objet ou pour effet « de conférer aux

[532] Françoise Chamoux, La loi du 12 juillet 1980 : une ouverture sur de nouveaux moyens de preuve, JCP éd. G 1981, II, 13 491, n° 25.
[533] Lamy informatique 1996, n°2408.
[534] Hervé Croze, Informatique, preuve et sécurité, D 1987.165, n°13.
[535] Civ. 1re 2 mai 1989, Droit de l'Informatique et des Télécoms 1990/2, p.38.
[536] Civ. 1re 8 novembre 1989, D 1990.369.
[537] Edition mars 1994, article 9-1.

enregistrements magnétiques détenus par les établissements financiers ou bancaires une valeur probante en dispensant ces derniers de l'obligation de prouver que l'opération contestée a été correctement enregistrée et que le système fonctionnait normalement »[538].

L'écrit est une condition de validité du contrat

L'écrit peut s'avérer nécessaire à titre de validité d'un acte. A côté des actes qui doivent obligatoirement être passés sous la forme notariée, il existe toute une série de dispositions rendant la forme écrite obligatoire pour la validité du contrat ou encore pour l'accomplissement d'une formalité. Par exemple, il serait difficile de procéder à une formalité d'enregistrement auprès de l'administration fiscale en l'absence de contrat écrit.

En matière de droit d'auteur, l'article L131-1 du Code de la propriété intellectuelle prévoit que :

« Les contrats de représentation, d'édition et de production audiovisuelle définis au présent titre doivent être constatés par écrit. Il en est de même des autorisations gratuites d'exécution. »

Pour la jurisprudence, cet écrit n'est pas requis pour la validité du contrat mais pour sa preuve et lorsque l'éditeur a la qualité de commerçant, l'auteur peut administrer la preuve de l'existence du contrat par tous moyens[539].

Les accords de coopération « doivent faire l'objet d'un contrat écrit en double exemplaires »[540].

L'article 1907 alinéa 2 du Code civil précise que le taux d'intérêt conventionnel doit être fixé par écrit. Dans une affaire où une photocopie avait été admise à titre de commencement de preuve par écrit, la Cour de cassation a en revanche refusé de considérer que la stipulation de l'intérêt sur la photocopie était suffisant.[541]

Lorsqu'un formalisme est imposé par la loi, il est évident que le recours aux documents numériques est exclu et que les moyens de communication offerts par l'Internet ne pourront pas être utilisés pour former un contrat.

Droit comparé et perspectives

L'Internet permettant les échanges avec des partenaires de différents pays, la question peut se poser de savoir si le droit du cocontractant reconnaît la recevabilité des données numériques comme moyen de preuve.

L'Europe continentale est marquée par le principe de la prééminence de l'écrit, tempéré par des adaptations législatives ou jurisprudentielles du droit de la preuve dans certains pays. En Allemagne, les documents informatiques entrent selon les cas, dans la catégorie des preuves écrites sans signature ou des preuves par « observations » (l'observation doit permettre au juge de se forger son opinion grâce à sa propre « perception concrète »). Les pays d'Europe continentale ont également adopté dans les domaines commerciaux, financiers et fiscaux, des lois tenant compte du développement de l'informatique.[542]

---

[538] Recommandation n°94-02 relative aux contrats porteur des cartes de paiement assorties ou non d'un crédit, BO.CCRF 30 mai 1995, p.182

[539] Civ. 1re 12 avril 1976 "Derrida", RTD Commercial 1976, p.484.

[540] Article 33 de l'Ordonnance du 1er décembre 1986 modifiée.

[541] Civ.1re 14 février 1995, D 1995.340.

[542] La recevabilité des moyens informatiques comme moyen de preuve, Note du service des affaires européennes du Sénat, division des études de législation comparée, novembre 1994, n°69.

Dans les pays anglo-saxons, qui sont des pays de droit coutumier, deux règles font obstacle à la preuve par document informatique : l'interdiction de la preuve par ouï-dire (hearsay rule) et la règle de la meilleure preuve (best evidence rule)[543].

Le témoignage, mode de preuve privilégié, n'est recevable que s'il émane de quelqu'un qui a eu personnellement connaissance des faits. Par exemple, un document est irrecevable si son auteur n'est pas présent pour témoigner de son contenu devant le tribunal. Cette règle a pour conséquence que les documents informatiques sont considérés comme preuve par ouï-dire irrecevable.

En vertu de la règle de la meilleure preuve, un document n'est en principe recevable que s'il est produit dans sa forme originale.

Ces règles ont été adaptées pour les documents numériques.

Le Royaume-Uni s'est doté d'un Civil Evidence Act de 1995, qui simplifie la preuve par document informatique. Un document informatique est admissible à titre de preuve mais devra être authentifié selon une procédure spécifique (par exemple tenue d'un registre) et être suffisamment fiable pour emporter la conviction du juge.

Aux Etats-Unis, les règles fédérales sur la preuve ont été modifiées en 1975 pour autoriser la recevabilité des documents informatiques, législation reprise par une majorité d'Etats américains. En outre, les tribunaux américains ont tendance à interpréter de façon évolutive les règles de preuve afin de tenir compte des évolutions de la technique et des pratiques professionnelles.

Certaines dispositions de droit américain peuvent nécessiter le recours à un écrit en fonction de la nature du bien vendu et de sa valeur[544]. Par exemple, la section 2201 de l'Uniform Commercial Code (UCC) californien prévoit qu'un écrit est nécessaire pour prouver la vente d'un bien supérieur à 500 dollars américains. Une interprétation extensive de la notion d'écrit et l'analogie avec la jurisprudence développée au sujet des télégrammes peut permettre d'utiliser un document informatique comme mode de preuve[545].

Les contraintes juridiques quant à l'admissibilité de la preuve informatique vont nécessiter des modifications législatives. Les organisations internationales ont publié des travaux et documents en ce sens. La Commission des Nations unies pour le droit commercial international recommande ainsi[546] « aux gouvernements :

- de réexaminer les règles juridiques touchant les enregistrements informatiques comme moyens de preuve en justice afin d'éliminer les obstacles superflus à leur recevabilité, de s'assurer que ces règles sont compatibles avec les progrès techniques et de donner aux tribunaux les moyens leur permettant d'apprécier la fiabilité des données contenues dans ces enregistrements ;
- de réexaminer les règles juridiques en vertu desquelles certaines transactions commerciales ou certains documents ayant trait au commerce doivent être sous forme écrite (…) ».

[543] O. Hance, Business et Droit d'Internet, Best Of Editions 1996, p. 225 et suivantes.

[544] Règle de la "statute of fraud".

[545] Pour une analyse du droit américain de la preuve au regard d'un contrat conclu par courrier électronique, voir : Richard Allan Horning, Has Hal signed a contract : the stature of frauds in cyberspace, intervention à un colloque organisé par l'Union des avocats européens, Le droit des autoroutes de l'information et du mulitmédia : un nouveau défi, Monaco, 3 mai 1996, disponible à : <http://www.iway.fr/groupecx/uae/Horning.html>.

[546] Recommandation concernant la valeur juridique des enregistrements informatiques, rapport de la CNUDCI sur les travaux de sa 18e session.

La valeur probante d'un document numérique

Le fait qu'un document informatique puisse être admis comme mode de preuve ne signifie pas que son contenu soit incontestable. Il est soumis à la règle de la libre appréciation par le juge qui est libre de le considérer comme fiable ou non. C'est la question de la valeur probante d'un document électronique.

Un mode de preuve est sûr s'il permet d'éviter les contestations.

Même s'il n'est pas obligatoire, l'écrit reste un instrument privilégié de la preuve du contrat. La primauté de l'écrit est fondée sur l'idée selon laquelle ce mode de preuve offre plus de sécurité[547]. Le papier offre un support tangible, lisible et dont les altérations vont pouvoir être décelées.

Pour un document électronique, la notion d'original disparaît. L'original qui se trouve sur le disque dur de l'ordinateur n'est pas directement accessible au sens humain et le document est en réalité produit sous forme de copie. La numérisation des données autorise toutes les manipulations de ce document et ces modifications ne sont pas décelables.

Or, le document électronique doit pouvoir être fiable pour emporter la conviction du juge et ne pas être remis en question par celui à qui on l'oppose. Si on prend l'exemple du courrier électronique, il est possible de créer un message qui n'a jamais été envoyé, de modifier le contenu d'un message. S'agissant d'un réseau ouvert, on ne peut pas connaître à l'avance le chemin qui sera emprunté par un message, on ne peut pas être sûr qu'il a bien été reçu et si une personne nie avoir reçu un message, il ne sera pas possible de prouver le contraire.

En cas de contestation, il va être difficile de démontrer la réalité de l'échange, s'il n'est pas possible de recourir à d'autres éléments. C'est le problème de la fiabilité des enregistrements numériques en général.

Par exemple, il a été jugé que compte tenu des possibilités de montage et de trucage qu'offre l'évolution des techniques, un film vidéo ne présente pas de garanties suffisantes d'authenticité, d'impartialité et de sincérité, concernant tant sa date que son contenu, pour qu'il puisse être considéré comme probant des fautes invoquées comme motif de licenciement[548].

La preuve en l'absence d'écrit

Liberté de la preuve ne signifie pas absence de preuve. Il sera donc nécessaire d'imaginer comment il va être possible de prouver une opération en l'absence d'écrit, dans des conditions qui permettent d'éviter les contestations.

La fiabilité du système

Le Code civil du Québec, qui contient des dispositions relatives aux « inscriptions informatisées » prévoit ainsi que :

Article 2837. « Lorsque les données d'un acte juridique sont inscrites sur support informatique, le document reproduisant ces données fait preuve du contenu de l'acte, s'il est intelligible et s'il représente des garanties suffisamment sérieuses pour qu'on puisse s'y fier. Pour apprécier la qualité du document, le tribunal doit tenir compte des circonstances dans lesquelles les données ont été inscrites et le document reproduit. »

[547] HervéCroze, Informatique, Preuve et sécurité, D 1987.165, n° 5.
[548] Aix 18e Ch. 4 janvier 1994, JCP éd. G, II, 22 514.

Article 2838. « L'inscription des données d'un acte juridique sur support informatique est présumée présenter des garanties suffisamment sérieuses pour qu'on puisse s'y fier lorsqu'elle est effectuée de façon systématique et sans lacunes, et que les données inscrites sont protégées contre les altérations. Une telle présomption existe en faveur des tiers du seul fait que l'inscription a été effectuée par une entreprise. »

Article 2839. « Le document reproduisant les données d'un acte juridique inscrites sur support informatique peut être contredit par tous moyens. »

Un projet de loi-type de la Commission des Nations unies pour le droit commercial international (CNUDCI)[549], censé servir de guide d'implantation pour le législateur qui entend adopter une loi pour faciliter les transactions commerciales dématérialisées, indique que :

Article 8. « Admissibilité et valeur probante d'un message de données.

2 - Une information présentée sous la forme d'un message de données se voit accorder la force probante voulue. Lors de l'évaluation de la force probante d'un message de données, il est tenu compte de la fiabilité du mode de création, de conservation ou de communication du message de données, de la fiabilité du mode de préservation, de l'intégrité de l'information, de la manière dont l'utilisateur a été identifié et de tout autre facteur pertinent. »

Quels sont les moyens à mettre en œuvre qui seraient aptes à donner les garanties évoquées dans ces textes ?

De juridique, le problème de la preuve devient technique.

Quel serait du point de vue de la preuve le système idéal ?

En premier lieu, le système devrait être conçu de manière à donner des garanties sur son bon fonctionnement. Les juges accorderaient plus volontiers leur confiance à des enregistrements effectués dans les situations où le système mis en place est convenablement organisé, ou encore à des documents de sortie d'ordinateur édités régulièrement[550]. Une analyse de la jurisprudence en matière d'appareils de mesure tend à démontrer que les juges s'appuient sur la fiabilité de l'appareil utilisé pour apprécier la vraisemblance de la créance réclamée[551].

Chaque fois qu'il y a traitement informatique de masse, toutes les situations identiques sont traitées de la même manière, et il est peu probable que l'on ait reçu un traitement particulier[552].

Une sauvegarde systématique de toutes les opérations devrait dans cette perspective être mise en place.

Cependant, le stockage systématique n'est pas suffisant : les données sauvegardées peuvent être modifiées, volontairement ou non, et les altérations ne peuvent pas être détectées. Les sauvegardes devraient donc en second lieu être effectuées sur un support irréversible. On peut utiliser par exemple des disques optiques non réinscriptibles.

Toutefois, il reste possible d'effectuer des copies des données ainsi inscrites sur un support non réinscriptible : s'agissant de données numériques, il n'est pas possible de détecter les copies qui auraient été effectuées. Il faudrait donc en troisième lieu que le support permette de détecter le nombre de lecture des données enregistrées.

Le système devrait en quatrième lieu permettre de connaître la date d'émission d'un document et de s'assurer qu'il a été reçu sans modifications qui porteraient atteinte à son intégrité.

---

[549] Projet de loi-type sur les aspects juridiques de l'échange de données informatisées et des moyens connexes de communication des données, 28e session, 2-26 mai 1995.

[550] Jérôme Huet, Formalisme et preuve en informatique et télématique : éléments de solution en matière de relation d'affaires continues ou de rapports contractuels occasionnels, JCP éd. G 1989, I, 3 406, n° 1.

[551] Daniel Ammar, Preuve et vraisemblance, contribution à l'étude de la preuve technologique, RTD Civ. 1993,p.499.

[552] Hervé Croze, Informatique preuve et sécurité, D 1987.167, n° 9.

Il a par exemple été jugé que le simple fait de répertorier des documents de « confirmation de commande » ne faisait pas preuve de leur envoi et en tout cas pas à une date donnée[553].

Sur l'Internet, il est possible de s'assurer de l'émission, de la réception et de l'intégrité d'un message transmis en ayant recours à des procédés de cryptographie[554].

Enfin, ces précautions n'empêcheront jamais que des défaillances puissent survenir : une erreur au niveau de l'émission, une panne des moyens de communication est toujours susceptible de se produire. Le degré zéro de sécurité n'existe pas.

En outre, la preuve d'une défaillance est difficile à rapporter, surtout si l'on ne possède pas la maîtrise technique du système.

Pour certains, « il existe aujourd'hui des systèmes informatiques fournissant une force probante supérieure sur le plan technique, au papier. On passe à un système de preuve probabiliste, dans lequel la force probante d'une preuve est inversement proportionnelle à sa probabilité de fraude »[555].

En pratique, aucun système ne remplit toutes les conditions examinées. Si le bon fonctionnement technique du système est en général assuré, l'utilisation de supports non réinscriptibles n'est pas systématique.

On n'exige pas toujours de l'écrit lui-même autant de garanties : un faux peut être réalisé, une lettre simple n'offre pas de certitude quant à sa date d'envoi et de réception, on peut toujours soutenir qu'un lettre recommandée était vide, antidater un acte. Il convient de souligner également que les manipulations volontaires des données numériques exigent un degré de compétence d'autant plus grand que le système est complexe : du point de vue juridique, ces manipulations constituent l'infraction de faux.

En effet, aux termes de l'article 441-1 du Code pénal :

"Constitue un faux toute altération frauduleuse de la vérité de nature à causer un préjudice et accomplie par quelque moyen que ce soit, dans un écrit ou tout autre support d'expression de la pensée qui a pour objet ou qui peut avoir pour effet d'établir la preuve d'un droit ou d'un fait ayant des conséquence juridiques. »

Cette référence à « tout autre support d'expression de la pensée » inclut fonctionnement d'un système de traitement automatisé de données, introduction ou suppression frauduleuse de données dans un système[556].

Reste le cas des manipulations involontaires, des défaillances du système.

L'argument du dérèglement du système peut toujours être invoqué et être accueilli par un juge.

Par exemple, la Cour d'appel de Paris a refusé d'imputer au client d'une banque les retraits effectués auprès d'un distributeur avec sa carte prétendue volée et son numéro de code secret, au motif qu'« il n'est pas exclu que par suite d'une défaillance du système de sécurité du distributeur celui-ci puisse fonctionner à l'aide de la seule carte sans le secours du numéro de code personnel »[557]. La jurisprudence ultérieure a évolué et reconnaît la valeur de l'utilisation simultanée de la carte et du numéro de code secret[558].

En matière de facturation téléphonique, une décision de la Cour de cassation du 28 mars 1995[559] a admis la présomption résultant de l'enregistrement de communications, confirmée

---

[553] Lyon 10 avril 1987, Sté Résistub c/Sté Pachod, cité par Lamy informatique 1996, n°2407.
[554] Voir supra
[555] Alain Bensoussan, Contributions théoriques au droit de la preuve dans le domaine informatique : aspects techniques et solutions juridiques, Gaz. Pal. 1991, 2, p.362.
[556] Voir supra
[557] D 1981.369, note C.Gavalda.
[558] Pau 17 octobre 1984, D 1985, I.R.343 ; Paris 15e Ch. B 29 mars 1985, D 1986, I.R.327.
[559] Civ. 1re, Sté France Télécom c/ Berthe, JCP éd. G 1995, II, 22539.

par trois enquêtes techniques. L'abonné avait fait état de la possibilité d'un branchement clandestin et d'anomalies. La Cour de cassation a considéré que cela n'était pas suffisant pour mettre en doute cette présomption.

La force probante des documents fournis repose sur la confiance apportée au système. On passerait ainsi d'un problème de preuve à un problème de responsabilité.

Certains juristes préconisent une prise en charge des risques par une assurance prise par l'organisme qui met à disposition du public un système de transmission d'information en liaison avec son activité[560].

Pour que le commerce électronique se développe, une organisation des échanges électroniques doit être mise en place.

Des EDI aux tiers certificateurs

Les EDI

L'EDI[561] ou Echanges de Données Informatisées peut se définir comme le transfert électronique de données commerciales et administratives sous la forme d'un message normalisé. L'objectif est de développer un système servant à l'échange national et international de données commerciales.

Les grandes entreprises vont échanger des documents commerciaux avec leurs partenaires, leurs fournisseurs. Elles y gagnent en rapidité, économie, qualité et efficacité des communications de données informatisées.

Les EDI ont donné lieu à l'établissement de réseaux informatiques et de normes de communication de données sectorielles (par exemple secteur automobile, agro-alimentaire, transport aérien, réseau SWIFT des banques) puis multisectorielles.

Juridiquement, la mise en place d'un système d'EDI s'accompagne d'un contrat appelé « accord d'interchange » et destiné à régler les relations entre les partenaires utilisateurs de l'EDI. L'accord va comporter une partie technique, une partie relative à la sécurité des échanges de données ainsi qu'une partie juridique qui réglera notamment, en raison de l'absence de documents écrits signés originaux, les questions relatives à la preuve : validité et formation du contrat, admissibilité et valeur probante des messages EDI, ainsi que les questions juridiques soulevées par les contrats entre absents. Pour guider les entreprises dans la rédaction des contrats d'interchange, les organismes nationaux et internationaux ont publié de nombreux rapports et élaboré des contrats-types[562].

Les EDI ont suscité énormément d'intérêt. En France, une loi du 29 décembre 1990[563] est venue autoriser la transmission télématique des factures à condition qu'une autorisation préalable soit obtenue de l'administration fiscale et que soit respecté un certain nombre de procédures de contrôle[564].

---

[560] Jérôme Huet, Formalisme et preuve en informatique et télématique : éléments de solution en matière de relation d'affaires continues ou de rapports contractuels occasionnels, JCP éd. G 1989, I, 3 406, n°8.

[561] Il existe de nombreux articles et documents sur les EDI. Voir par exemple, outre les articles cités : Jérôme Huet, Aspects juridiques de l'EDI, D 1991.181 ; Thierry Piette-Coudol, L'échange de données informatisé, Gaz. Pal. 1991, 2, 551 ; Anne de la Presle, L'administration et l'échange de données informatisées, AJDA 1992, p.707.

[562] Voir par exemple : recommandation du 19 octobre 1994 concernant les aspects juridiques de l'échange de données informatisées, JOCE 28 décembre 1994, n° L338 avec en annexe l'accord type européen; CCI, Règles de conduite uniformes pour l'échange de données commerciales par télétransmission; contrat-type d'interchange EDI du Centre international de recherches et d'études du droit de l'informatique et des télécommunications.

[563] Loi de finances rectificative 1990 n°90-1169, article 47, JO du 30 décembre 1990.

[564] Voir Thierry Piette-Coudol, Le remplacement de l'écrit par un message électronique : le cas de la facture, Gaz. Pal. 1992.2.804.

L'article 4 de la loi du 11 février 1994[565], dite loi Madelin, autorise la mise en place de procédures de déclaration des entreprises aux administrations par voie électronique dans des conditions fixées par contrat entre l'entreprise et l'administration[566]. En matière douanière, on peut citer un arrêté du 19 décembre 1994[567], portant approbation du cahier des charges pour la transmission par voie informatique de la déclaration d'échanges de biens entre états membres de la Communauté européenne : sur autorisation et dans le cadre d'une convention particulière, les entreprises peuvent transmettre leurs déclarations d'échange de biens à l'administration des douanes par voie informatique.

Cependant, le système des EDI paraît inadapté à l'Internet.

D'un point de vue technique, les EDI sont utilisés aujourd'hui en réseaux fermés, c'est-à-dire en réseaux privés non ouverts aux tiers.

Or l'Internet est un réseau ouvert qui n'est soumis à aucun contrôle en limitant l'accès.

En réalité, les entreprises sont peu nombreuses à utiliser les EDI. L'implantation d'un réseau EDI reste une opération coûteuse, réservée à de grandes entreprises. Pour augmenter l'accessibilité du commerce électronique au plus grand nombre d'entreprises, les EDI n'apparaissent pas comme le moyen approprié[568].

En outre, les EDI supposent une relation commerciale préexistante entre les partenaires qui l'utilisent. Les EDI ne sont donc pas adaptés aux relations commerciales isolées, de premier contact, ou de faible importance.

L'accord d'interchange est un document complexe et pointu qui peut s'avérer trop compliqué[569].

Des études ont ainsi montré que la majorité des activités par EDI aux Etats-Unis était menée en dehors de tout accord d'interchange, et ce y compris dans des sociétés multinationales[570].

D'autres instruments juridiques sont recherchés afin de s'exonérer de la lourdeur de l'accord d'interchange.

Les Editerms[571]

Les Editerms sont inspirés des Incoterms établis par la CCI, qui a codifié aux fins d'interprétation uniforme les usages du commerce international[572]. Les Editerms sont un document écrit et extérieur qui émane des milieux professionnels auxquels se réfèrent les partenaires.

Afin d'établir et d'apporter un mécanisme permettant le commerce électronique sécurisé en environnement ouvert, la CCI a mis en place un groupe de travail qui doit élaborer un répertoire d'Eterms (Electronic Terms) composé de termes de deux sortes :

- ceux provenant des utilisateurs du répertoire ;
- ceux provenant d'experts et constituant les règles de droit les plus utiles au commerce électronique.

---

[565] Loi n° 94-126 du 11 février 1994 relative à l'initiative et à l'entreprise individuelle.

[566] Voir Anne de la Presle, Licéité des téléprocédures : déclaration d'entreprises à organismes publics, Droit de l'Informatique et des Télécoms 1994/2, p.84.

[567] JO du 27 décembre 1994.

[568] David Masse, L'autoroute de l'information : convergence du droit et de la technologie, intervention dans le cadre d'une conférence organisée par l'Association québécoise pour le développement de l'informatique juridique, 10 novembre 1995, disponible à : <http://www.droit.umontreal.ca/AQDIJ/Colloque_10_11_95/Masse/aqd95.html 11_95/Masse/aqd95.html>.

[569] Nicolas Viallard, EDI : les accords d'interchange, Mémoire DEA, Montpellier, 1993, p.57.

[570] Idem, p.23.

[571] Sur les Editerms voir : Caprioli, Aspects juridiques du concept d'Editerms, Droit de l'Informatique et des Télécoms 1994/1, p. 14 ; Nicolas Viallard, préc., p. 60 et suivantes.

[572] Voir le Guide des Incoterms, publié par la CCI, site Web : <http://www1.usa1.com/~ibnet/icchp.html>.

Il pourra être fait référence à ces Eterms sur les pages du service Web des entreprises utilisatrices de ce système[573]. Cependant l'opération relèvera toujours par définition du contrat-type. La question de la manifestation de volonté du cocontractant d'être engagée reste posée : le contrat préétabli ou de référence doit nécessairement être repris par les consentements individuels des parties[574]. Ces Eterms s'avéreront sans doute utiles pour préciser les contenus des conditions contractuelles mais laissent entier le problème de l'échange des consentements lui-même, par des personnes identifiées, à la base de la formation du contrat.

Le recours à des contrats-types n'est donc pas suffisant et la CCI a l'intention de mettre en place un système de signature électronique ainsi que l'intervention d'un tiers certificateur afin d'authentifier les échanges commerciaux.

La signature électronique

Le recours aux procédés de cryptographie à clé publique permet la création de signatures électroniques pratiquement infalsifiables[575].

Dans un système de cryptographie par clé publique, un message crypté avec l'une des deux clé ne peut être décrypté qu'avec l'autre et *vice versa*. La clé privée ne peut pas être recomposée à partir de la clé publique.

Comment ce système permet-il de gérer une signature ?

Une personne A envoie un message par courrier électronique à une personne B. A crypte son message avec une clé privée connue d'elle seule. A cette clé privée correspond une clé publique. Le message crypté avec la clé privée de A ne pourra être lu qu'en utilisant la clé publique de A. En outre, une empreinte numérique est calculée à partir du texte même du message. Si le texte du message a été altéré, la valeur générée par le logiciel du destinataire ne sera pas identique à l'empreinte numérique émise par le logiciel de A.

Toutes ces opérations complexes peuvent être réalisées automatiquement par un logiciel de courrier électronique, auquel aura été incorporé un logiciel de cryptage.

Ce système permet de s'assurer, d'une part, de l'identité de l'expéditeur du message, et d'autre part, de l'absence d'altération en transit : il y a création d'une signature électronique.

La reconnaissance juridique de la signature électronique

La notion de signature désigne à la fois un signe permettant d'identifier une personne physique et le fait d'apposer ce signe sur un support contenant des informations [576]. Traditionnellement cette signature est manuscrite. Peut-on admettre la validité d'une signature dématérialisée ?

Certains juristes ont souligné que la signature n'est nulle part définie en droit français et qu'elle n'est qu'un procédé d'authentification manifestant l'adhésion de celui qui en use[577].

Des législations étrangères ont défini la signature en des termes suffisamment larges pour permettre de reconnaître la validité de la signature électronique. Par exemple, le Code civil luxembourgeois[578], ou encore l'article 2827 du Code civil du Québec :

« La signature consiste dans l'apposition qu'une personne fait sur un acte de son nom ou d'une marque qui lui est personnelle et qu'elle utilise de façon courante, pour manifester son consentement ».

---

[573] Stéphane Lefer, Sécuriser le commerce électronique, Expertises n° 165 juin 1996, p. 212.
[574] Caprioli, Aspects juridiques du concept d'Editerms, Droit de l'Informatique et des Télécoms 1994/1, p.20.
[575] Voir supra p.
[576] Hervé Croze, Informatique, preuve et sécurité, D 1987.165, n° 17.
[577] J. Larrieu, Les nouveaux moyens de preuve : pour ou contre l'identification des documents informatiques à des écrits sous seing privé ? Cahiers Lamy informatique, novembre 1988 (H), p.8.
[578] Lamy informatique n° 2402.

L'Etat américain de l'Utah, qui a adopté une loi relative à la signature électronique, l'Utah Digital Signature Act (1996)[579], modifiant le titre 46, chapitre 3 du Code de l'Utah, définit la signature électronique par rapport au procédé technique utilisé.

« Lorsqu'une règle de droit requiert une signature, ou prévoit certaines conséquences en l'absence de signature, cette règle est satisfaite par le recours à une signature électronique si :

1- Cette signature électronique est vérifiée par référence à une clé publique mentionnée dans un certificat valide émis par une autorité de certification »[580].

Il est plus facile d'imiter une signature manuscrite que de découvrir le code secret à quatre chiffres correspondant à une carte bancaire (0,03% de chances de découvrir le code secret avec 3 essais[581]) ou encore de décrypter une clé privée.

Selon la longueur de la clé, soit il est nécessaire de recourir à des ordinateurs très puissants, soit cela est impossible en l'état des techniques actuelles.

Cependant, d'autres auteurs considèrent qu'une signature électronique ne doit pas être considérée comme l'équivalent d'une signature manuscrite car l'on ne peut pas s'assurer de la présence du signataire, élément essentiel de la signature : on ne sera jamais sûr que derrière un terminal informatique se trouve l'individu qu'on a pu identifier[582].

La jurisprudence française a admis la validité de la signature électronique donnée par l'utilisation simultanée d'une carte à microprocesseur et d'un code secret[583], mais par le moyen de la liberté des conventions de preuve.

La question de la validité d'une signature électronique en l'absence de convention préalable reste posée en droit français.

Les tiers certificateurs

Les procédés de cryptographie à clé publique fournissent une solution au problème d'identification des interlocuteurs et même de confidentialité des messages échangés en réseau ouvert. Ce système peut nécessiter l'intervention d'un tiers : le tiers certificateur, dont le rôle va consister à administrer et publier les clés publiques[584].

Ce tiers certificateur va permettre de s'assurer qu'une clé publique est bien celle du correspondant, et donc de vérifier son identité et ses pouvoirs. En l'absence d'un réseau de certification, la question des échanges entre personnes qui ne sont jamais rentrées en relation auparavant reste entière : comment ces personnes vont-elles échanger de manière sécurisée leurs clés publiques, qui garantira que la clé donnée est bien celle de la personne annoncée et non pas celle d'un imposteur. Sans certitude sur l'identité du cocontractant, la validité de la signature et donc de la transaction peut être contestée. Il existe actuellement des serveurs de clés publiques[585], mais qui ne fournissent pas toujours de garanties quant à la vérification de l'identité des déposants.

Pour que le recours au système de cryptage à clé publique offre une sécurité juridique, des réseaux de certification doivent être mis en place.

---

[579] Sur le Digital Signature Act de l'Utah, voir le site Web Utah Digital Signature Law : <http://www.gov.state.ut.us/ccjj/digsig/>.

[580] "Where a rule of law requires a signature, or provides for certain consequences in the absence of a signature, that rule is satisfied by a digital signature, if : 1. That digital signature is verified by reference to the public key listed in a valid certificate issued by a licensed certification authority".

[581] Isabelle Pottier, La preuve dans les transactions financières à distance, Banque mars 1996, n° 568, p. 71.

[582] Etienne Dubuisson, la personne virtuelle : propositions pour définir l'être juridique de l'individu dans un échange télématique, Droit de l'Informatique et des Télécoms 1995/3, p. 8.

[583] Montpellier 9 avril 1987, JCP éd. G 1988, II, 20 984 ; Civ. 1re 8 novembre 1989, D 1990.369.

[584] Sur le tiers certificateur voir : David Masse, L'autoroute de l'information : convergence du droit et de la technologie, intervention dans le cadre d'un conférence organisée par l'Association québécoise pour le développement de l'informatique juridique, 10 novembre 1995, disponible à : <http://www.droit.umontreal.ca/AQDIJ/Colloque_10_11_95/Masse/aqd95.html> ; M. Froomkin, The Essential Role of Trusted Third Parties in Electronic Commerce, <http://www.law.miami.edu/~froomkin/>, 2 avril 1996.

[585] Pour obtenir une liste de tiers certificateur, activer la fonction "Options", puis "Securities Preferences", puis "Sites Certificates" du logiciel de navigation de Netscape, version 3.0.

Le tiers certificateur est un organisme, public ou privé, qui émet des certificats électroniques. Le certificat est un registre informatique revêtu d'une signature électronique qui identifie l'émetteur du certificat, identifie le souscripteur et donne sa clé publique. Il s'agit d'une sorte de carte d'identité électronique qui serait émise par un tiers indépendant et neutre. La signature électronique correspondant à un certificat est considérée appartenir à la personne mentionnée dans le certificat.

Un certificat peut permettre de vérifier l'identité d'une personne, mais également ses pouvoirs et sa capacité, ses qualifications professionnelles (par exemple il sera possible de vérifier si la personne est bien médecin, avocat, etc.), le pouvoir d'engager une société.

A l'heure actuelle, seul un Etat a tenté de fournir un cadre légal aux tiers certificateur, l'Etat américain de l'Utah, qui a adopté en 1995, modifié en 1996, l'« Utah Digital Signature Act »[586].

Des projets seraient en cours dans d'autres Etats américains comme la Californie. Ces projets américains sont inspirés d'un rapport diffusé par l'Information Security Commitee de l'American Bar Association (association de barreaux américains) : Digital Signature Guidelines[587].

Plusieurs questions se posent en ce qui concerne ces tiers certificateurs.

Quelle profession sera la plus apte à remplir ce rôle ?

Société privée, banque, assureurs, notaires ? Va-t-on voir l'émergence d'une nouvelle profession ? Les professions réglementées comme les avocats, les notaires, les médecins devront peut-être mettre en place leur propre système de certification.

Plusieurs réseaux seront sans doute créés en fonction des besoins.

Le tiers certificateur est un métier nouveau. Son rôle est différent de celui du banquier, il ne gère pas de fonds, différent de celui de l'assureur, il ne gère pas de risque. Il se porte garant de l'identité et de la capacité d'une personne en vue de valider une transaction.

Sa fonction pourrait ressembler à celle du notaire qui a pour fonction de « recevoir les actes et contrats auxquels les parties doivent ou veulent faire donner le caractère d'authenticité attaché aux actes de l'autorité publique, et pour en assurer la date, en conserver le dépôt, en délivrer des grosses et expéditions » (c'est-à-dire en délivrer des originaux et copies certifiées)[588].

Certains emploient d'ailleurs le terme de « notaire électronique » pour désigner ces tiers certificateurs.

A la différence du notaire, le tiers certificateur n'est pas un dépositaire d'un acte ou d'un contrat. Il permet de s'assurer qu'une clé publique est bien celle d'un correspondant. Le notaire a directement une fonction de conservation de la preuve organisée par la loi. Il possède un monopole pour certains contrats pour lesquels son concours est obligatoire. La fonction du notaire français est étroitement liée à notre système de la preuve. Le tiers certificateur est un nouveau métier résultant du bouleversement en matière de preuve que créent les transactions immatérielles.

Compte tenu de la nouveauté de la fonction de tiers certificateur, certains estiment que la mise en place d'un réseau de tiers certificateur nécessite un statut légal pour définir leurs obligations et leurs responsabilités[589].

L'organisation du système peut également se faire dans un cadre contractuel.

---

[586] Utah Code Annotated, Title 46, chapitre 3, Voir sur cette loi le site : <http://www.gov.state.ut.us/ccjj/digsig/>.

[587] Disponible à : <http://www.gov.state.ut.us/ccjj/digsig/> ; pour le commander : < http://www.intermarket.com/ecl/>

[588] Article 1er de l'Ordonnance n°45-2590 du 2 novembre 1945 relative au statut du notariat.

[589] H. Henry Perritt, Cyberpayment Infrastructure, 1996 Journal of Online Law, art.6, par.2,< http://warthog.cc.wm.edu/law/publications/jol/>.

L'étendue des obligations et de la responsabilité encourue par ces tiers certificateurs reste ouverte.

Quelle responsabilité encourra un tiers certificateur si un certificat erroné est émis ?

En cas de perte de la clé privée, d'un changement dans les informations portées sur le certificat, ledit certificat devra être révoqué. Les modalités et les effets de cette révocation devront être précisés. Quelle sera l'étendue de la responsabilité du tiers certificateur si une personne utilise une fausse identité pour se procurer un certificat ? Sur ce point, une analogie peut être faite avec la responsabilité du banquier en matière d'ouverture de compte.

La jurisprudence, avant que la loi n'intervienne en ce sens, avait consacré l'idée que le banquier, avant d'ouvrir un compte, devrait procéder à certaines vérifications concernant le postulant, sous peine d'engager sa responsabilité envers les tiers, si le nouveau client utilisait son compte pour leur porter préjudice.

Le banquier doit vérifier l'identité du postulant au moyen d'un document officiel dont il enregistre les caractéristiques, son adresse, ainsi que ses pouvoirs[590].

La réflexion sur les tiers certificateur commence à peine en France.

Outre ces questions sur le statut et la responsabilité des tiers certificateurs, l'usage généralisé de la cryptographie à clé publique comme technique permettant d'assurer la sécurité du commerce électronique se heurte à des obstacles législatifs.

En France, tant que la loi sur la cryptographie ne sera pas assouplie, il sera difficile de pouvoir l'utiliser. La loi du 26 juillet 1996 ne change pas fondamentalement le système antérieur. Les procédés de cryptographie à des fins d'authentification peuvent être librement utilisés, mais à condition qu'ils ne permettent pas d'assurer des fonctions de confidentialité. Or les logiciels de cryptage utilisant les systèmes à clé publique ont des fonctions de confidentialité.

Les réglementations à l'exportation des procédés de cryptographie sont généralement restrictives. Or, il est indispensable que les deux partenaires utilisent le même logiciel de cryptage ou un logiciel compatible. L'absence de standard international légalement admissible gêne le recours à ce procédé dans les échanges internationaux, et encore une fois plus particulièrement en France.

Le seuil de rentabilité de l'activité de tiers certificateur devra également être déterminé.

La valeur probante du courrier électronique

En attendant que ces réseaux de tiers certificateurs soient mis en place, s'ils le sont un jour, que l'usage de la cryptologie aux fins d'authentification et d'intégrité puisse être généralisée, les facilités offertes par les nouvelles techniques de communication vont être de plus en plus utilisées par les particuliers et les entreprises sans que ces acteurs se posent nécessairement la question de la sécurité juridique des moyens utilisés.

Il s'agit d'apprécier en fonction de l'importance d'une transaction donnée le seuil de risque acceptable.

Une comparaison peut être effectuée avec la télécopie, dont l'usage est aujourd'hui courant, alors qu'elle ne constitue pas d'un point de vue juridique un écrit original signé.

La télécopie présente des faiblesses techniques :

Des erreurs de transmission peuvent survenir. Un requérant avait ainsi envoyé son mémoire à une Cour administrative d'appel et produisait un reçu d'émission du télécopieur. Mais le mémoire n'avait pas pu être reçu par son destinataire en raison d'un défaut

[590] Responsabilité civile du banquier en matière de compte, Juriscl. Banque, Fasc. 150, n° 9 et suivants.

d'approvisionnement en papier du récepteur. Le mémoire a été considéré comme envoyé hors délai[591].

Les coordonnées de l'expéditeur, le numéro de la ligne appelante, la date d'émission peuvent être aisément modifiés[592].

Il est techniquement possible d'éditer un faux accusé de réception.

Il est possible de falsifier l'original ou le document reçu.

L'avis de réception ne marque pas la réception de l'information par le destinataire, mais la réception matérielle par l'appareil du correspondant.

La télécopie est malgré ces inconvénients un instrument privilégié des échanges d'informations dans la vie des affaires, et chaque année plus de 3 millions de documents sont transmis au moyen de télécopieurs[593]. Les télécopies sont souvent admises à titre de preuve dans les relations commerciales, dès lors qu'aucune forme particulière n'est exigée.

Dans plusieurs décisions, un échange de télécopie a été estimé suffisant pour engager les parties[594] :

- un arrêt de la Cour d'appel de Paris du 27 février 1995 a ainsi considéré qu'il y avait eu conclusion d'un contrat concernant l'organisation d'un voyage à l'étranger, en l'absence de contrat signé dès lors qu'il y a eu un échange de télécopies manifestant l'accord des parties ;
- dans un affaire où le retrait d'une offre de promesse de cession d'actions avait été transmise par télécopie, la Cour d'appel de Paris a reconnu la validité du retrait de l'offre (27 mai 1994) ;
- un arrêt de la Cour d'appel de Lyon (18 avril 1994) a considéré que la preuve de la vente de boulons était rapportée lorsque la commande passée par télécopie est confirmée par un télex ;
- la priorité de l'acheteur d'un bateau a été rapportée par la production d'une télécopie adressée au premier acheteur (Aix-en-Provence 27 mars 1991).

On peut également citer des affaires où des photocopies, en l'absence de l'original, ont été admises à titre de preuve .

Une décision a ainsi admis que la photocopie d'une reconnaissance de dette écrite et signée par l'emprunteur, qui ne conteste ni l'existence de l'acte, ni la conformité de la photocopie à l'original, valait commencement de preuve par écrit[595].

Cependant, si la photocopie est contestée, elle perd sa valeur probante.

Dans une affaire où la signature apposée sur un document produit en photocopie a été contestée, la Cour de cassation a considéré qu'une photocopie n'a pas, par elle-même, de valeur juridique, et que la charge de la preuve n'incombe pas à celui qui dénie sa signature[596].

D'une manière générale, l'acceptation de la valeur probante des télécopies par le juge va dépendre des circonstances et n'est pas garantie. Un arrêt de la Cour d'appel de Paris a considéré qu'une télécopie n'établissait pas le contrat de transport entre commerçants[597].

Du point de vue de la preuve, la télécopie reste fragile et subordonnée à l'absence de contestation par les parties.

---

[591] CAA Nancy 8 avril 1993, D 1994 som.com.288.
[592] Sur les problèmes liés à l'identification de l'expéditeur, voir JO ANQ 1er avril 1996, p. 1804.
[593] L.Lautrette, Télex, télécopie, télégramme : valeur juridique et force probante, Petites Affiches, 10 mai 1996,n°57, p. 5.
[594] Jean Michel Hocquard, Télécopie et preuve, Petites Affiches, 29 mai 1996, n°65, p. 24.
[595] Civ. 1re 14 février 1995, D 1995.340 ; Voir aussi Civ. 1re 30 juin 1993, Gaz. Pal. 23 octobre 1993, p.20.
[596] Com. 15 décembre 1992, Bull. Civ. IV, n°419.
[597] Décision citée par Jean-Michel Hocquard, préc.

En pratique, les contestations portent davantage sur le contenu de l'accord et ses conditions d'exécution que sur l'existence même de la transaction conclue par télécopie, dont le principe n'est pas remis en cause[598].

Les questions soulevées aujourd'hui par l'utilisation massive de la télécopie par les entreprises vont se poser dans les mêmes termes en ce qui concerne le courrier électronique.

D'ores et déjà des millions de messages sont échangés par ce biais chaque jour, et les facilités pratiques qu'il offre devrait en faire un moyen de communication de plus en plus répandu.

On peut sans doute lui prédire le même succès à terme que la télécopie, qu'il pourrait même supplanter et en tout cas concurrencer sérieusement.

Dans les domaines où la preuve est libre, notamment dans les relations commerciales, le courrier électronique pourra être admis à titre de preuve.

La question de la force probante de ces courriers dépendra des contestations qui pourront être soulevées par les parties, notamment quant à leur émission, à leur réception, et à l'identité de l'auteur du message. Le courrier électronique présente les mêmes possibilités de manipulation que le télécopieur.

Le courrier électronique présente l'inconvénient par rapport à la télécopie de ne pas faire apparaître la signature de l'auteur du message.

Toutes les falsifications opérées dans un courrier électronique relèvent du délit de faux en écriture privée ainsi que des infractions prévues en matière de fraude informatique[599].

Une telle manipulation apparaîtra si les deux messages ne comportent pas les mêmes mentions ou des mentions incompatibles entre elles. Bien que cela puisse arriver, il est cependant rare que le contenu du message soit modifié pendant son transfert. Lorsque la boîte aux lettres du destinataire est inaccessible ou que ses coordonnées ont été mal précisées, le courrier est retourné à son expéditeur.

Les entreprises doivent faire preuve de prudence dans l'utilisation du courrier électronique en vue d'éviter les contestations ultérieures. S'agissant d'un procédé nouveau, il pourrait être accueilli avec circonspection par des juges qui n'auront pas nécessairement eu l'occasion de se familiariser avec ce procédé. Des juges américains ont ainsi refusé d'admettre à titre de preuve un message de courrier électronique échangé entre deux employés de Microsoft[600].

Les entreprises peuvent, par exemple, demander à leur correspondant de leur confirmer la réception du courrier électronique (ce qui en pratique ne prend que quelques secondes) organiser un archivage systématique de tous les courriers émis et reçus, et si possible une sauvegarde sur support irréversible, ou au moins éditer une impression du courrier électronique.

[598] Jean-Michel Hocquard, préc.
[599] Voir supra
[600] Monotype Corp. PLC v. International Typeface Corp. 43 F3d 443 (9th cir. 1994).

Troisième partie

Le paiement électronique

Jusqu'au siècle dernier, les paiements s'effectuaient avec des pièces et des billets. Aujourd'hui, une majorité de transactions est réglée par des chèques et virements de compte à compte : paiement des salaires, loyers, impôts, etc.

La carte de crédit a fait son apparition et tend de plus en plus à supplanter les paiements par chèque. Elle est couramment utilisée pour les retraits d'argent de son compte bancaire. Certains ont même évoqué l'arrivée d'une « société sans argent ». Nous n'en sommes pas encore là. Malgré le développement des systèmes de paiement électronique, une majorité de paiements interentreprises s'effectue par des transferts de fonds non électroniques. Les paiements en liquide représentent encore une partie importante des règlements effectués et les paiements par chèque n'ont pas disparu.[601]

Les paiements à travers un réseau informatique vont nécessairement s'effectuer de manière dématérialisée, sans support papier. Un système de paiement électronique simple et fiable doit être mis en place pour que le commerce électronique puisse démarrer sur l'Internet[602].

Les banques ont développé depuis les années 70 leurs propres réseaux internationaux de paiement électronique. Le plus connu est le réseau SWIFT (Society for Worldwide Interbank Financial Telecommunications)[603]. Cependant, il s'agit de réseaux propriétaires coûteux qui ne peuvent pas convenir pour des paiements de faible importance.

Au surplus, les banques se méfient d'un réseau ouvert comme l'Internet, non pensé pour véhiculer des informations financières en toute sécurité, mais conçu pour le libre échange d'informations non confidentielles.

La carte de crédit, massivement utilisée dans le monde entier, est un mode de paiement électronique, mais qui n'est pas adapté aux paiements sur l'Internet. En France, nous utilisons la Carte Bleue avec puce électronique incorporée. L'ordre de paiement est donné par le client qui saisit son code confidentiel sur un terminal spécifique. Il faudrait pour transposer ce système que l'ordinateur du client dispose d'un lecteur de carte, ce qui n'est pas très répandu. Il faudrait en outre que le commerçant ait passé un contrat avec un émetteur français.

Sur le plan juridique, l'ordre de paiement donné avec le seul numéro apparent de la carte en l'absence de signature ou de code confidentiel est révocable.

En effet, les contrats commerçants de cartes bancaires passés par les sociétés de vente à distance avec les émetteurs de cartes prévoient que le commerçant s'engage à assumer la responsabilité de tout débit erroné donnant lieu à contestation. Dans ce cas, le commerçant autorise expressément les banques ou organismes financiers à débiter d'office son compte du

---

[601] Secure International Payment and Information Transfer, Towards a Multi-Currency Electronic Wallet, Report for the Project CAFE, Frankfurt 1995, p.9.

[602] H. Henry Perritt, Cyberpayment Infrastructure, 1996 Journal of Online Law, art.6, par.2, <http://warthog.cc.wm.edu/law/publications/jol/>.

[603] Andreas Crede, Electronic Commerce and the Banking Industriy : The requirement and Opportunities for New Payment Systems Using the Internet, JCMC, Vol.1 N°3, December, 1995, Special issue on electronic commerce, <http://www.usc.edu/dept/annenberg/vol1/issue3/>.

montant de toute opération de paiement qui serait reprise ou contestée par écrit par le titulaire de la carte[604].

Dans une majorité de pays, un reçu est émis par le commerçant à partir de la carte de crédit, qui est ensuite signé par le client. Compte tenu du fait que la transaction est réalisée à distance, le commerçant ne peut pas obtenir de reçu signé de son client.

Dans une majorité de cas, y compris en France pour les opérations réalisées par Minitel, le paiement par carte est réalisé sur la seule indication du numéro de la carte bancaire. Une telle procédure ne donne aucune garantie quant à l'identification du donneur d'ordre. Les fraudes par utilisation abusive du numéro de carte apparent d'un tiers sont à craindre. L'interception du numéro de la carte pendant son transfert semble relever davantage du mythe que de la réalité (un escroc dépensera moins d'énergie en se procurant les numéros de carte par un moyen traditionnel : complicité avec l'employé d'un magasin, récupération des doubles des reçus des cartes des clients dans une poubelle, par exemple). Le risque existe cependant qu'un pirate accède à une base regroupant des milliers de numéros de cartes bancaires.

En d'autres termes, le risque de fraude résultant de l'utilisation d'un numéro de carte appartenant à un tiers est supporté par le commerçant. Le commerçant peut également craindre les fraudes de clients de mauvaise foi[605].

La solution serait la même dans d'autres pays comme les Etats-Unis[606]. Un paiement réalisé avec le seul numéro de carte présente de l'avis général une sécurité insuffisante.

Des procédures de télépaiement sécurisées en réseau ouvert doivent pouvoir être mises en place. Vers le milieu de l'année 1996, plusieurs systèmes étaient encore en cours d'expérimentation ou de phase de test. Il existe une concurrence entre des solutions différentes émanant d'entreprises venant d'horizons variés. Il est encore trop tôt pour savoir quels systèmes seront adoptés par les utilisateurs, lesquels disparaîtront, si une des solutions préconisées va devenir un standard de fait et éclipser ses concurrentes ou si elles vont coexister.

Une procédure de télépaiement doit prendre en compte un certain nombre d'objectifs que je vais rappeler avant d'examiner les solutions préconisées ou en développement.

Le cadre juridique du télépaiement sera ensuite étudié.

Les objectifs d'une procédure de télépaiement

La première condition que devra remplir la procédure de télépaiement est d'être sécurisée. Sécurité pour protéger aussi bien le client, les institutions financières que le commerçant. La sécurité concerne la fiabilité du système de paiement contre les défaillances techniques, les fraudes en tous genres et les contrefaçons.

La sécurité est également juridique : le client doit pouvoir identifier le vendeur, le vendeur s'assurer de l'identification du donneur d'ordre, vérifier le cas échéant ses pouvoirs, éventuellement sa nationalité en raison de certaines réglementations à l'exportation. En ce qui concerne le paiement proprement dit, le client va vouloir un système simple, intégré à la phase de commande, utilisé par le plus grand nombre de commerçants. Il va vouloir également qu'un recours en cas de paiement non autorisé et de perte soit prévu. Dans certains cas, il souhaitera rester maître de l'opération et être en mesure de confirmer la transaction.

---

[604] Voir par exemple : article 4 - Contestation d'une opération de paiement par le titulaire de la carte des conditions particulières de fonctionnement du système de paiement par carte dans le cadre de la vente par correspondance, par téléphone ou par vidéotexte du groupement des cartes bancaires "CB".

[605] Olivier Itéanu, Internet et le Droit, Aspects juridiques du commerce électronique, éditions Eyrolles 1996, p.136.

[606] O. Hance, Business et Droit d'Internet, Best Of Editions 1996, p. 158; Aspects juridiques de la banque à domicile et du télépaiement, rapport du groupe de travail du Comité consultatif du Conseil national du crédit, Droit de l'Informatique et des Télécoms 1993/3, p.93, note 54.

Le commerçant cherchera quant à lui à se prémunir contre les révocations abusives des ordres de paiement et à ce que le coût de traitement du télépaiement soit adapté aux transactions de petit montant.

La sécurité est la principale préoccupation des organismes financiers, avec la rentabilité du système.

Avec la collecte croissante d'informations personnelles sur les consommateurs, une nouvelle préoccupation apparaît : celle du respect de la vie privée. Certains commencent à trouver désagréable que tous nos faits et gestes puissent être tracés et conservés par un nombre de plus en plus grand d'organismes : banques, établissements émetteurs de cartes de crédit, sociétés diverses[607], etc.

Les procédés de paiement électronique

Il existe quatre types d'approches à la question du paiement électronique

L'adaptation du système des cartes de crédit

Des projets sont à l'étude afin de permettre le paiement par carte de crédit sur l'Internet de manière sécurisée. Les inconvénients des paiements par carte de crédit ont déjà été examinés ci-dessus. Néanmoins, les cartes de crédit présentent l'avantage d'être déjà utilisées dans le monde entier.

Le 1er février 1996, Visa et Mastercard ont publié un communiqué de presse pour annoncer la mise au point d'un standard technique commun pour les paiement par cartes de crédit, appelé Secure Electronic Transactions (SET). D'autres entreprises américaines participent au projet : GTE, IBM, Microsoft, Netscape, SAIC, Terisa Systems et Verisign. Auparavant, Visa et Mastercard avaient développé des spécifications chacune de leur côté : Secure Electronic Payment Protocol (SEPP)[608] pour Mastercard et Secure Transaction Technology (STT)[609] pour Visa.

Des sociétés comme Microsoft et Netscape vont intégrer des fonctions qui permettront d'effectuer des transactions en utilisant ce standard dans les logiciels qu'elles vendent dans le monde entier.

L'idée de ce procédé, en simplifiant, est de remplacer le reçu délivré au client et sa signature par une signature électronique générée par des procédés de cryptographie à clé publique. La transaction comporte l'émission de certificats électroniques, et donc la mise en place d'une infrastructure de tiers certificateurs.

La monnaie électronique

L'idée est de développer un système de paiement qui fournira un équivalent électronique à l'argent liquide.

---

[607] Secure International Payment and Information Transfer, Towards a Multi-Currency Electronic Wallet, Report for the Project CAFE, Frankfurt 1995, p23.

[608] 3 novembre 1995, version 1.2.

[609] 26 septembre 1995, version 1.0.

La société hollandaise Digicash[610] fondée par le chercheur d'origine américaine David Chaum propose la mise en place d'un système de monnaie électronique pour laquelle les banques pourraient offrir une parité avec l'argent liquide classique.

Cette monnaie électronique est représentée mathématiquement par une suite de nombres. Ces nombres sont générés par des algorithmes sophistiqués. Chaque nombre contient la somme représentée, la signature de l'émetteur (la banque) et une partie de l'identifiant du compte du client, le tout crypté. Les nombres sont calculés de telle sorte à ne pouvoir être générés qu'une seule fois pour éviter les fraudes.

L'utilisateur doit disposer d'un compte dans une banque qui accepte de faire la conversion entre l'e-cash (nom donné à l'argent électronique généré par le système Digicash) et l'argent. Il retire de l'argent de son compte bancaire pour le mettre sur son compte e-cash. Le compte e-cash se trouve sur l'ordinateur du client.

Lorsque l'e-cash est utilisé auprès d'un commerçant pour effectuer un paiement, le commerçant vérifie auprès de la banque que l'e-cash est valable. Le commerçant a ensuite le choix entre demander la conversion en argent de l'e-cash reçu ou faire un dépôt sur son propre compte e-cash.

Le système présente l'originalité de permettre les transferts d'e-cash d'une personne à une autre. Cependant, à chaque opération, la validité de l'e-cash doit être confirmée par la banque : les e-cash reçus en paiement doivent être retournés à la banque, qui soit effectue la conversion sur le compte bancaire, soit émet de nouveaux e-cash. Le montant d'e-cash qui circule entre les personnes est donc connu de la banque.[611]

Le système de Digicash a la particularité de permettre l'anonymat du payeur qui n'a pas à révéler son identité au vendeur. Le système est conçu de telle sorte que les e-cash sont validés par la banque sans que la banque elle-même sache par qui et comment l'e-cash a été dépensé. Le principe utilise le concept de « blind signature » (signature aveugle), proposé par David Chaum[612]. La banque, en signant avec une clé secrète, valide l'e-cash, mais sans voir ce nombre, comme si elle signait quelque chose à travers du papier carbone sans voir ce qu'elle signe, tout en étant capable de vérifier plus tard qu'elle a bien signé.

En revanche, le montant perçu par chaque usager est connu de la banque.

A la différence de l'argent liquide, l'anonymat est à sens unique : lorsque la banque valide l'e-cash, elle a connaissance de l'identité de celui qui lui présente l'e-cash.

Tous les transferts d'e-cash sont enregistrés, de telle sorte qu'en cas de besoin, il est possible de retrouver la trace d'une transaction.

Une banque américaine, la Mark Twain Bank, permet depuis le 23 octobre 1995 de convertir des dollars en argent électronique généré par le logiciel de la société Digicash[613].

Pour utiliser ce système, il est nécessaire d'ouvrir un compte dans cette banque[614]. Le logiciel de Digicash permet de générer les e-cash. Le client transfère des fonds de son compte courant (le World Currency Access Account, WCA) sur son compte électronique (ou Ecash Mint) ou *vice versa*. A partir du compte Ecash Mint, le client génère avec le logiciel E-cash, de la monnaie électronique qu'il va utiliser chez les commerçants qui acceptent cette monnaie. Aujourd'hui, le commerçant doit lui-même avoir un compte chez la Mark Twain Bank, mais dans le futur, d'autres institutions pourraient prendre une licence e-cash, et les paiements d'un système à un autre seraient rendus possible[615].

---

[610] Site Web : <http://www.digicash.com>.
[611] An introduction to e-cash, <http://www.digicash.com/publish/ecash_intro/ecash_intro.html>.
[612] Blind Signatures for Untraceable Payments, Advances in Cryptology : Proceedings of CRYPTO'82, New York 1983,p.199-203.
[613] Jérôme Thorel, « Les dollars numériques de Mark Twain, entretien avec Frank Trotter, vice-président », *Planète Internet* n° 8 mai 1996,p.56.
[614] Voir : <http://www.marktwain.com/ecash>.
[615] What does the future Hold, Ecash from Mark Twain Bank FAQ, <http://www.marktawain.com/digifaq.html>.

La société Digicash a conclu ou négocie des accords de licence avec d'autres institutions financières[616]. Demain, si le système se développe, il serait possible de transférer de l'e-cash entre personnes ayant des comptes auprès de banques différentes : la validité de l'e-cash peut être vérifiée indépendamment de l'émetteur.

Le recours à un intermédiaire

Dans cette solution, la procédure de paiement est réalisée par un intermédiaire qui s'occupe des procédures de paiement entre la banque du client et la banque du commerçant.

First Virtual

Un tel système est par exemple utilisé par la First Virtual Holdings Inc.[617], une société américaine de l'Etat du Wyoming. Ce procédé est un des plus simple car il n'utilise ni logiciel spécifique, ni cryptage. Le vendeur doit cependant posséder un compte dans une banque américaine pour avoir recours aux services de First Virtual.

L'acheteur effectue une demande de création de compte chez First Virtual en lui communiquant hors réseau le numéro de son compte et de sa carte de crédit. First Virtual lui attribue ensuite un identifiant que le client utilisera lors de ses transactions. Le commerçant vérifie la validité du compte auprès de First Virtual, qui envoie un courrier électronique au client correspondant à l'identifiant pour lui demander de confirmer la transaction. First Virtual s'occupe du paiement entre les comptes bancaires des parties hors réseau : elle paie le commerçant et se fait payer par l'utilisateur.

Kleline

La Société Kleline[618], filiale de la Compagnie bancaire, propose également une plate-forme de gestion sécurisée des transactions commerciales. Le système utilisé est appelé Globe ID, et a été mis au point par la société GC Tech.

Lors d'une transaction, Kleline intervient en tant qu'intermédiaire afin d'authentifier les parties en présence et de gérer l'interface avec le monde bancaire.

L'utilisateur doit installer sur son ordinateur le logiciel de paiement sécurisé appelé « kleboxe ». En réponse à une commande, le commerçant émet un ticket de paiement électronique et l'envoie à Kleline. Kleline authentifie le marchand et envoie ce ticket au client. Ce dernier accepte le ticket en le validant électroniquement. Kleline valide la transaction et émet un « bon de caisse » auprès du commerçant. Pour sécuriser les opérations de vérification et de communication des données, on recourt à des procédés de cryptage.

Dans ce système, le client ne passe pas de contrat avec Kleline, hormis la licence d'utilisation du logiciel, c'est le commerçant qui mandate Kleline pour faire les opérations de paiement . Le client peut choisir de payer avec sa carte bleue, ou d'ouvrir un porte-monnaie virtuel chez le commerçant ou dans une galerie virtuelle, c'est-à-dire un site regroupant plusieurs commerçants. Si un porte-monnaie électronique est ouvert par le consommateur, c'est Kleline qui gère les fonds correspondants.

Le paiement peut être effectué en plusieurs devises. Kleline offre également un système de gestion de la comptabilité relative aux opérations effectuées par ce procédé: chiffre d'affaires, facturation, TVA, etc.

Ce système présente plusieurs inconvénients : en premier lieu, il n'est ouvert qu'aux commerçants français, il n'est donc pas universel, à la différence des autres systèmes existants. En second lieu, le client doit ouvrir un porte-monnaie virtuel auprès de chaque commerçant.

---

[616] « Digicash tisse sa toile », *Planète Internet* n° 8 mai 1996, p.58.
[617] Site Web : <http://www.fv.com>.
[618] Site Web : <http://www.kleline.fr>.

Si le paiement est effectué avec la carte, aucune signature électronique n'est générée comme dans le procédé SET (Visa et Mastercard). Pour se prémunir contre les risques de révocation des paiements et les usages frauduleux des cartes bancaires, Kleline attend 45 jours avant de régler le commerçant du montant de la transaction. Enfin, si le système de gestion de la comptabilité est intéressant, il suppose la mise en place d'un réseau EDI avec Kleline, ce qui rend la mise en place de cette technique de télépaiement beaucoup plus onéreuse pour le commerçant, et risque de dissuader les petites et moyennes entreprises de recourir à ce système.

Il existe d'autres organismes de type intermédiaire comme celui de Cybercash Inc.[619] ou Openmarket[620] qui fonctionnent sur le même principe : l'intermédiaire fait la relation avec les organismes bancaires pour effectuer les opérations de virement et obtenir les autorisations nécessaires au paiement[621].

Le porte-monnaie électronique

Un porte-monnaie électronique est une carte de paiement prépayée, c'est-à-dire chargée d'une somme payée par avance et multiprestataire, c'est-à-dire non limitée au paiement d'un service fourni par un seul prestataire, comme la carte téléphonique. La séparation entre le processus d'authentification qui n'a pas lieu en ligne et la communication entre les partenaires à la transaction sécurise la transaction. Il existe un programme européen de recherche sur le porte-monnaie électronique, le projet CAFE (Conditionnal Access For Europe) auquel participent plusieurs sociétés européennes comme la Royal PTT (Hollande), Digicash, France Télécom, Siemens[622].

Afin d'utiliser un porte-monnaie électronique pour les paiements en ligne, il est nécessaire que l'utilisateur dispose d'un lecteur de carte sur son ordinateur.

Comme avec l'argent liquide, le porte-monnaie électronique CAFE permet d'assurer l'anonymat des transactions et de connaître le montant des fonds disponibles. Comme avec les cartes de crédit, il peut être utilisé dans des transactions transfrontières, et permet de mettre en place une protection en cas de perte ou de vol.

Pour les paiement en ligne, il existe donc deux grandes catégories de systèmes :

- les systèmes basés sur la notion d'argent électronique, qu'il soit sous forme de porte-monnaie électronique matérialisé dans une carte ou de « monnaie électronique » générée par logiciel ;
- les systèmes basés sur les paiements par cartes de crédit.

Le cadre juridique du télépaiement

Nature juridique du télépaiement

Les instruments de paiement électronique sont des moyens de mobiliser des avoirs en compte à distance.

---

[619] Site Web : <http://www.cybercash.com>.

[620] Site Web : <http://www.openmarket.com>.

[621] Reis Marson, « Paiement électronique : quelle est la bonne formule ? » *le Monde informatique* 17 novembre 1995, p.42 ; Henry H. Perritt, Cyberpayment Infrastructure, 1996, Journal of Online Law, art.6, §.8 et suivants, <http://warthog.cc.wm.edu/law/publications/jol/>.

[622] Secure International Payment and Information Transfer, Towards a Multi-Currency Electronic Wallet, Report for the Project CAFE, Frankfurt 1995.

Le terme de monnaie électronique désigne « les diverses techniques qui assurent l'informatisation des moyens de paiement et les détachent ainsi du support papier »[623].

Le système de paiement sert à transférer la monnaie qui garde sa nature, son caractère[624]. La monnaie scripturale est simplement gérée électroniquement.

La première catégorie de paiement examinée utilise les mécanismes du système actuel des cartes de crédit. Dès lors que le paiement peut être déclenché par le biais d'une carte, les règles relatives au paiement par carte sont applicables.

La monnaie électronique, de type e-cash, ou le porte-monnaie électronique, type CAFE, est un nouveau moyen de paiement, mais qui repose toujours sur des mécanismes de mouvements de compte à compte : le porte-monnaie électronique ou le compte Ecash Mint est chargé d'une somme dont le compte du titulaire a déjà été débité.

A cet égard, les conditions générales du « World Currency Deposit Accounts and Ecash Agreement » de la Mark Twain Bank précise que le compte mis en place avec le système

e-cash ne représente pas un dépôt auprès de la banque mais du liquide géré par le client dans son ordinateur avec le système e-cash.

Frank Trotter, vice-président de la Mark Twain Bank explique : « A mon sens, il n'y a pas de création monétaire. L'e-cash n'est que le mécanisme de transport pour transférer des fonds existants d'un ordinateur à l'autre.[625] »

Juridiquement, tous les mouvements de comptes déclenchés par ces procédures de paiement reçoivent la qualification d'ordres de virement. L'argent électronique peut s'analyser comme un ordre de virement dans un compte du donneur à affectation spécifique puis un ordre de créditer les bénéficiaires lorsqu'ils auront été déterminés[626].

Sont également applicables au télépaiement les règles relatives au paiement, à la preuve et au contrat.

Le monopole bancaire

En France, les instruments qui, quel qu'en soit le support, permettent à toute personne de transférer des fonds, leur émission et leur gestion, relèvent de la compétence exclusive des établissements bancaires[627].

Au niveau communautaire, il n'existe pas encore de directive relative aux paiements électroniques et transfrontières. Il existe cependant plusieurs recommandations en la matière, les paiements transfrontières ayant l'attention particulière de la Commission[628]. On peut citer notamment une recommandation du 17 novembre 1988 « concernant les systèmes de paiement et en particulier les relations entre titulaires et émetteurs de carte[629] » et une recommandation du 14 février 1990[630] dans laquelle il est demandé aux établissements de crédit et aux services financiers de respecter certains principes visant à faciliter les virements opérés entre Etats membres distincts.

Tant que les techniques de paiement sont en pleine évolution, l'adoption d'une directive sera difficile.

---

[623] M. Cabrillac, Monétique et droit du paiement, Mélanges de Juglart, LGDJ 1986, p.83.
[624] Lamy informatique 1996, n° 2459.
[625] Entretien avec Jérôme Thorel, « Les dollars numériques de Mark Twain », *Planète Internet* n° 8 mai 1996,p.56.
[626] Lamy informatique 1996, n°2 446.
[627] Articles 1er et 4 de la loi n°84-46 du 24 janvier 1984 relative à l'activité et au contrôle des établissements de crédit.
[628] Xavier Favre-Bulle, Les systèmes de paiements dans la Communauté européenne : perspectives juridiques dans l'optique de l'utilisateur, Droit de l'Informatique et des Télécoms 1993/4, p.17.
[629] JOCE L317 du 24 novembre 1988.
[630] JOCE L67 du 15 mars 1990.

La question peut se poser de savoir si les mécanismes mis en place portent atteinte à la réglementation bancaire.

L'émission de monnaie est réservée aux banques centrales. Les banques et les établissements de crédit ont le monopole des opérations de banque qui comprennent la réception de fonds du public, les opérations de crédit, ainsi que la mise à la disposition de la clientèle ou la gestion de moyens de paiement.[631]

Les procédures de paiement mises en place sur l'Internet doivent-elles se voir appliquer cette réglementation ? En réalité l'examen des systèmes de paiement évoqués montre qu'il n'y a pas atteinte au monopole des banques sur la gestion et le transfert des fonds.

Notamment, dans les hypothèses où il est fait appel à un intermédiaire comme la First Virtual, l'intermédiaire laisse aux organismes financiers leur rôle, mais ne collecte pas et ne gère pas de fonds. Les transferts d'argent sont toujours réalisés par le système bancaire. Un exemple déjà connu de ce type d'organisation est celui des cartes de crédit dites accréditives, de type American Express. Or, American Express n'est pas une banque[632]. L'utilisation de la carte accréditive ne provoque aucune imputation directe du compte du titulaire de la carte. Le règlement du fournisseur est effectué par l'émetteur de la carte, à charge pour lui de s'en faire rembourser le montant par le titulaire de la carte[633].

De la même manière lorsque sur l'Internet on a recours aux services d'un intermédiaire, le processus de paiement n'est pas direct : l'intermédiaire n'est qu'un relais entre la banque de l'acheteur et la banque du fournisseur.

Avec le système Globe ID, La société Kleline va être amenée à gérer les fonds affectés au porte-monnaie électronique. Kleline est la filiale d'une banque. Des garanties ont été données par la maison mère. En outre, l'article 12 de la loi bancaire prévoit que le monopole des établissements de crédit ne fait pas obstacle « à ce qu'une entreprise, quelle que soit sa nature, puisse :

(…)

5°-Emettre des bons et cartes délivrés pour l'achat auprès d'elle, d'un bien ou d'un service déterminé ».

Le porte-monnaie électronique correspond à une telle carte puisqu'il est nécessairement affecté à un commerçant particulier. C'est donc dans le cadre de cette exception que semble s'inscrire le système Kleline, et c'est ce qui explique que le porte-monnaie électronique qu'elle propose ne puisse pas être multifournisseurs. Il faudrait pour qu'elle soit autorisée à le faire que Kleline prenne le statut d'établissement de crédit.

Le procédé de Digicash nécessite obligatoirement le concours d'un établissement financier qui « convertit » de la monnaie scripturale en e-cash et inversement.

En ce qui concerne le porte-monnaie électronique, son émission devrait être *a priori* réservée aux banques. En tout cas pour des raisons de solidité de l'émetteur, les autorités monétaires souhaitent que les émetteurs soient des banques ou des institutions financières, afin qu'ils soient assujettis aux réglementations appropriées, notamment en matière de liquidité et de contrôle par les autorités en charge de la surveillance des établissements de crédit. Certains pays veulent même réserver l'émission de ces porte-monnaie électroniques aux banques centrales[634].

Le porte-monnaie électronique, ou la monnaie électronique, soulève également des questions d'ordre monétaire. On a évoqué le fait qu'elle pourrait gêner le contrôle de la masse moné-

---

[631] Article 1er de la loi n° 84-46 du 24 janvier 1984.

[632] H. Henry Perritt, Cyberpayment Infrastructure, 1996 Journal of Online Law, art.6, par.22, <http://warthog.cc.wm.edu/law/publications/jol/>.

[633] Didier R. Martin, La carte de paiement et la loi, D 1992.278.

[634] Jean Hesbert, La menace du porte-monnaie électronique sur les cartes bancaires est-elle réelle ? Rev. Huissiers 1995 n°6, p.680.

taire[635] car elle représente un substitut des pièces et des billets. Il va falloir la classer parmi les instruments de paiement.

On craint surtout que la monnaie électronique ne rende plus difficile la lutte contre la fraude fiscale et le blanchiment de l'argent sale. Mais à la différence de l'argent liquide, l'argent électronique n'assure pas un anonymat absolu. Les montants convertis en e-cash et l'e-cash qui circule sont connus des banques. Il y a moins de risques d'abus qu'avec l'argent liquide[636].

Ce n'est que dans l'hypothèse où cet argent électronique était implémenté de manière à être intraçable qu'il pourrait remplacer l'argent liquide pour les activités illégales[637].

La question de l'influence de l'argent électronique sur les fluctuations des taux de change mériterait également d'être étudiée. Le commerce électronique va multiplier les hypothèses de paiement particulières. Commerçants et utilisateurs, pour bénéficier d'un système de paiement spécifique qui ne serait pas offert par une banque française ou à des conditions moins attrayantes, peuvent décider d'ouvrir un compte dans une banque étrangère.

Sept mois après le lancement de son opération, la moitié des clients de la Mark Twain Bank pour son offre de e-cash ne sont pas des résidents américains[638]. Pour la conversion de la monnaie électronique, les utilisateurs pourraient préférer certains émetteurs à d'autres en fonction de la solidité de la monnaie utilisée par l'émetteur.

En ce qui concerne le respect de la réglementation bancaire, il ne semble pas y avoir de bouleversement, mais plutôt adaptation des systèmes existants. Les paiements continuent à être matérialisés par des inscriptions de compte à compte.

Les tiers certificateurs

Certains systèmes, et notamment ceux qui transposent le paiement par carte de crédit en lui associant des procédés de cryptographie pour sécuriser la transaction et authentifier les parties supposent la mise en place d'une infrastructure de tiers certificateurs. Ce sont ces tiers certificateurs qui émettent les certificats électroniques contenant les informations nécessaires à l'authentification des parties, et notamment la clé publique qui permet de vérifier la validité d'une signature électronique générée avec la clé privée qui lui est associée. L'organisation de ces réseaux de tiers certificateurs reste entièrement à mettre en place[639].

En l'absence d'un statut clairement défini, le premier réseau de tiers certificateurs pourrait être organisé par Visa et Mastercard, pour la mise en place de leur solution de paiement sécurisé sur l'Internet.

L'irrévocabilité du paiement

Dans la plupart des hypothèses, les moyens de paiement sont irrévocables. Il en va ainsi dans le cas de paiement par chèque, ou en espèces. En ce qui concerne la carte de paiement, depuis une loi du 11 juillet 1985[640], « l'ordre ou l'engagement de payer donné au moyen d'une carte de paiement est irrévocable ». Cette irrévocabilité ne s'applique pas si seul le numéro apparent de la carte est donné.

---

[635] Jean Hesbert, préc., p.681.

[636] David Chaum's testimony for US House of Representatives, Committee on Banking and Financial Services, July 25, 1995, disponible à : <http://www.digicash.com/publish/testimony.html>.

[637] Secure International Payment and Information Transfer, Towards a Multi-Currency Electronic Wallet, Report for the Project CAFE, Frankfurt 1995, p.63.

[638] Jérôme Thorel, « Les dollars numériques de Mark Twain, entretien avec Frank Trotter, vice-président », *Planète Internet* n° 8 mai 1996,p. 56.

[639] Voir supra

[640] Article 22 de la loi n° 85-695, modifiant l'article 57-2 du décret -loi du 30 octobre 1935.

La question se pose de savoir si le paiement par carte en ligne (sans recours à un lecteur de carte) avec signature électronique pourra être considéré comme irrévocable. La signature électronique recrée le formalisme de la signature apposée sur une facturette papier ou de l'utilisation conjointe d'un code confidentiel et de sa carte.

Lorsque seul le numéro de la carte est donné, on considère qu'il n'y a pas de véritable ordre de paiement[641]. Ainsi, dans le système de First Virtual, même si l'acheteur a confirmé la transaction par courrier électronique à First Virtual, il peut faire annuler la transaction par sa banque. First Virtual se retourne alors contre le commerçant et annule le compte de l'acheteur[642]. De même dans le système Kleline, cette possibilité de révocation du paiement conduit la société Kleline à ne payer le commerçant qu'après 45 jours.

En revanche, le paiement par carte réalisé avec une véritable procédure d'authentification devrait pouvoir être considéré comme un ordre de paiement irrévocable.

Les opérations de paiement s'analysent en des ordres de virement. Juridiquement, un ordre de virement peut être révoqué tant qu'il n'a pas été inscrit au débit du compte du donneur d'ordre[643] et il n'est définitif que lorsque son montant a été porté au crédit du compte du bénéficiaire. D'une manière générale, les organismes bancaires et les institutions financières souhaitent que l'on tende vers l'irrévocabilité générale des ordres de télépaiement[644]. La recommandation européenne du 17 novembre 1988 consacre également le principe de l'irrévocabilité des télépaiements[645]. Le télépaiement peut en tout état de cause être déclaré irrévocable par convention. Le caractère irrévocable des paiements réalisés par argent électronique découle du caractère instantané de l'opération, comme lorsqu'il y a paiement en espèce. Une fois l'opération réalisée, il n'est plus possible de revenir en arrière. Ceci supposerait sans doute de lever l'anonymat de l'acheteur. En réalité, il y a dissociation dans le temps : les fonds ont déjà été débités du compte de l'acheteur. L'opération devient définitive lorsque le bénéficiaire du virement, soit le commerçant, est déterminé. L'irrévocabilité donne plus de sécurité à la banque et au fournisseur. Le client ne peut pas revenir sur l'ordre de paiement donné, alors même que s'il est consommateur, l'opération commerciale peut toujours faire l'objet d'une rétractation dans un délai de 7 jours à compter de la livraison. Le consommateur devra donc obtenir directement auprès du commerçant son remboursement, ce qui n'est pas avantageux pour lui.

La collecte de données sur les paiements

Toutes les transactions effectuées par les consommateurs avec des cartes de crédit sont enregistrées et peuvent être conservées, puis analysées et triées grâce aux techniques informatiques[646]. Les intermédiaires sont en mesure de recueillir un grand nombre de données sur les opérations effectuées par les clients des commerçants.

L'avantage de l'e-cash et du porte-monnaie électronique de type CAFE est qu'ils permettent de sauvegarder l'anonymat de l'acheteur, et par conséquent d'éliminer ce type d'inconvénient. Pour la CNIL, « la voie la meilleure pour assurer la protection des personnes est encore la règle de l'anonymat de la consommation des services à venir.[647] » Paradoxalement, c'est justement cet anonymat retrouvé par les citoyens qui semble déranger.

---

[641] Jérôme Huet, Aspects juridiques du télépaiement, JCP éd. G, I, 3524, n°5.
[642] First Virtual Buyer Terms and Conditions, December 16, 1995, Q10.2, disponible à : <http://www.fv.com/pubdocs/fineprint-buyer.txt>.
[643] Com. 23 janvier 1983, RTD Com. 1984, p.129.
[644] Aspects juridiques de la banque à domicile et du télépaiement, rapport du groupe de travail du Comité consultatif du Conseil national du crédit, point 2.2.2 (b), Droit de l'Informatique et des Télécoms 1993/3, p.78.
[645] article 4.1 lit. d.
[646] Voir supra
[647] Voix, Image et protection des données personnelles, Rapport de la CNIL, 1996, La Documentation française.

Le risque du paiement

Malgré toutes les précautions prises pour assurer la sécurité du télépaiement, un certain nombre d'incidents peuvent survenir : défaillance du système, perte par le client de sa carte ou de son numéro d'identifiant (clé privée, code secret), vol, utilisation frauduleuse d'un compte.

Les responsabilités encourues respectivement par le client et la banque ou l'intermédiaire devront être précisées contractuellement. Pour les cartes de paiement, la loi précise qu'il ne peut être fait opposition au paiement qu'en cas de perte ou de vol de la carte, de redressement ou de liquidation judiciaire du bénéficiaire.

En ce qui concerne les cartes bleues, la procédure et les partages de responsabilité entre client, banque et commerçant est connue : la responsabilité du titulaire de la carte est dégagée pour les opérations effectuées après l'opposition, mais engagée pour les opérations antérieures, avec un plafond plus ou moins élevé selon que l'opération comportait ou non un contrôle du code confidentiel[648]. Certains contrats réservent la faculté au banquier de rechercher la responsabilité du porteur en cas de faute ou d'imprudence dans la garde de la carte ou du code confidentiel, même après déclaration de perte ou de vol[649].

Le commerçant, s'il respecte la procédure prévue par la banque, bénéficie d'une garantie de paiement.

Pour les paiements à distance, le commerçant prend en charge les opérations contestées par le client[650]. Il devrait être tenu compte dans les contrats entre banques et commerçants de la sécurité offerte par le système de télépaiement utilisé.

Quels sont les types de risques engendrés par les nouvelles techniques de télépaiement ?

En ce qui concerne la signature électronique, il peut y avoir perte de la clé privée, ce qui obligera le titulaire de cette clé à révoquer son certificat électronique contenant la clé publique correspondante. L'hypothèse recouvre la situation où il y a perte de la carte. Il peut y avoir vol de la clé privée, par exemple résultant du vol de l'ordinateur.

La clé privée n'est pas nécessairement matérialisée dans une carte, elle est générée par un logiciel. Il peut y avoir « vol » de la clé par un tiers, sans que le porteur soit lui-même dépossédé de sa clé.

On peut imaginer l'hypothèse où un pirate s'introduit frauduleusement dans un système, ce qui nécessite toutefois des compétences particulières.

Le problème risque surtout de survenir si les ordinateurs sont partagés entre plusieurs personnes, ou pour les ordinateurs en réseau, ce qui est souvent le cas dans les entreprises.

En cas de perte du porte-monnaie électronique, il y a perte du pouvoir d'achat que le porte-monnaie contenait. Le système CAFE peut permettre d'intégrer une protection en cas de perte[651], mais le choix de sa mise en place appartient à l'émetteur.

Pour l'e-cash détenu dans le compte Ecash Mint, le risque est celui de la dégradation du matériel du client, entraînant la perte de l'e-cash et des registres des transactions récentes.

En cas d'incident avec l'ordinateur de l'utilisateur, il existe une procédure pour restaurer le compte e-cash[652].

---

[648] Article 11.2 du contrat porteur Carte Bleue du groupement des cartes bancaires, octobre 1995.

[649] Voir par exemple : conditions de fonctionnement de la Carte Bleue de la BNP, mars 1994, article 12-3.

[650] Conditions particulières de fonctionnement du système de paiement par carte dans le cadre de vente par correspondance, par téléphone ou par vidéotex, article 4.

[651] Secure International Payment and Information Transfer, Towards a Multi-Currency Electronic Wallet, Report for the Project CAFE, Frankfurt 1995, loss tolerance scheme p. 67.

[652] Recovery, an introduction to e-cash, <http://www.digicash.com/publish/ecash_intro/ecash_intro.html>.

Une utilisation frauduleuse de l'ordinateur du client peut éventuellement se produire. Les conditions générales du contrat de la Mark Twain Bank précisent que « le client traitera les montants détenus sur le compte Ecash Mint comme s'il s'agissait de liquide et que ce liquide est sous sa responsabilité contre les attaques. »[653]

D'une manière générale, par analogie avec ce qui se passe aujourd'hui pour les cartes de crédit, on peut penser que pèsera sur l'usager un devoir de prudence.

Ces différents codes ne sont pas toujours mémorisables. C'est le cas notamment des clés générées par les logiciels de cryptage.

Or, une opération réalisée avec l'identifiant et le mot de passe va avoir tendance à être réputée émaner du client lui-même, qui devra supporter les conséquences de l'utilisation frauduleuse de son compte par des tiers non autorisés, même dans les hypothèses où il n'aurait commis aucune faute dans la conservation de ses moyens d'accès.

Ainsi, des juges ont retenu une responsabilité à hauteur d'un quart à la charge du titulaire d'une carte privative parce qu'il avait tardé à se rendre compte de sa disparition[654].

Si le paiement nécessite le recours à une carte, le problème se pose surtout en pratique dans les hypothèses où il y aurait utilisation à son insu par un proche du titulaire de la carte. Dans les autres hypothèses, le client devra veiller à conserver dans un endroit distinct de son ordinateur les éléments d'information relatifs à son compte bancaire.

Dans tous les cas où le système de paiement utilisé implique l'utilisation de logiciels se trouvant sur l'ordinateur du client, l'utilisateur devra prendre les mesures nécessaires afin d'empêcher les tiers non autorisés d'utiliser son ordinateur et ses logiciels de paiement, ce qui ramène la question à un problème de sécurité informatique.

Les modalités d'opposition à l'utilisation d'un compte, de révocation d'un certificat devront être précisées dans les contrats.

La recommandation communautaire du 17 novembre 1988 prévoit que le titulaire doit prendre les mesures propres à assurer la sécurité de ses moyens d'accès au système de paiement, et qu'il devra informer l'émetteur sans délai excessif s'il constate la disparition desdits moyens d'accès ou l'enregistrement d'opérations non autorisées ou erronées sur son compte[655].

L'émetteur doit quant à lui faire en sorte que les clients puissent l'aviser jour et nuit de la perte, du vol ou de la contrefaçon de leur moyen de paiement[656]. Il devra également tout mettre en œuvre pour empêcher l'utilisation frauduleuse de moyens de paiement s'il est informé de la disparition de ceux-ci[657].

Jusqu'au moment de la notification de la perte, du vol ou de la contrefaçon du moyen de paiement, c'est le titulaire cocontractant qui devra supporter la perte subie, mais sa responsabilité sera limitée à un montant maximum de 150 écus[658]. Si le client a agi frauduleusement ou a fait preuve de négligence extrême, sa responsabilité peut être engagée au-delà de ce plafond et même après la notification.

Cette recommandation n'a de valeur qu'incitative, elle n'est pas obligatoire.

En conclusion, si aucune clause conventionnelle ne vient plafonner sa responsabilité en cas d'utilisation frauduleuse du compte par un tiers, le client supporte le risque. Hormis le cas où cette opération est effectuée par un proche du client, une telle opération nécessite cependant des compétences très particulières.

---

[653] Point 13 des conditions générales, disponibles à : <http://www.marktwain.com/ecash>.
[654] Civ. 1re 14 juin 1988, Droit de l'Informatique et des Télécoms 1990/2, p.49, note J.Huet.
[655] Article 4.1.
[656] Article 8.1.
[657] Article 8.4.
[658] Article 8.3

La preuve

La question de la preuve du paiement est identique aux problèmes posés par la preuve en général dans le cas des transactions dématérialisées.

La preuve de l'ordre de paiement sera généralement apportée par les enregistrements informatiques détenus par les intermédiaires ou les établissements financiers ou bancaires. Les conditions générales du contrat First Virtual attirent ainsi l'attention des clients sur le fait que pour garder les traces des transactions, les courriers électroniques sont stockés[659].

Peut se poser également la question de la preuve d'un ordre d'opposition, sur une carte ou sur un compte, de la révocation d'un certificat auprès d'une banque, d'un intermédiaire ou encore d'un tiers certificateur.

En matière de cartes de crédit, l'opposition peut être faite téléphoniquement, puis doit être confirmée par lettre remise ou expédiée en recommandé si elle n'a pas fait l'objet d'une déclaration signée par le titulaire de la carte. En cas de contestation, l'opposition est réputée avoir été effectuée à la date de réception de la lettre par l'établissement émetteur de ladite carte[660].

Ce type de problème est survenu dans une affaire où une personne avait été victime d'un vol à son domicile dans la nuit de vendredi à samedi de sa Carte Bleue et de documents dont celui mentionnant son numéro de code secret.

La personne avait fait opposition téléphoniquement mais s'était trompée sur les références de sa carte. L'opposition n'a pu être confirmée que le lundi matin. Entre temps, le voleur avait effectué des retraits à hauteur de 9 600 francs. Le tribunal saisi avait estimé que la banque devait supporter la charge des retraits frauduleux. Cette décision a été cassée par la Cour de cassation [661] au motif que le tribunal aurait dû rechercher à quelle date la cliente avait formé utilement opposition à l'utilisation de sa carte bancaire auprès du groupement « Carte Bleue ».

Une solution quant au problème de la date et de l'heure de l'opposition pourrait être de donner au client un numéro d'ordre lorsqu'il effectue sa plainte par téléphone[662].

Le coût et le seuil de rentabilité de ces nouveaux procédés de paiement devront être évalués. Il s'agit également de savoir comment les frais vont être répartis entre les fournisseurs et les clients. Du point de vue légal, il n'y a pas d'obstacle de principe à la mise en place de ces nouveaux procédés de paiement.

De nouvelles lois pour venir réglementer ces systèmes n'apparaissent pas nécessaires, dès lors qu'ils s'intègrent dans le cadre de la réglementation bancaire. Les relations entre clients, intermédiaires, institutions financières, fournisseurs pourront être réglées par la voie des contrats, qui devront régir les différentes situations et les devoirs et responsabilités de chacun des intervenants à l'opération.

Le contrat présente l'avantage de pouvoir être adapté aux questions nouvelles qui se poseront. Un professeur d'université français soulignait à propos du télépaiement que le contrat

---

[659] First Virtual Buyer Terms and Conditions, December 16, 1995, Q.7, disponible à : <http://www.fv.com/pubdocs/fineprint-buyer.txt>.
[660] Article 10.2.
[661] Com. 1er mars 1994, D 1995.167.
[662] Jérôme Huet, Aspects juridiques du télépaiement, JCP éd. G, I, 3524, n°9.

avait été « pour les cartes de paiement, un laboratoire de création de règles juridiques. Il le sera certainement aussi pour le télépaiement »[663], opinion que partage un de ses collègues américain : « Le système des cartes de paiement traite des milliards de dollars chaque année, et pourtant, il est presque entièrement régi par des contrats privés avec les émetteurs »[664].

[663] Jérôme Huet, préc., n°12.

[664] H. Henry Perritt, Cyberpayment Infrastructure, 1996 Journal of Online Law, art.6, par.17, <http://warthog.cc.wm.edu/law/publications/jol/>.

Quatrième partie

TVA et commerce électronique

Le commerce électronique est, comme les autres activités économiques, soumis au droit fiscal.

Les échanges de données dématérialisées vont soulever un certain nombre de questions nouvelles en droit fiscal, que l'on peut regrouper en deux grandes catégories.

La première catégorie concerne les relations avec l'administration. Les règles fiscales existantes sont basées sur l'écrit. Par exemple, la facture doit être un document écrit, comportant certaines mentions obligatoires[665]. Le remplacement des factures écrites par des messages électroniques n'est pas un processus évident.

L'informatisation des échanges pourra être progressivement intégrée dans la réglementation fiscale ainsi qu'en attestent deux ouvertures récentes[666] : la reconnaissance de la facture EDI, sous certaines conditions par l'article 47 de la loi du 29 décembre 1990[667], et les transferts de déclaration par voie informatique prévus par la loi Madelin du 11 février 1994, dans des conditions fixées par voie contractuelle.

Le deuxième domaine où le développement du commerce électronique influencera le droit fiscal est lié au caractère international des réseaux informatiques. La souveraineté fiscale est liée à la souveraineté nationale. Or les échanges de données informatiques sont étrangers à toute frontière politique ou économique. « Certains cycles complets d'opérations de vente de biens ou de prestations de services, y compris leur paiement peuvent être délocalisés sur des réseaux, à commencer par l'Internet, et échapper à toute imposition et en tout cas à quelque contrôle que ce soit[668]. »

La dématérialisation des échanges peut rendre délicate la détermination de la résidence du destinataire, la localisation de la livraison, la qualification des opérations, données qui intéressent le droit fiscal.

L'ensemble de ces aspects ne sera pas abordé en détail dans le cadre de cet ouvrage.

Il existe cependant un domaine où cette dématérialisation des échanges ne va pas manquer de soulever de nombreuses difficultés pratiques, c'est celui de la TVA.

La facturation de la TVA française dépend à la fois de la localisation de l'opération et de sa nature, le régime étant différent selon qu'il s'agit d'une livraison de biens ou une prestation de services.

---

[665] Thierry Piette-Coudol, Le remplacement de l'écrit par un message électronique : le cas de la facture, Gaz. Pal. 1992.2.804.
[666] Voir supra
[667] Loi de finances rectificative, article 289 bis du Code général des impôts.
[668] Jean-Pierre Le Gal, Fiscalité et échanges de données informatisées, JCP éd. E 1996, I,558, n° 10.

Vente à distance aux particuliers

La vente à distance aux particuliers établis dans un autre Etat membre de la CEE fait l'objet de dispositions particulières[669].

Concernant les ventes à distance à partir de la France, le lieu de livraison est considéré comme étant situé dans l'Etat membre d'arrivée des biens lorsque le vendeur a réalisé l'année précédente ou l'année en cours des ventes à distance à destination de cet Etat pour un montant supérieur à un seuil de 35 000 ou 100 000 écus fixé par cet Etat. Sinon le lieu de livraison est situé en France, et la TVA française facturée.

Pour les ventes à distance d'un Etat membre vers la France, ce seuil est fixé à 700 000 francs hors taxes. Dans les cas d'imposition en France, la délivrance de factures est obligatoire et le vendeur qui n'est pas établi en France doit y désigner un représentant fiscal.

Facturation de la TVA sur les biens immatériels

Concernant les prestations de service, le principe est que l'imposition a lieu en France lorsque le prestataire est établi en France. Cependant un certain nombre de prestations dites « immatérielles » font l'objet de règles de territorialité spécifiques : la facturation de la TVA ne dépend pas du lieu d'exécution de la prestation, mais du lieu d'établissement du bénéficiaire de la prestation. Sont notamment concernées les cessions et concessions de droits d'auteur, de droits de licence, les prestations de publicité, les traitements de données et la fourniture d'informations, les cessions de logiciels en l'absence de support matériel.

Le commerce électronique de biens non matériels directement livrés à travers le réseau, est donc tout particulièrement concerné. Il est possible de commander des logiciels directement sur l'Internet, l'acheteur téléchargeant le logiciel sans qu'une disquette lui soit nécessairement adressée.

Pour ce type d'opérations, la TVA doit être facturée :

- si le preneur (le client) est établi en France ;
- si le preneur est établi dans un autre Etat membre sans y être assujetti (cela concerne notamment les particuliers).

La TVA n'a pas à être facturée si :

- le preneur est assujetti dans un autre Etat membre de la CEE ;
- le preneur est établi hors de la Communauté européenne.

Par ailleurs, même si le prestataire est établi hors de France, les prestations sont imposables en France :

- si le preneur établi en France est assujetti à la TVA ;
- si le prestataire est établi hors CEE, lorsque le preneur est établi en France, n'est pas assujetti à la TVA, mais utilise le service en France.

Ce régime particulier est notamment applicable aux importations de logiciels en l'absence de support matériel[670].

La fourniture par une entreprise établie hors de la Communauté européenne à un client français de logiciels qui sont transmis sans support matériel est imposable à la TVA en France,

[669] Articles 258 A et 258 B du Code général des impôts.
[670] Instruction du 16 février 1996 du SLF et de la DGI relative à la TVA, BOI 3 A-1-96, 26 février 1996.

dès lors que le client est lui-même assujetti à la TVA en France (cas des entreprises) ou s'il est domicilié en France sans y être assujetti (cas des particuliers) dès lors que le logiciel est utilisé en France.

Lorsque le preneur est assujetti à la TVA, la taxe doit être réglée par le bénéficiaire qui est le client. Le prestataire doit mentionner sur la facture qu'il adresse à son client « prestation désignée à l'article 259 B du CGI. Taxe due par le preneur ».

Le prestataire étranger a la possibilité de désigner un représentant fiscal en France qui effectue les formalités nécessaires. La facture établie par le prestataire doit faire apparaître distinctement le prix hors taxes, le taux et le montant de la TVA.

En cas de défaut de paiement, le recouvrement est poursuivi auprès du preneur ou à défaut du prestataire.

En cas de non-déclaration de la taxe, le redevable est passible d'une amende de 5 % du rappel de taxe, outre les pénalités de retard.

Si le client n'est pas assujetti à la TVA, le prestataire étranger doit, s'il n'est pas établi en France, désigner un représentant fiscal en France qui s'engage à acquitter la taxe[671]. A défaut de représentant accrédité, la taxe, et le cas échéant, les pénalités sont dues par le destinataire.

En résumé, les entreprises françaises qui téléchargent directement leurs logiciels sur l'Internet doivent auto-acquitter la TVA auprès de l'administration fiscale et veiller à demander à leur correspondant de leur adresser une facture conforme aux exigences de l'administration.

Concernant les consommateurs, l'entreprise établie hors CEE est censée avoir désigné un représentant fiscal en France, ce qui est en pratique assez aléatoire.

Pour les entreprises, l'administration a les moyens de vérifier lors des contrôles qu'elle effectue le respect de ces dispositions si les biens ont été pris en compte dans la comptabilité.

On imagine mal en revanche l'administration fiscale procéder à ces contrôles de TVA auprès de particuliers pour vérifier que les taxes exigibles sur des biens immatériels ont bien été acquittées. C'est en pratique tout un ensemble d'opérations qui risque d'échapper à l'impôt.

Il n'est pas réaliste d'imaginer que des entreprises situées par exemple en Amérique ou en Asie vont se préoccuper de désigner un représentant fiscal en France, si elles n'y ont pas déjà de filiale ou d'établissement.

D'autres difficultés peuvent survenir. Par exemple, l'entreprise française qui veut facturer de la TVA pour des biens qu'elle délivre en ligne à des consommateurs doit connaître le lieu de résidence du consommateur. S'il réside en France ou dans un pays de la CEE, la TVA est facturée, sinon elle ne l'est pas. Or quelle contrôle peut réellement exercer l'entreprise sur les déclarations des clients quant à leur lieu de résidence ? Ainsi tous les abonnés de Compuserve ont comme boîte aux lettres une adresse composée de cette manière : numéro@compuserve.com, quel que soit leur lieu de résidence. Les consommateurs ne vont-ils pas être tentés lorsqu'ils en auront la possibilité de déclarer qu'ils sont résidents hors CEE pour éviter de payer de la TVA à un taux de 20,6% ?

Inversement, les entreprises, pour éviter les complications, pourraient décider de facturer à tous la TVA française. Si le destinataire est lui-même tenu dans son pays de payer certaines taxes, il serait pénalisé car il serait doublement taxé.

Les problèmes soulevés rien qu'en matière de TVA par la dématérialisation des échanges ne sont pas simples.

La facturation de la TVA a des incidences en matière de prix, de trésorerie pour les entreprises et de concurrence.

---

[671] Article 289 A du Code général des impôts.

Si des entreprises situées à l'étranger commercialisent auprès de consommateurs français des biens sans facturer de TVA, il est évident que ces biens seront moins cher et que cela crée une distorsion de concurrence en défaveur des entreprises françaises et inversement si une entreprise vend hors taxes ses biens à un consommateur hors CEE.

On peut penser que la réglementation fiscale va évoluer pour prendre en compte la spécificité des échanges dématérialisés.

Le règlement des différents

Première partie

L'identification des acteurs de la communication

Comment faire assurer le respect de ses droits sur l'Internet, dans un contexte immatériel et international ?

L'émetteur d'une information sur l'Internet est présumé responsable de la légalité du contenu de cette information : émetteur d'un courrier électronique, auteur d'un message envoyé dans un newsgroup, éditeur d'un service Web. Si cette information est illicite, il est normal et logique que son émetteur puisse être poursuivi afin que sa responsabilité civile ou pénale puisse être engagée.

Cependant un certain nombre de difficultés d'ordre pratique et juridique peuvent rendre difficile voire impossible la mise en cause des auteurs directs des informations incriminées. Préalablement, l'émetteur de l'information va devoir être identifié.

Une démarche amiable ou judiciaire à l'encontre de l'émetteur d'une information suppose que cet émetteur soit identifiable et localisable.

Dans d'autres situations, cette identification s'avérera difficile voire impossible, en raison de l'utilisation des techniques d'anonymat.

Enfin, la question de l'utilisation du courrier électronique pour délivrer mises en demeure et notifications sera examinée.

L'identification des intervenants

Editeurs de services d'information

Chaque ordinateur relié à l'Internet doit pouvoir être identifié et localisé, et dispose d'une adresse IP. De plus, chaque nom de domaine est attribué par un organisme de nommage (NIC-France, NSI, etc.) spécifique[672].

La personne enregistrant un nom de domaine doit notamment fournir les coordonnées (adresse, téléphone, télécopie, courrier électronique) de son responsable administratif, de son responsable technique et les adresses des serveurs de noms. Toutes ces informations sont regroupées dans des bases de données sur lesquelles tout un chacun peut effectuer des recherches en ligne pour vérifier si un nom de domaine n'a pas été enregistré ou quel est le titulaire d'un nom de domaine particulier.

[672] Voir supra

L'organisme auprès duquel la recherche devra être effectuée est facilement identifié par la zone à laquelle appartient le nom de domaine.

Exemple :

Vous voulez savoir qui a déposé le nom de domaine <france.com>.

Une recherche sur la base de données Whois de l'InterNIC[673] (le top level domain est <com> qui est géré par l'InterNIC) donne :

```
_____________________________________________________________
France Online (FRANCE-DOM)
6201 Sunset bldv #124
Los Angeles, CA 90028
USA
Domain name : france.com.
Administrative contact, Technical contact :
Frydman Jean-Noel (JF57) jnf@france.com
Record last updated on 05-janvier-96 (dernière mise à jour)
Record created on 10-Feb-94 (date de création du nom de domaine)
Domain servers in listed order :
PARIS.FRANCE.COM   199.4.122.1
NS1.WCO.COM                199.4.94.1
_____________________________________________________________
```

L'identification du responsable d'un serveur d'information est donc très facile si un nom de domaine a été déposé.

Dans d'autres cas, le service n'a pas de domaine propre, il est hébergé chez un fournisseur de services. Par exemple, l'adresse d'un site sera <http//www.serveur.fr/site>.

Les coordonnées de la personne ayant déposé le nom de domaine <serveur.fr> peuvent être facilement retrouvées dans la base de données du NIC-France[674]. Et l'entité qui gère le service correspondant au nom de domaine <serveur.fr> connaît les coordonnées de <site> puisqu'elle l'héberge sur son propre serveur.

L'adresse du site pourrait être : <http//www.site.serveur.fr>.

Dans ce cas <serveur.fr> n'héberge pas nécessairement <site> sur ses ordinateurs, qui peut se trouver dans n'importe quelle place géographique. En revanche, <serveur.fr> gère le serveur de nom et connaît l'adresse IP de la machine qui gère les noms de la zone <site> hébergeant la machine <www.site.serveur.fr>. En remontant en cascade, on finit donc par être en mesure de retrouver les éléments nécessaires à l'identification de <site>.

Auteurs de messages

Dans un message envoyé dans un newsgroup, dans une liste de diffusion ou encore adressé directement par courrier électronique, l'adresse e-mail de l'émetteur figure généralement dans le message lui-même. Le nom de domaine de l'entité fournissant l'accès à l'Internet, ou un compte à l'émetteur du message figure dans le courrier électronique, après l'arobace @. Par exemple, la personne qui se cache derrière <10056.8563@compuserve.com> n'est pas directement identifiable, mais la société Compuserve devrait connaître l'adresse de la personne à laquelle elle a attribué ce compte s'agissant d'un de ces abonnés.

Il est toujours possible à l'expéditeur d'un message de ne pas préciser ses coordonnées ou de mettre de fausses coordonnées. Il est néanmoins possible de savoir depuis quel serveur le

[673] <http://internic.net/cgi-bin/whois>, recherche effectuée le 12 mai 1996.
[674] <http://www.nic.fr/info/whois.html>.

message a été envoyé. Le chemin suivi par chaque courrier est inclus dans le message et permet de remonter jusqu'à la machine d'émission.

Voici un exemple :

```
_____________________________________________________________
Received : from mexico.brainstorm.eu.org (193.56.58.253) by aqueduc.argia.fr
 (EMWAC SMTPRS 0.80) with SMTP id <B00000037348@aqueduc.argia.fr>;
 Wed, 25 Sep 1996 13:26:28 +0200
Received : from brasil.brainstorm.eu.org (brasil.brainstorm.eu.org [193.56.58.33]) by
mexico.brainstorm.eu.org (8.7.5/8.7.3) with ESMTP id NAA00161; Wed, 25 Sep 1996 13:31:38
+0200
Received : from mexico.brainstorm.eu.org (root@mexico.brainstorm.eu.org [193.56.58.35])
by brasil.brainstorm.eu.org (8.6.12/8.6.12) with ESMTP id NAA00847 for <aui-
partners@aui.fr>; Wed, 25 Sep 1996 13:31:17 +0200
Received : from universe.digex.net (universe.digex.net [205.197.248.2]) by mexi-
co.brainstorm.eu.org (8.7.5/8.7.3) with SMTP id NAA00157 for <aui-partners@aui.fr>; Wed,
25 Sep 1996 13:31:12 +0200
Received : from 204.91.138.85 (mail.epic.org [204.91.138.85]) by universe.digex.net
(8.6.12/8.6.12) with SMTP id HAA17036; Wed, 25 Sep 1996 07:18:59 -0400
Received : from athena.romoidoy.com (208.193.64.15) by mail.privacy.org
with SMTP (Apple Internet Mail Server 1.1); Wed, 25 Sep 1996 07:16:28 -0400
Received : from [206.14.141.118] (cyberpolis.org [206.14.141.118]) by athena.romoidoy.com
(8.6.12/Romoidoy-Hub-022896) with ESMTP id AAA16375 for <gilc@mail.privacy.org>; Wed, 25
Sep 1996 00:29:48 -0700
_____________________________________________________________
```

En remontant, on sait que le message en question a été envoyé depuis le serveur <cyberpolis.org [206.14.141.118]> le 25 septembre 1996 à 00h29.

Il est donc déjà envisageable de situer géographiquement le serveur ayant permis l'envoi. Il est de plus fort probable que toutes les connexions à ce serveur soient enregistrées, du moins pendant un certain temps.

Avec l'aide du fournisseur d'accès, il est possible de connaître l'identité de l'utilisateur final qui était connecté à l'heure dite.

Le principe est le même pour les messages postés dans les newsgroups.

Si la fabrication de messages complètement anonymes et intraçables est à la portée d'un technicien déterminé et compétent, cette manipulation reste largement hors de portée du grand public.

Un dernier exemple illustre le fait que les personnes qui se connectent peuvent être tracées dans une majorité de cas.

Une enquête effectuée après que le site de l'Ecole polytechnique a fait l'objet d'intrusions a révélé que le pirate était situé en Israël, et qu'il se connectait via son prestataire d'accès à l'Internet, un site universitaire. L'article du *Monde* daté du 4 Juin 1996 relatant l'affaire explique : « Le repérage des troubles s'est effectué classiquement. Les gestionnaires de réseaux informatiques disposent d'équipes et de consignes de surveillance leur permettant de noter l'origine de tous les ordinateurs se connectant sur leur système. Ils peuvent aussi repérer rapidement certaines modifications anormales de fichiers qui, sans cette vigilance, pourraient passer inaperçues »[675].

[675] Erich Inciyan et Annie Kahn, « Le site Internet de Polytechnique a été fermé à la suite d'intrusions », *le Monde* du 4 juin 1996, p. 13.

Obtenir les coordonnées d'une personne auprès d'un fournisseur d'accès ou d'hébergement

Le fournisseur d'accès connaît généralement les noms et adresses de ses clients. A défaut, il est au moins en possession de leurs coordonnées bancaires. Il est donc en mesure de fournir des éléments nécessaires à leur identification directe ou indirecte.

Le fournisseur d'accès pourrait-il se retrancher derrière des dispositions contractuelles ou encore le secret professionnel pour refuser de divulguer les coordonnées d'un client.

Trois hypothèses sont à distinguer suivant que le client est une personne physique, une personne morale ou un éditeur de service d'information.

L'obtention des coordonnées d'une personne physique

Il existe un droit à l'anonymat, à l'incognito, et il existe un droit au secret de l'adresse, car elle désigne, pour la plupart, le lieu d'habitation, domicile ou résidence, donc un espace réservé à la vie privée et familiale[676].

« Chacun a droit au respect de sa vie privée[677] », et l'adresse est considérée par la jurisprudence comme un élément de la vie privée.

Ainsi, il a été jugé que la divulgation de l'adresse du domicile ou de la résidence d'une personne sans le consentement de celle-ci constituait une atteinte illicite à sa vie privée[678].

Les abonnés d'un fournisseur d'accès font très certainement partie d'un traitement automatisé d'informations nominatives. Or, l'article 226-22 du Code pénal prévoit que :

« Le fait par toute personne qui a recueilli, à l'occasion de leur enregistrement, de leur classement, de leur transmission ou d'une autre forme de traitement, des informations nominatives dont la divulgation aurait pour effet de porter atteinte à la considération de l'intéressé ou à l'intimité de sa vie privée, de porter sans autorisation de l'intéressé, ces informations à la connaissance d'un tiers qui n'a pas qualité pour les recevoir est puni d'un an d'emprisonnement et de 100 000 francs d'amende. »

Le fournisseur d'accès va donc être tenu d'une obligation de non-divulgation aux tiers de l'identité et de l'adresse de ses clients. Cette obligation s'applique également si le fournisseur de connexion est l'employeur de la personne dont on voudrait obtenir les coordonnées.

Ce droit à l'anonymat et au secret de l'adresse n'est pas absolu, et doit cesser dès lors qu'il peut causer un préjudice au tiers.

Le droit au respect de la vie privée cède devant les impératifs de prévention et de répression des infractions pénales par l'autorité publique[679]. En matière pénale, les autorités judiciaires seront fondées à obtenir auprès du fournisseur d'accès les éléments nécessaires à l'identification de la personne soupçonnée d'être l'auteur d'une infraction.

Cependant, la personne s'estimant victime de pratiques illégitimes ne va pas nécessairement agir sur le plan pénal, elle peut préférer une procédure civile qui sera plus rapide et lui permettra généralement d'obtenir des dommages et intérêts plus importants.

Ainsi même si une contrefaçon est un délit pénal, beaucoup d'affaires vont devant les tribunaux civils.

---

[676] Dominique Velardocchio, note sous Civ. 1re 19 mars 1991, D 1991.568.
[677] Article 9 du Code civil.
[678] Paris 14 mars 1988, D 1988, IR.104.
[679] Article 8.2 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales.

Sans aller jusqu'à diligenter une procédure judiciaire, une personne peut vouloir simplement être en mesure d'adresser une mise en demeure afin de faire cesser amiablement une atteinte à ses droits d'auteur ou une marque dont elle est titulaire.

Hormis le cas où l'abonné a donné son consentement au fournisseur d'accès pour que son identité et son adresse soit révélées à la personne qui en fait la demande, est-il possible d'obtenir une injonction judiciaire à cette fin ?

L'article 10 du Code civil prévoit que :

« Chacun est tenu d'apporter son concours à la justice en vue de la manifestation de la vérité. Celui qui, sans motif légitime, se soustrait à cette obligation lorsqu'il en a été légalement requis, peut être contraint d'y satisfaire, au besoin à peine d'astreinte ou d'amende civile, sans préjudice de dommages et intérêts. »

L'obligation d'apporter son concours à la justice pour la manifestation de la vérité est un devoir civique.

Selon la jurisprudence, le juge civil a le pouvoir d'ordonner à un tiers de produire tout document qu'il estime utile à la manifestation de la vérité, et ce pouvoir n'est limité que par l'existence d'un motif légitime tenant soit au respect de la vie privée, sauf si la mesure s'avère nécessaire à la protection des droits et libertés d'autrui, soit au secret professionnel[680].

Le fournisseur d'accès est-il astreint au secret professionnel ?

L'article 226-13 du code pénal prévoit que :

« La révélation d'une information à caractère secret par une personne qui en est dépositaire soit par état ou par profession, soit en raison d'une fonction ou d'une mission temporaire, est punie d'un an d'emprisonnement et de 100 000 francs d'amende. »

C'est la jurisprudence qui fixe au cas par cas les personnes dépositaires de secrets. Il s'agit principalement des professions médicales, des assistantes sociales, des personnes qui participent au fonctionnement du service public de la justice (avocats, magistrats, greffiers, huissiers, notaires), des banquiers, experts-comptables, ministres du culte.

D'autres catégories de personnes ne sont tenues qu'à une obligation de discrétion, susceptible seulement d'engager leur responsabilité civile en cas de divulgation des faits venus à leur connaissance[681].

Tel est le cas, par exemple, des éducateurs de prévention d'enfants inadaptés ou de détenus[682] ou encore du directeur du personnel d'une compagnie d'assurance[683].

Pour la Cour de cassation, « ce que la loi a voulu garantir c'est la sécurité des confidences qu'un particulier est dans la nécessité de faire à une personne dont l'état ou la profession dans un intérêt général et d'ordre public fait d'elle un confident nécessaire »[684].

Le fournisseur d'accès est tenu de respecter le secret des correspondances de ses clients, mais est-il astreint au secret professionnel en ce qui concerne leur nom et leur adresse ?

Surtout, le fournisseur d'accès pourrait-il se retrancher derrière un tel secret pour refuser d'exécuter la décision d'un juge lui faisant injonction de communiquer les noms et adresses de son client ?

La jurisprudence est venue préciser que certaines catégories de personnes, comme les avocats, les médecins, les assistantes sociales, les ministres du culte, sont liées par un secret professionnel général et absolu et même le consentement de celui qui leur a fait la confi-

[680] Civ. 1re 21 juillet 1987, Gaz. Pal. 1988.1.322, note Renard.
[681] M. Véron, Droit pénal spécial, L'atteinte au secret professionnel, éditions Masson, p.140 et s.
[682] Crim. 4 novembre 1971, JCP 72, II, 17256, note Mayer-Jack.
[683] Crim. 19 novembre 1985, Bull. Crim., n° 364.
[684] Crim. 19 novembre 1985, Bull. Crim., n°364.

dence ne peut les relever de leur obligation au silence. Ces catégories de personnes sont dispensées de témoigner en justice, sauf dans les cas expressément prévus par la loi.

On peut également citer le droit des journalistes de ne pas révéler leurs sources, prévu par l'article 109 du Code de procédure pénale[685].

Cependant, la Cour de cassation a refusé de considérer que le ministère des Télécommunications pouvait invoquer comme motif légitime justifiant un refus d'exécuter la décision d'un juge lui demandant de lui communiquer l'identité et l'adresse d'une personne inscrite sur la « liste rouge », les règles relatives au secret professionnel[686].

Dans une autre espèce où un employeur invoquait l'article 9 du Code civil pour refuser de communiquer l'adresse d'une de ses employées à son créancier, la Cour de cassation a posé le principe que :

« Si toute personne est en droit, notamment pour échapper aux indiscrétions ou à la malveillance, de refuser de faire connaître le lieu de son domicile ou de sa résidence, de sorte qu'en principe sa volonté doit être sur ce point respectée par les tiers, il en va autrement lorsque cette dissimulation lui est dictée par le seul dessein illégitime de se dérober à l'exécution de ses obligations et de faire échec aux droits des créanciers ; qu'il appartient au juge des référés de mettre un terme à une telle manœuvre frauduleuse »[687].

D'autres décisions de jurisprudence vont dans le même sens.[688] La communication de l'adresse sans le consentement de l'intéressé doit avoir pour but « la sauvegarde d'un droit légalement reconnu ou judiciairement constaté »[689].

Une personne justifiant d'un intérêt légitime peut demander à un juge qu'il soit fait injonction à un fournisseur d'accès de communiquer les éléments nécessaires à l'identification d'un de ses clients.

L'obtention des coordonnées d'une personne morale

Si la demande concerne une personne morale, l'argument tenant au risque d'atteinte à la vie privée ne semble plus pouvoir être opposé pour faire obstacle à la communication de la raison sociale et de l'adresse du siège de ladite personne morale.

En effet, une personne morale n'est pas protégée par l'article 9 du Code civil sur le droit au respect de la vie privée[690].

Le fournisseur d'accès pourrait néanmoins refuser d'accéder à une demande amiable, en invoquant soit des dispositions contractuelles en ce sens, soit le secret professionnel s'il s'estime lié par un tel secret. Pour passer outre ce refus, une injonction à l'encontre du fournisseur d'accès devrait être obtenue auprès d'un juge.

L'obtention des coordonnées d'un éditeur de service d'information

Un service d'information sur l'Internet de type service Web s'analyse en un service de communication audiovisuelle, auquel les dispositions de la loi sur l'audiovisuel sont applicables[691].

---

[685] "Tout journaliste entendu comme témoin sur des informations recueillies dans l'exercice de son activité est libre de ne pas en révéler l'origine".
[686] Civ. 1re 21 juillet 1987, Gaz. Pal. 1988, somm.ann.148.
[687] Civ. 1re 19 mars 1991, D 1991.568.
[688] Voir les décisions citées sous l'article 10 du Mégacode, éditions Dalloz.
[689] Civ. 1re 6 novembre 1990, IR.278.
[690] En ce sens : Paris 1re ch. 21 mars 1988, Jurisdata n°021125.
[691] Voir supra

Il résulte de la combinaison des articles 37 et 43 de la loi du 30 septembre 1986 que le fournisseur d'un service de communication audiovisuel doit tenir en permanence à la disposition du public :

« 1- Si elle n'est dotée de la personnalité morale, les nom et prénom de la ou des personnes physiques propriétaires ou copropriétaires ;

2- Si elle est dotée de la personnalité morale, sa dénomination ou sa raison sociale, son siège social, le nom de son représentant légal et de ses trois principaux associés. »

S'agissant d'une obligation légale, le fournisseur d'accès devrait être tenu de communiquer ces informations si l'éditeur d'un service ne les avait pas mises à disposition du public comme exigé par la loi.

En conclusion, dans toutes les hypothèses où le fournisseur d'accès est situé en France, obtenir les informations nécessaires à l'identification de l'émetteur d'un message ou de l'éditeur d'un service est légalement possible. Si le fournisseur d'accès est localisé à l'étranger, les démarches adéquates devraient être effectuées dans le pays de localisation du fournisseur d'accès selon la loi locale applicable.

Ce schéma est compliqué par la possibilité d'émettre sur l'Internet des messages anonymes.

L'anonymat sur l'Internet

Il existe sur l'Internet différents outils qui permettent d'envoyer des messages de manière anonyme[692].

Il est possible de faire transiter un message par un « anonymous remailer », un réexpéditeur anonyme, qui supprime avant de réexpédier le message les informations sur l'émetteur, et les sites par lesquels il a transité, éléments qui permettent de remonter jusqu'au fournisseur d'accès de l'émetteur du message.

Evidemment, l'anonymat constitue un obstacle sérieux à la mise en cause de l'auteur d'une information. L'anonymat est beaucoup critiqué, mais il présente également des aspects positifs[693].

Avantages et inconvénients de l'anonymat sur l'Internet

Les inconvénients

Les communications anonymes facilitent les activités illicites et immorales en empêchant de retrouver l'identité de l'auteur de l'information illégale.

L'incitation à la haine raciale, à la violence, la diffamation, la désinformation, la dissémination de matériel pornographique, la violation des droits de propriété intellectuelle et des secrets de fabrique sont encouragés par le sentiment d'impunité que procure l'anonymat.

---

[692] On trouve des informations en ligne sur les réexpéditeurs anonymes à : <http://www.cs.bekerley.edu/~raph/remailer.list.html>.

[693] Sur les aspects juridiques de l'anonymat, voir :

A. Michael Froomkin, Anonymity and its Enmities, 1995, Journal of Online Law, article. 4, <http://warthog.cc.wm.edu/law/publications/jol/>,

A. Michael Fromkin, Flood Control on the Information Ocean : Living with Anonymity, Digital Cash, and Distributed databases, article présenté à la conférence du 21 septembre 1995 de la faculté de droit de l'université de Pittsburgh, publié dans le symposium Volume of the University of Pittsburgh Journal of Law and Commerce 1996, disponible à : <http://www.law.miami.edu/~froomkin/> ; D. Post, Pooling Intellectual Capital : Thoughts on Anonymity, Pseudonymity, and Limited Liability in Cyberspace, présenté à la conférence des 3 et 4 novembre 1996 de la faculté de droit de Chicago, <http://www-law.lib.uchicago.edu/forum/96vol.htm>.

Par exemple, le 9 septembre 1994, un anonyme a posté sur une liste de diffusion un code source qui serait celui de RC4, un algorithme de cryptographie propriétaire[694].

Un exemple frappant des méfaits de l'anonymat qui a choqué l'Amérique est celui de ce message anonyme posté sur l'Internet peu après l'attentat terroriste d'Oklahoma City : « Recevoir les informations détaillant les composants et les matériaux nécessaires pour construire une bombe identique à celle d'Oklahoma ? L'information détaille spécifiquement la construction, le déploiement et la détonation d'engins à haut pouvoir explosif. Elle inclut également des détails complets de la bombe utilisée à Oklahoma, comment elle a été utilisée et comment cela aurait pu être mieux[695]. »

L'anonymat empêche l'application de la loi, en rendant difficile, voire impossible l'obtention d'informations sur la personne responsable d'un acte dommageable.

Il supprime la notion de responsabilité de ses actes et de ses paroles.

Les avantages

L'anonymat peut être aussi utilisé à des fins tout à fait légitimes.

Il peut permettre à des minorités politiques, religieuses ou ethniques, des dissidents de s'exprimer sans craindre des représailles contre eux-mêmes ou des membres de leur famille.

Des activités illégales pourraient être dénoncées sans risque de perdre sa place. Certains objecteront que dans ces situations, le caractère anonyme de l'information lui ôte toute crédibilité, que dans certains pays, le problème n'est pas tant la possibilité de pouvoir s'exprimer de manière anonyme que d'avoir accès à l'Internet et de pouvoir communiquer avec l'extérieur, ou encore que la dénonciation anonyme s'apparente plus à de la délation qu'à un acte civique.

Un autre domaine où le droit à l'anonymat peut s'avérer important est celui de la protection de la vie privée.

Par exemple, dans le cadre d'interventions dans des forums consacrés à des questions médicales ou psychologiques, une personne peut souhaiter rester anonyme pour des raisons d'ordre personnel (victime d'une agression sexuelle, personne séropositive par exemple). Il faut savoir en outre que les contributions faites dans les newsgroups sont archivées sur des sites en libre accès sur le Web, où en faisant une simple recherche sur le nom, on peut retrouver les messages envoyés par une personne il y a plusieurs mois[696].

La compilation et l'analyse de données disséminées sur l'Internet sont rendues possible par les nouvelles techniques qui permettent d'organiser et de trier les données.

Certains défendent l'idée que l'anonymat est un moyen pour l'utilisateur de lutter contre de telles pratiques[697].

Les différents degrés d'anonymat

L'anonymat relatif ou traçable

Un message anonyme est un message qui ne fournit aucune information sur l'identité de l'expéditeur. La traçabilité mesure la facilité avec laquelle on peut obtenir des informations additionnelles sur l'identité de l'émetteur.

Il existe plusieurs types de réexpéditeurs ou serveurs de courrier anonyme.

---

[694] Cité par A. Michael Froomkin, Flood Control on the Information Ocean : Living with anonymity, Digital Cash, and Distributed Databases, préc.

[695] Déclaration d'un sénateur cité par David Post, Thoughts on Anonymity, Pseudonymity and Limited Lialibility in Cyberspace, préc.

[696] Notamment sur Dejanews : <http://www.dejanews.com>.

[697] A. Michael Froomkin, Flood Control on the Information Ocean : Living with anonymity, Digital Cash, and Distributed Databases, préc.

Certains réexpéditeurs conservent dans leur base de données les informations sur l'origine du message qui a transité par leur service. Le serveur donne simplement une adresse anonyme qui permet d'envoyer et de recevoir des messages de façon anonyme.

Le serveur de courrier anonyme le plus connu était celui de Johan Helsingius, en Finlande, <annon.penet.fi>[698]. Cependant, Johan Helsingius a fermé son serveur fin août au motif que « les problèmes juridiques concernant l'Internet en Finlande ne sont pas tranchés. La protection légale des utilisateurs doit être clarifiée. Pour le moment, le caractère privé des messages circulant sur l'Internet n'est pas garanti juridiquement »[699].

Si le destinataire du message ne connaît pas l'origine du message, en revanche le réexpéditeur le connaît et peut être amené à la divulguer sur demande judiciaire. Même si la démarche est plus compliquée, elle n'est pas impossible, comme le montre l'exemple de l'église de scientologie, qui en février 1995, a réussi à obtenir la coopération de la police finlandaise pour obtenir un mandat contre le serveur finlandais afin qu'il communique le nom d'un utilisateur qui, selon elle, avait fait usage de son serveur anonyme pour poster des documents dans un forum de discussion en violation de ses droits d'auteur.

Les auteurs des messages identifiés, l'église de scientologie les a ensuite assignés devant les tribunaux américains (il s'agissait de citoyens américains)[700].

Dans ce type de serveur, le respect de l'anonymat repose en réalité entièrement sur la confiance de l'utilisateur en l'administrateur du site. De plus le message envoyé au serveur ne devient anonyme que lorsqu'il atteint le réexpéditeur. Ce système, s'il est très facile d'utilisation, est loin d'être infaillible et n'est pas assez sûr pour des activités illégales.

L'anonymat intraçable

D'autres réexpéditeurs permettent un anonymat total car ils ne conservent aucune donnée permettant d'identifier leurs utilisateurs, aucune trace de l'adresse de départ[701].

Voici un exemple de message reçu d'un tel remailer :

```
_____________________________________________________________
Received : from abraham.cs.berkeley.edu (128.32.37.121) by aqueduc.argia.fr
(EMWAC SMTPRS 0.80) with SMTP id <B0000033342@aqueduc.argia.fr>;
Sat, 07 Sep 1996 13:15:04 +0200
Received : (from daemon@localhost) by abraham.cs.berkeley.edu (8.7.5/local) id EAA15279
for sedallian@argia.fr; Sat, 7 Sep 1996 04:10:23 -0700
Date : Sat, 7 Sep 1996 04:10:23 -0700
Message-Id : <199609071110.EAA15279@abraham.cs.berkeley.edu>
subject : http://www.HIPCRIME.com
To : sedallian@argia.fr
From : nobody@cypherpunks.ca (John Anonymous MacDonald)

Comments : There is no way to determine the originator of this message. If you wish to be
blocked from receiving all anonymous mail, send your request to the <remailer-
operators@c2.org> mailing list.
The operator of this particular remailer can be reached at <remailer-
admin@cypherpunks.ca>.
(Commentaire : il n'y a aucun moyen de déterminer l'origine de ce message. Si vous voulez
bloquer les messages anonymes, envoyez votre requête à la liste de diffusion <remailer-
operators@c2.org>. L'administrateur de ce remailer peut être joint à <remailer-
admin@cypherpunks.ca>.)
```

[698] Voir l'interview qu'il a accordé au journal *Libération*, supplément multimédia, 3 mai 1996, p. V.
[699] Communiqué de presse du 30 Août 1996.
[700] "Alt.scientology.war", magazine Wired, décembre 1995, p. 172.
[701] Cas par exemple du serveur de Community Connexion : <http://www.c2.org>.

Dans ce cas, le réexpéditeur qui a permis l'envoi d'un message anonyme intraçable risque de voir sa responsabilité recherchée, à défaut de pouvoir remonter jusqu'à l'auteur du message.

Une personne qui gère un de ces serveurs de courrier anonyme racontait ainsi qu'elle avait été contactée par le FBI, son serveur ayant servi à réexpédier des messages de menace. Son serveur ne conservant pas la trace des messages transitant par son serveur, elle se demandait si sa responsabilité pouvait être engagée[702].

De tels remailers n'existent pas en France, où d'une manière générale, l'anonymat est assez mal perçu par les internautes.

L'anonymat absolu

Des personnes ayant de très bonnes compétences techniques sont en mesure d'envoyer des messages anonymes et intraçables sans passer par des réexpéditeurs. Cela n'est pas à la portée du grand public, mais il faut savoir que cela peut arriver.

Perspectives

Le fait que l'anonymat soit utilisé dans le but de nuire à autrui ou à la société en général n'est pas nouveau. Les corbeaux, les lettres anonymes, les dénonciations malveillantes n'ont pas attendu l'Internet. Les nouveaux moyens techniques, en facilitant le recours à l'anonymat dans le cadre d'un réseau de communication international, rendent le problème de société posé par l'anonymat plus flagrant.

Les Etats vont vouloir réglementer, afin de contenir les aspects négatifs des communications anonymes.

La section 502 de la loi américaine sur les télécommunications prévoit ainsi qu'est un délit le fait de faire un appel téléphonique ou d'utiliser un outil de télécommunication, sans révéler son identité et avec l'intention d'importuner, d'insulter, de menacer, de harceler toute personne au numéro appelé, ou qui reçoit la communication[703].

Le problème est qu'il suffit que d'autre pays avec des connexions adéquates aux réseaux informatiques internationaux soient plus libéraux envers les communications anonymes pour que la législation édictée dans un autre pays sur l'anonymat soit contournée. Par exemple, il n'existe pas de réexpéditeurs anonymes en France, ce qui n'empêche pas toute personne connectée à l'Internet depuis la France de pouvoir accéder aux services offerts par les réexpéditeurs anonymes.

L'utilisation du courrier électronique pour effectuer mises en demeure et notifications

Mises en demeure, notifications, injonctions, assignations, convocations à comparaître doivent pouvoir être délivrées à une personne physique ou morale disposant d'une adresse où elle peut être touchée.

Des avocats londoniens, du cabinet Schilling and Lom ont obtenu l'autorisation d'un juge de délivrer une injonction par courrier électronique à une personne qui avait envoyé à leur cabinet des messages menaçant de diffuser sur l'Internet des documents diffamatoires

[702] Hal Finney, Law & Policy of Computer, Cyberia-L, <CYBERIA-L@LISTSERV.AOL.COM>, 20 mai 1996.
[703] Section 502 du Telecommunication Act de 1996.

concernant l'un de leurs clients. Ils devaient prouver que le défenseur avait reçu le courrier en utilisant la fonction « accusé de réception » de leur logiciel de courrier électronique[704].

Du point de vue de la sécurité juridique, la solution est discutable : obtenir un accusé de réception d'un serveur signifie que le message a été délivré au serveur de courrier électronique, pas que le destinataire du message a effectivement été chercher son courrier électronique ou ait été en mesure de le faire.

Le seul moyen d'être certain qu'un message a été délivré à son destinataire, est un retour formellement identifié de celui à qui on écrit et qui confirme cette réception.

Une telle utilisation du courrier électronique serait-elle envisageable en France ?

En droit français, une notification doit être effectuée selon les formes prévues par les articles 651 et suivants du Nouveau Code de procédure civile.

Dans certains cas, les notifications sont obligatoirement effectuées par acte d'huissier. Les notifications ordinaires sont faites selon l'article 667 « sous enveloppe ou pli fermé, soit par la voie postale, soit par la remise de l'acte au destinataire contre émargement ou récépissé ».

Comme on peut le constater, les moyens évoqués font explicitement référence à un envoi postal ou à une remise directe, ce qui exclut des méthodes modernes comme la télécopie, sans parler du courrier électronique.

Certains textes prévoient expressément l'utilisation de moyens spécifiques pour l'accomplissement de certaines formalités, ce qui fait obstacle au recours aux nouveaux moyens de communication.

Par exemple, l'article 105 du Code de commerce prévoit que la protestation motivée adressée au transporteur doit être effectuée par acte extrajudiciaire (acte d'huissier) ou par lettre recommandée. La Cour de cassation a donc déclarée inopérante une réclamation effectuée par télex[705].

De même, l'article 950 du Nouveau Code de procédure civile exige que la déclaration d'appel contre une décision en matière gracieuse soit effectuée par une déclaration faite ou adressée par pli recommandé au secrétariat greffe de la juridiction ayant rendu la décision. La Cour de cassation a logiquement estimé que l'envoi d'une télécopie ne répondait pas à ces conditions et qu'en conséquence la déclaration d'appel était nulle[706].

En matière d'assurance, l'article L114-2 du Code des assurances exige l'envoi d'un lettre recommandée avec avis de réception pour interrompre la prescription.

D'une manière générale, toutes les fois que la loi exige l'envoi d'un recommandé avec accusé de réception, cette formalité légale ne peut être remplacée ni par une télécopie, ni par un courrier électronique.

L'usage du courrier électronique pour effectuer des mises en demeure supposerait que les logiciels de courrier électronique intègrent des mécanismes assurant la non-répudiation, l'intégrité et une fonction d'accusé de réception des messages reçus, c'est-à-dire qu'ils puissent fournir une garantie équivalente à l'envoi d'une lettre recommandée avec accusé de réception.

Les juges sont parfois hostiles envers les nouvelles technologies de communication. Dans un domaine où il était prévu qu'un recours était formé par déclaration orale ou écrite, faite, remise ou adressée au secrétariat greffe du tribunal d'instance, la Cour de cassation a considéré comme irrecevable le recours formé par télécopie[707].

---

[704] Robert Uhlig, Libel writ served by e-mail, Electronic Telegraph, 1st may 1996, <http://www.telegraph.co.uk>.
[705] Com. 30 novembre 1993, Droit de l'Informatique et des Télécoms 1994/2, p.24, note Huet.
[706] Cass. 2e 8 juin 1995, AGRP c/ Groussard, Petites Affiches 1er mars 1996, p. 8 note Huet.
[707] Civ. 2e 8 juin 1995, Préfet du Tarn-et-Garonne c/ Maurette et autres, Petites Affiches, 1er mars 1996, p. 8 note Huet.

Dans cette affaire, considérer que l'envoi d'une télécopie n'était pas admissible ne s'imposait nullement au regard du texte considéré[708].

Toutes les juridictions ne se montrent pas aussi hostiles à l'utilisation de la télécopie dans le cadre d'une procédure[709].

On peut aussi citer la décision du directeur de l'INPI d'autoriser le dépôt des demandes de brevet, d'enregistrements des marques, de déclarations de renouvellement de marque et de dépôt des dessins et modèles par télécopie[710].

[708] Note J. Huet, sous l'arrêt préc.

[709] Le juge administratif semble plus libéral que le juge judiciaire : voir l'étude sur la valeur juridique de la télécopie en matière de procédure, Les notes bleues de Bercy, n°70, 1-15 septembre 1995.

[710] BOPI 95/28, vol. 2.

Deuxième partie

La preuve des faits

Sur le principe, rien ne s'oppose à l'utilisation des données électroniques comme mode de preuve parmi d'autres. Pour les faits, la preuve est libre, elle peut être apportée par tous moyens.

Cependant, comme avec la preuve en matière contractuelle, se pose la question de la valeur probante des documents numériques.

Les techniques informatiques ont la particularité de rendre les manipulations très aisées.

Par exemple, les versions les plus récentes du logiciel de navigation de Netscape permettent de faire une modification en local des pages d'un service Web, sur l'ordinateur de l'utilisateur du consultant. Le site, hébergé sur un serveur quelconque relié au réseau, n'aura pas été modifié.

En matière civile, le demandeur doit apporter la preuve de ce qu'il avance. Si une personne estime que les informations disponibles sur un service, ou les messages diffusés par une personne portent atteinte à ses droits et lui sont préjudiciables, il devra trouver un moyen de fixer une information disponible sous forme électronique sur un support tangible aisément consultable par le juge et les parties.

Dans un certain nombre d'hypothèses, un tirage papier de ce qui est disponible à l'écran (on parle de capture d'écran) lorsque l'on se connecte sur le service incriminé pourra suffire.

Cependant, l'information disponible sur l'Internet est volatile et susceptible d'évoluer dans le temps. Une page Web peut être très facilement modifiée par son éditeur, un message envoyé dans un newsgroup peut être annulé par l'envoi de la commande adéquate.

De plus, un procès peut durer plusieurs mois, voire plusieurs années, délai pendant lequel les sites Internet peuvent disparaître, changer d'adresse, voir leur contenu renouvelé.

Le défendeur pourrait être tenté de supprimer les informations incriminées et prétendre ensuite qu'elles n'ont jamais figuré sur son site, arguant de ce que les données ont été manipulées avant d'être recueillies.

Il va donc se révéler nécessaire de constituer des preuves attestant sans contestation possible un état donné, une situation de fait à une date certaine. La manière dont la preuve sera recueillie devra être la plus fiable possible, au besoin en ayant recours aux services d'un expert.

Deux moyens peuvent être utilisés à cette fin : le constat et la saisie.

Le constat

Les huissiers sont des officiers ministériels dont les constatations font foi jusqu'à inscription de faux, une attaque particulièrement grave.

Un huissier peut intervenir à la demande d'une personne qui sollicite son concours de sa propre autorité.

Il est cependant nécessaire d'obtenir une autorisation d'un juge si le constat est réalisé dans un lieu privé même s'il est accessible au public : magasin, cinéma ou encore cybercafé.

Les demandes de mesure sont généralement fondées sur l'article 145 du Nouveau Code de procédure civile qui précise que :

« S'il existe un motif légitime de conserver ou d'établir avant tout procès la preuve de faits dont pourrait dépendre la solution d'un litige, les mesures d'instruction légalement admissibles peuvent être ordonnées à la demande de tout intéressé, sur requête ou en référé. »

La condition exigée pour obtenir la mesure demandée est souple : un motif légitime. Cette condition s'apprécie par rapport à trois critères : le demandeur doit montrer qu'il existe d'ores et déjà des raisons suffisantes de penser qu'un litige pourrait naître, que les faits dont il s'agit d'établir ou de conserver la preuve sont utiles et pertinents à la solution du litige et qu'il y a un risque de dépérissement de preuve.

Cependant, la mesure ordonnée ne doit pas porter atteinte aux intérêts légitimes de l'autre partie comme le secret des affaires.

Pour ménager l'effet de surprise, les constatations sont généralement ordonnées de manière non contradictoire par voie d'ordonnance sur requête.

L'huissier ne doit procéder qu'à des constatations matérielles, ne relever que des éléments de fait. Il ne doit pas en tirer de conséquences, interpréter ce qu'il voit, il ne doit exprimer aucun avis. Il peut joindre à son constat des photographies. Dans notre cas, il pourra s'agir d'impressions de captures d'écran.

En matière de réseaux informatiques, le risque n'est pas tant que l'huissier donne un avis outrepassant son rôle de constatant, mais que faute de maîtriser les aspects techniques, il dresse un constat qui soit insuffisant ou qui ne soit pas satisfaisant.

Il a, par exemple été jugé que faute d'éléments de comparaison et surtout de connaissances techniques suffisantes de l'huissier en matière informatique, un constat ne permet pas de dire si un logiciel est bien le même ou présente des similitudes suffisantes avec un autre logiciel pour que la violation d'une cause d'exclusivité puisse être retenue[711].

Or, un huissier ne maîtrise pas nécessairement la manipulation des différents logiciels utilisés pour consulter les diverses applications de l'Internet, et ne connaît pas nécessairement les méthodes pour effectuer des recherches, retrouver une information sur l'Internet, savoir par quels serveurs un message est passé.

Une partie pourrait, par exemple, être tentée de remettre en cause les conditions dans lesquelles le constat aura été effectué.

C'est ce qui est arrivé dans l'affaire UEJF où le juge a relevé au sujet d'un constat d'huissier produit par l'UEJF que :

(…) « sans qu'il soit le moins du monde question de suspecter la bonne foi des intervenants, diverses incertitudes existent, notamment en ce qui concerne le processus exact de la démonstration opérée devant le constatant, manifestement profane en la matière, par un étudiant dont l'identité n'est d'ailleurs point fournie »[712].

[711] Paris 4e Ch., 24 février 1993, DIT 95/3 p. 33.
[712] TGI Paris, référé, 12 Juin 1996 REF : 53061/96, décision reproduite en annexe.

En fonction des circonstances, il pourrait donc être demandé au juge que l'huissier soit accompagné d'un technicien, qui sera évidemment extérieur au demandeur et ne sera pas notamment un de ses salariés.

On pourrait aussi imaginer le recours à huissier ayant l'habitude de se connecter à l'Internet, qui serait à même de réaliser les constatations depuis son office, ce qui supprimerait toutes discussions sur les possibles manipulations des outils informatiques utilisés.

En effet, si pour faire un constat dans sa propre entreprise ou à son propre domicile, une autorisation du juge n'est pas nécessaire, une partie de mauvaise foi pourrait, soit remettre en cause les conditions de l'opération, soit procéder à des manipulations sur son ordinateur que l'huissier ne sera pas en mesure de déceler.

En droit, les constatations doivent être considérées comme de simples moyens de renseignements. Les parties peuvent en contredire librement la portée.

En pratique, les constatations effectuées peuvent se révéler déterminantes en terme de preuve.

En matière de droit d'auteur, il peut être possible de demander à des agents assermentés de sociétés d'auteur de procéder à des constats d'infraction. L'APP, Agence pour la protection des programmes, s'est par exemple vue dotée de la possibilité d'avoir de tels agents assermentés par un arrêté du ministère de la Culture en date du 21 mars 1996.

La saisie

Un simple constat de ce que l'on trouve lorsqu'on se connecte sur un site particulier ne va pas être toujours suffisant. Il peut se révéler nécessaire de faire procéder à une saisie des disques informatiques de l'adversaire.

En matière de contrefaçon de logiciels, la procédure est connue. Elle est organisée par l'article L332-4 du Code de la propriété intellectuelle :

« En matière de logiciels, la saisie-contrefaçon est exécutée en vertu d'une ordonnance rendue sur requête par le président du tribunal de grande instance. Le président autorise, s'il y a lieu, la saisie réelle.

L'huissier instrumentaire ou le commissaire de police peut être assisté d'un expert désigné par le requérant.

A défaut d'assignation ou de citation dans la quinzaine de la saisie, la saisie-contrefaçon est nulle.

En outre, les commissaires de police sont tenus à la demande de tout auteur d'un logiciel protégé par la présente loi ou de ses ayants droit, d'opérer une saisie-description du logiciel contrefaisant qui peut se concrétiser par une copie. »

La saisie réelle est une mesure grave puisqu'elle tend à déposséder le saisi de ses disques durs où sont mémorisés les programmes, en vue de faire obstacle à la poursuite de toute exploitation des logiciels estimés contrefaisants.

Lorsque la saisie, comme c'est généralement le cas, est effectuée à des fins probatoires, on effectue en pratique une saisie-description, qui peut se concrétiser par une copie du programme informatique litigieux et des éléments associés.[713]

D'autres saisies sont organisées par le Nouveau Code de la propriété intellectuelle.

[713] Voir Claire Jarlaud Lang, La contrefaçon de logiciels : Aspects théoriques et pratiques, Gazette du Palais du 8 octobre 1991, p. 6.

En matière de marques, l'article L716-7 du Code de procédure civile prévoit que :

« Le titulaire d'une demande d'enregistrement, le propriétaire d'une marque enregistrée ou le bénéficiaire d'un droit exclusif d'exploitation est en droit de faire procéder en tout lieu par tout huissier assisté d'experts de son choix, en vertu d'une ordonnance du président de grande instance rendue sur requête, soit à la description détaillée avec ou sans prélèvement d'échantillons, soit à la saisie réelle des produits ou des services qu'il prétend marqués, offerts à la vente, livrés ou fournis à son préjudice en violation de ses droits. »

De même, l'article L521-1 du Code de la propriété intellectuelle prévoit qu'une partie peut, sur production du certificat de dépôt, faire procéder à une description, avec ou sans saisie, des objets en cause, sur ordonnance.

Les textes évoquent la possibilité d'effectuer des saisies d'échantillons. Il est vrai que le terme « échantillon » ne convient guère en matière de données sur support électronique. Mais la demande d'autorisation de saisie-description pourrait tout à fait prévoir la possibilité de faire une copie des disques informatiques, fondée au besoin sur le droit commun des mesures d'instructions.

En effet, s'il apparaît nécessaire d'effectuer une saisie-description à des fins probatoires hors des cas où une procédure de saisie autonome a été spécifiquement aménagée par la loi, rien n'empêche de faire une demande aux fins de saisie sur le fondement du droit commun, à savoir l'article 145 du Nouveau Code de procédure civile examiné ci-dessus.

Compte tenu de la spécificité de la matière, l'assistance d'un technicien va certainement se révéler nécessaire. Son intervention devra être prévue dans l'ordonnance pour éviter toute contestation sur ce point.

En matière de marque la jurisprudence de la Cour d'appel de Paris considère toutefois que la présence du conseil en propriété industrielle du requérant ne remet pas en cause la régularité de la saisie[714].

[714] Paris, 18 avril 1985, Ann. 1984 tome 3, p. 243.

Troisième partie

Aspects internationaux

Le caractère international du réseau va nécessairement multiplier les situations de conflit avec un élément d'extranéité, c'est-à-dire un élément étranger au sens de non français.

Par exemple, une entreprise constate qu'un nom de domaine correspondant à une marque dont elle est titulaire en France et dans d'autres pays européens a été déposé par un concurrent ou une société exerçant une activité similaire à la sienne.

Un site Web hébergé aux Etats-Unis reproduit sans autorisation un livre dont l'éditeur est une société française.

Un message qui a été posté depuis le Canada dans le newsgroup <fr.soc.divers> porte atteinte à la réputation d'une personne domiciliée en France. Si l'ensemble des faits avait été réalisé en France, et qu'une suite judiciaire était envisagée, le tribunal compétent, le bienfondé d'une demande, les chances de succès sont connus du praticien.

Le caractère international du litige complique nécessairement les choses : la situation juridique pouvant se rattacher à plusieurs pays, il va falloir choisir entre différentes lois, entre différents tribunaux, parfois demander d'appliquer à un tribunal une loi qui n'est pas la sienne. Toutes ces questions relèvent de ce que l'on appelle le droit international privé.

Le droit international privé ne met pas directement en cause comme en matière de droit pénal, la souveraineté des Etats. Il concerne les litiges qui surviennent entre personnes privées.

Son développement suppose nécessairement un développement des relations et des échanges internationaux, tous deux grandement facilités par les réseaux informatiques internationaux.

Avant d'examiner si les règles du droit international vont pouvoir s'appliquer aux litiges survenant sur l'Internet, ou si de nouvelles solutions devront être trouvées pour tenir compte de la spécificité des réseaux, il convient de rappeler les principes du droit international privé[715].

Les principes du droit international privé

Chaque fois qu'une situation juridique peut être rattachée à plusieurs pays, et compte tenu du fait que les droits internes de ces différents pays peuvent apporter une solution différente à un même problème, il est indispensable de déterminer la loi qui sera appliquée au litige, loi française ou étrangère.

[715] Sur le droit international privé, voir notamment : Batiffol et Lagarde, Droit international privé, LGDJ, 8e édition 1993 ; P.Guiho, Le droit international privé, l'Hermès 1995 ; Y. Loussouam et P. Bourel, Droit international privé, précis Dalloz, 4e édition 1993, utilisé comme ouvrage de référence.

Dans les litiges présentant un caractère international, il y a conflit de loi lorsqu'il faut choisir, entre plusieurs lois, celle qui sera utilisée pour régir le rapport de droit considéré, et conflit de juridiction lorsqu'il faut déterminer si les tribunaux français sont ou non compétents.

Les principes régissant la détermination de la loi applicable

Chaque Etat a son propre système de solution de conflits de lois : le juge détermine la loi applicable en se référant à ses propres règles de conflit de loi.

Il s'agit d'une règle universelle.

Pour choisir la loi applicable dans chaque cas, on se réfère à des catégories dites de rattachement, qui correspondent aux grandes catégories du droit privé.

Par exemple, pour tout ce qui concerne l'état et la capacité des personnes (état civil, nom, mariage, divorce, filiation), la loi applicable est déterminée en fonction soit de la nationalité, soit du domicile de la personne.

En matière de biens immobiliers, on applique la loi de situation de l'immeuble[716] pour des raisons pratiques évidentes.

Les contrats relèvent de la loi d'autonomie, c'est-à-dire de la loi désignée par les parties dans le contrat.

Les faits juridiques (exemple : un accident de voiture) relèvent de la loi du pays sur le territoire duquel ils sont survenus[717]. En cas d'accident survenant en Espagne, la loi espagnole sera appliquée.

Evidemment il y a des nuances, des cas particuliers, des exceptions.

Le détail des règles particulières et propre à chaque matière sortirait du cadre de cet ouvrage, mais les grandes catégories évoquées sont appliquées dans la plupart des pays.

La règle de conflit de loi peut parfaitement conduire à l'application d'une loi étrangère par le juge saisi du litige.

Dans certaines hypothèses, cette loi étrangère normalement compétente va être écartée, lorsque l'on estime qu'elle contient des dispositions inadmissibles, qu'elle est en contradiction avec nos conceptions fondamentales. Par exemple, un étranger ne peut pas se marier en France si son premier mariage n'est pas dissous, même si sa loi nationale admet la polygamie. De 1816 à 1884, le divorce était interdit en France, et les tribunaux français refusaient le divorce aux étrangers dont la loi nationale admettait le divorce.

Parfois l'ordre public est justifié par des impératifs nationaux d'ordre économique.

La loi étrangère normalement compétente va également être écartée lorsqu'il y a fraude à la loi française. En effet, comme les lois divergent d'un pays à l'autre, on peut être tenté de se placer volontairement sous l'empire d'une loi particulière estimée plus favorable pour échapper à la loi normalement applicable.

Dans ces hypothèses, est invoquée l'exception de fraude à la loi. Un exemple célèbre chez les juristes est celui de l'affaire de la princesse de Bauffremont. Cette dernière voulait divorcer pour se remarier, mais le divorce était interdit à l'époque. La princesse obtint une naturalisation dans un autre pays qui acceptait le divorce et se remaria. Le divorce et le remariage furent jugés dépourvus de toute validité en France[718].

---

[716] *Lex rei sitae.*
[717] *Lex loci delicti.*
[718] Cassation 18 mars 1878, S 1878.I.193, note Labbé ; Grands arrêts de la jurisprudence en droit international privé, p. 45 et suivantes.

L'autorité des lois se trouve diminuée si les règles du droit international privé offrent le moyen de se soustraire aux lois normalement applicables pour se placer volontairement sous une législation plus favorable. C'est ce que l'on appelle le forum shopping.

Certes, le procédé suppose de déménager, parfois de changer de nationalité, d'installer son entreprise ailleurs, ce qui n'est pas forcément très pratique et présente des inconvénients qui freineront le phénomène.

Cependant, avec l'Internet, il est très simple de délocaliser un service, ce qui pourrait faciliter d'autant ce type d'opérations.

Selon la jurisprudence française, la fraude suppose l'utilisation volontaire d'une règle de conflit, dans l'intention d'échapper à une disposition impérative de la loi.

Au niveau européen, les délocalisations sont en principe licites, elles sont le corollaire de la liberté d'établissement et de prestation de service.

Une jurisprudence dite « anticontournement » admet cependant que le bénéfice des dispositions du droit communautaire puisse être refusé à un ressortissant qui fait usage des libertés reconnues par le traité de Rome dans le but de se soustraire à la réglementation nationale qui lui était normalement applicable[719].

Une affaire concernant la télévision illustre bien cette jurisprudence. L'audiovisuel néerlandais possède une réglementation particulière pour garantir le pluralisme du système. Les organismes nationaux ne peuvent pas être des chaînes purement commerciales. Pour échapper à cette réglementation, TV 10, chaîne commerciale, s'est établie au Luxembourg et diffuse des programmes à l'intention du public néerlandais : les programmes sont principalement réalisés par des Néerlandais, les messages publicitaires sont réalisés aux Pays-Bas, la chaîne n'a pas conclu de contrat avec des câblo-distributeurs d'autres pays. Compte tenu de ces éléments, les autorités néerlandaises ont refusé à la chaîne de transmettre ses programmes par câble.

A l'occasion de cette affaire, la Cour de justice des communautés européennes a précisé que :

« Les dispositions du traité relatives à la libre prestation des services doivent être interprétées en ce sens qu'elles ne s'opposent pas à ce qu'un Etat membre assimile à un organisme de radiodiffusion national, un organisme de radiodiffusion constitué selon la législation d'un autre Etat membre et établi dans cet Etat, mais dont les activités sont entièrement ou principalement tournées vers le territoire du premier Etat, lorsque cet établissement a eu lieu en vue de permettre à cet organisme de se soustraire aux règles qui lui seraient applicables au cas où il serait établi sur le territoire du premier Etat »[720].

Il y a également une série de cas dans lesquels le juge ne se pose pas la question du choix de la loi car il est obligé d'appliquer aux faits de la cause une loi impérative. Il en existe notamment en matière de droit de la consommation. Ce sont les lois dites de police.

Lorsque la loi étrangère normalement applicable est écartée ou qu'une loi de police s'impose au juge, on applique au litige la loi du for, la loi du tribunal saisi.

A côté des règles traditionnelles, divers traités internationaux viennent tenter de résoudre les problèmes posés par les divergences entre les législations nationales. Certains de ces traités seront évoqués plus loin.

Il faut savoir qu'il existe plusieurs types de traités.

Certains traités tendent à l'unification des règles de conflit.

Il faut en effet savoir que d'un pays à l'autre, les règles de conflit utilisées n'aboutissent pas nécessairement au même résultat, voire sont contradictoires. Par exemple, un juge français

[719] CJCE 3 décembre 1974, Van Binsbergen, Rec. CJCE 1974, p.1299 ; CJCE 3 février 1993, Véronica, Rec. CJCE 1993, I, p.487.
[720] CJCE 5 octobre 1994, TV 10 saet Commissariat voor de Media, aff. C-23/93.

est saisi d'un litige concernant le statut personnel (état et capacité des personnes) d'un Anglais domicilié en France. La règle de conflit de loi française désigne la loi anglaise (loi de la nationalité), dont la règle de conflit désigne elle-même la loi française (loi du domicile).

Si un traité prévoit qu'en matière de statut personnel, on applique la loi du domicile, les pays adhérents au traité n'auront plus entre eux ce type de systèmes.

D'autres traités sont plus ambitieux et tendent à l'unification des règles de fond.

On peut citer par exemple, la Convention de Berne de 1886 sur la propriété intellectuelle ou encore la Convention de Vienne du 11 avril 1980 sur les contrats de vente internationale de marchandises.

Certains traités sont bilatéraux, ils ne concernent que deux pays, d'autres sont multilatéraux, car ils sont passés entre un grand nombre d'Etats.

Un traité suppose toujours quelque part un abandon de souveraineté par l'Etat signataire.

En raison des particularismes des différents systèmes juridiques, des différences culturelles d'un pays à l'autre sur des points parfois ressentis comme fondamentaux, l'adoption de traités internationaux est un processus long et difficile.

Les règles de procédure

Une fois trouvée la loi applicable, il faut déterminer les règles de la procédure civile qui vont régir un litige comportant des éléments internationaux.

Il n'existe pas de tribunaux internationaux : la Cour internationale de justice de La Haye ne peut être saisie que par des Etats, elle statue dans des affaires touchant le droit public, pas le droit privé.

Il faut donc désigner le tribunal qui sera considéré comme compétent pour connaître le litige. Comme en matière de conflits de lois, ce choix se fait en fonction des règles nationales : règles françaises en France, règles allemandes en Allemagne, etc.

Précisons que chaque tribunal national applique ses propres règles de procédure.

En matière contractuelle, il est possible aux parties de prévoir une clause attributive de compétence. Alors qu'en droit interne, ces clauses ne sont valables qu'entre commerçants[721], la Cour de cassation, dans un arrêt en date du 17 décembre 1985, a considéré que les clauses prorogeant la compétence internationale sont licites lorsqu'il s'agit d'un litige international[722].

La bonne marche de la procédure va parfois nécessiter l'obtention de preuves à l'étranger. Les articles 733 et suivant du Code de procédure civile prévoient la possibilité d'adresser des commissions rogatoires internationales. Il faut également signaler la Convention internationale de La Haye du 18 mars 1970 sur l'obtention des preuves à l'étranger en matière civile et commerciale. Cette convention prévoit la désignation dans chacun des Etats contractants d'une autorité centrale ayant pour mission de recevoir les commissions rogatoires émanant d'un autre Etat contractant.

Une fois un jugement obtenu, s'il n'est pas respecté de manière spontanée par la partie condamnée, il faut recourir à l'exécution forcée. Or, un jugement étranger n'est pas directement exécutable : ce jugement étranger relève de l'ordre d'une souveraineté étrangère.

La procédure qui permet de faire reconnaître la validité et la régularité d'un jugement étranger et d'obtenir qu'il ait force exécutoire s'appelle une instance en exequatur.

---

[721] Article 48 du Nouveau Code de procédure civile.
[722] Rev.cr.dr.int.pr., 1986.537, note Gaudemet-Tallon.

Par exemple, une société américaine obtient un jugement à l'encontre d'une société française. La décision du tribunal américain ne sera pas directement exécutable en France : une nouvelle procédure va devoir y être diligentée.

Chaque pays a ses propres règles en ce qui concerne l'exequatur, et selon les systèmes, le contrôle de la décision étrangère est plus ou moins étendu.

Pour obtenir un exequatur en France, diverses pièces sont à produire, dont une traduction jurée de la décision étrangère et un certificat du greffier compétent attestant que la décision rendue présente un caractère définitif.[723]

Le juge français ne procède pas à une vérification du fond de la décision étrangère, mais à une vérification de la régularité du jugement étranger. Depuis un arrêt Munzer du 7 janvier 1964[724], le juge de l'exequatur doit vérifier :

- la compétence internationale du juge étranger qui a rendu la décision ;
- la régularité de la procédure suivie par rapport à l'ordre public international français et au respect des droits de la défense ;
- l'application de la loi compétente d'après les règles françaises de conflit ;
- la conformité à l'ordre public international français ;
- l'absence de fraude à la loi.

Un certain nombre de conventions internationales, bilatérales ou multilatérales, prévoient une procédure différente de celle du droit commun. Des conventions ont ainsi été signées avec de nombreux pays africains, avec la Suisse. Plus récemment, la France a signé le 10 juin 1996 avec le Canada, une convention bilatérale sur l'exécution de décisions judiciaires en matière civile et commerciale.

En Europe, deux conventions particulièrement importantes viennent à la fois fixer des règles concernant la reconnaissance et l'exécution des jugements et les règles de compétence entre juridictions : la Convention de Bruxelles du 27 septembre 1968, entrée en vigueur le 1er février 1973, modifiée, qui s'applique aux Etats membres de l'Union européenne, et la Convention de Lugano du 16 septembre 1988, entrée en vigueur le 1er janvier 1992, qui lie les pays de l'Association européenne de libre Èchange (AELE), c'est-à-dire, outre les pays membres de l'ancienne CEE, l'Autriche, la Suisse, la Finlande, la Norvège, la Suède et l'Islande, et qui a repris les termes de la Convention de Bruxelles.

La Convention de Bruxelles pose le principe que chaque fois que le défendeur est domicilié dans un Etat contractant, l'action doit être portée devant un tribunal de cet Etat. Dans un certain nombre de cas, le défendeur peut être assigné devant le tribunal d'un autre Etat contractant, notamment en matière délictuelle ou contractuelle.

En matière d'exequatur, la convention pose le principe de la reconnaissance de plein droit des décisions rendues dans un Etat contractant sur le territoire des autres. La procédure d'exequatur est simplifiée, et s'effectue par simple requête. L'exequatur est refusé en cas de non-respect de l'ordre public et des droits de la défense.

---

[723] Voir : Guide formulaire de procédure civile, éditions Belleville Reneaux SA, 5e édition, preuve.597 et suivantes ; Camille Bernard, L'exequatur des jugements étrangers, renseignements pratiques sommaires, Gaz. Pal. 1977.2.426.

[724] Civ. 1re 7 janvier 1964, JCP 1964, II, 13 590, note Ancel.

L'application des règles du droit international privé aux litiges survenus sur l'Internet et ses limites

La détermination du juge compétent et de la loi applicable aux litiges survenus sur l'Internet

Le juge compétent en matière délictuelle

Il n'est pas possible de donner un aperçu exhaustif de toutes les situations particulières pouvant survenir, chaque matière appelant ses propres solutions.

Je prendrai comme exemple la détermination du tribunal compétent en matière délictuelle et la détermination de la loi applicable dans quatre matières : les droits de la personnalité, les droits d'auteur, les contrats, le droit de la consommation.

Le juge compétent en matière délictuelle

La matière délictuelle concerne les demandes qui visent à mettre en jeu la responsabilité civile du défendeur et ne se rattachent pas à un contrat. Elle inclut par exemple la contrefaçon, les atteintes à la vie privée, la diffamation, les accidents, etc.

En matière délictuelle, le demandeur a le choix entre attraire le défendeur devant le tribunal de son domicile, ou devant la juridiction du lieu du fait dommageable ou devant celle dans le ressort de laquelle le dommage a été subi.[725]

La Convention européenne de Bruxelles prévoit que le défendeur peut être attrait en matière délictuelle devant le tribunal du lieu où le fait dommageable s'est produit.[726]

La Cour de justice des communautés européennes est venue préciser que le « fait dommageable » pouvait s'entendre comme visant à la fois le lieu où le dommage est survenu et le lieu de l'événement causal[727].

Le droit américain reconnaît également la compétence judiciaire du tribunal du lieu du dommage subi.

Ce principe de compétence a amené un tribunal américain de l'Etat du Missouri à se déclarer compétent pour connaître d'une affaire de contrefaçon de marque reproduite sur un site Internet hébergé sur un serveur localisé dans l'Etat de Californie. Le seul point de contact du défendeur avec le Missouri est le fait que son site Web y est accessible[728].

Dans une autre affaire, le procureur de l'Etat du Missouri a assigné devant les tribunaux du Missouri l'éditeur d'un site Web qui avait fait de la publicité pour son futur service de paris en ligne, localisé dans l'Etat du Nevada. Il est reproché au site du Nevada de violer les lois de l'Etat du Missouri sur la publicité mensongère et la protection des consommateurs[729].

Inversement, un tribunal de l'Etat de New York s'est déclaré incompétent pour connaître d'une affaire en contrefaçon de marque concernant le site Web d'un club de jazz de l'Etat du Missouri. Le juge a considéré que maintenir un site Web qui est accessible partout n'emporte pas automatiquement compétence de toutes les juridictions dans le ressort desquelles le site Web peut être consulté[730].

---

[725] Article 46 du Nouveau Code de procédure civile

[726] Article 5 paragraphe 3

[727] CJCE 30 novembre 1976, D 1977.613

[728] Maritz Inc. v Cybergold, Case N° 96CV01340, US district Court for the Eastern District of Missouri.

[729] State v. Granite Gate Resorts, Inc., District Court, second judicial district, mémoires del'état du Missouri disponibles à : <http://www.state.mn.us/ebranch/ag/>.

[730] Bensusan restaurant v. King, 1996 US Dist. LEXIS 13035, 9 septembre 1996, affaire Blue Note.

Dans une affaire Yves Rocher/BNP, un juge parisien, en réponse à une exception d'incompétence soulevée par Yves Rocher qui ne réside pas à Paris, a considéré que les brochures contenant les accusations portées par Yves Rocher contre le groupe BNP-Banexi ayant été diffusées en différents points du territoire national, notamment à Paris, et ayant été reproduites sur le réseau Internet, accessible également pour tout intéressé à Paris, les requérants étaient en droit de saisir le tribunal de Paris.[731].

En matière de publication, la Cour de justice des communautés européennes est venue préciser que les juridictions de chaque Etat contractant dans lequel la publication a été diffusée et où la victime prétend avoir subi une atteinte à sa réputation, sont compétentes pour connaître des dommages causés dans cet Etat à la réputation de la victime.[732] Dans cette affaire, les victimes avaient saisi une juridiction anglaise en raison d'un article diffamatoire publié dans le journal *France Soir,* dont les exemplaires avaient été distribués en France et dans d'autres pays européens, dont l'Angleterre. Dans le cas d'une diffamation internationale par voie de presse, sont donc compétents le tribunal du lieu d'établissement de l'éditeur de la publication diffamatoire, et dans les lieux où la publication est diffusée lorsque la victime y est connue.

La Cour d'appel de Paris s'est prononcée dans le même sens. Elle considère en outre que les tribunaux français, compétents pour connaître des suites d'une atteinte à la vie privée par voie de presse, du chef du lieu de diffusion d'un magazine, ne peuvent connaître que du dommage directement causé en France par cette diffusion, à l'exclusion de celui éventuellement subi en pays étranger, qui ne se rattache à leur compétence ni par le lieu de réalisation du préjudice, ni par le lieu de l'acte fautif.[733]

Dans une affaire où intervenaient différents organismes de radiodiffusion, en réponse à une exception d'incompétence soulevée par des sociétés de droit luxembourgeoise et monégasque, la Cour d'appel de Paris a précisé que :

« L'implantation des émetteurs utilisés par les stations de radiodiffusion et de télévision dont il s'agit importe peu dès lors qu'il est constant que les émissions sont reçues en France par le public concerné et que c'est de cette réception ne donnant lieu à aucun versement qu'est né en France le préjudice dont réparation est demandée. »

La Cour a néanmoins relevé qu'au fait que le dommage était réalisé en France s'ajoutait la circonstance que le signal de départ doit être considéré comme émis à partir du territoire français.[734]

On voit que le principe de la compétence des tribunaux du lieu du dommage est une compétence assez largement reconnue et appliquée.

En pratique, le tribunal saisi préférera appliquer sa propre loi et non une loi étrangère. La compétence juridictionnelle précède souvent la loi applicable au fond du litige.

Les droits de la personnalité

On peut imaginer une action en responsabilité civile pour obtenir réparation d'une atteinte à l'honneur, à la réputation ou encore à la vie privée.

Dans une affaire où était en cause la protection du droit au respect de la vie privée et à l'image, la Cour de cassation s'est prononcée en faveur de la compétence de la loi du lieu où les faits ont été commis.[735]

En matière de réseaux informatiques internationaux, tout le problème est justement de localiser le lieu du délit : le fait générateur du délit, par exemple le message diffamatoire, peut être envoyé d'un lieu indépendant de la localisation du fournisseur d'accès de l'auteur du mes-

[731] TGI Paris référé, REF 54240/96.
[732] CJCE 7 mars 1995, aff. C-68/93, Rec.1995, I,p.450.
[733] Paris 19 mars 1984, D 1984, I.R.179
[734] Paris 19 décembre 1989, RIDA 1989, p.215..
[735] Civ. 13 avril 1988, Rev.cr.dr.int.pr 1988.546, note Bourel.

sage, et les conséquences dommageables (qui sont un élément du délit) relèvent elles-mêmes d'une troisième localisation, celle de la victime, voire d'une localisation multiple, le lieu de la diffusion.

Ainsi, en matière d'atteinte à la vie privée, il suffit que les données soient diffusées en France, pour que l'article 9 du Code civil relatif à la vie privée s'applique. C'est en tout cas ce qui ressort d'un arrêt de la Cour d'appel de Paris, dans une affaire où les tribunaux français avaient été saisis par le prince Karim Aga Khan pour des propos tenus dans les numéros diffusés en France de l'hebdomadaire britannique *the Mail on Sunday*[736].

Les droits d'auteur

Les droits d'auteur relèvent de la catégorie juridique des biens incorporels. Traditionnellement, en droit international français, les biens relèvent de la loi de localisation des biens.[737]

Le caractère immatériel des droits d'auteur rend l'application de ce critère de rattachement difficile.

La jurisprudence essaie de concilier la compétence de la loi d'origine et de la loi locale, c'est-à-dire du pays dans lequel la protection est réclamée : les droits de propriété intellectuelle doivent être régulièrement acquis dans un pays (publication de l'œuvre ou encore accomplissement des formalités prévues pour obtenir la protection). Les droits régulièrement acquis peuvent être ensuite invoqués dans d'autres pays. Pour la protection de l'œuvre, on applique la loi du pays dans laquelle l'œuvre est exploitée de manière non autorisée, qu'elle y soit reproduite, diffusée, visualisée, ou réceptionnée[738].

Par exemple, la Cour de cassation a considéré que le droit moral (respect de l'intégrité d'une œuvre) accordé aux auteurs en droit français, pouvait être invoqué en France par les héritiers du réalisateur d'un film américain, pour s'opposer à la diffusion d'un film colorisé, bien que le droit américain et les contrats conclus entre le producteur et les réalisateurs permettent la diffusion d'une telle version.[739]

Dans l'affaire des organismes de radiodiffusion évoquée ci-dessus, le litige portait sur la rémunération des artistes interprètes et exécutants dont les prestations, enregistrées sur phonogrammes, avaient été diffusées sans contrepartie par les défenseurs.

Chaque société étrangère revendiquait l'application de la législation de son pays.

La Cour a répondu que « la loi applicable est celle du lieu où le préjudice est réalisé, soit en l'espèce la loi française.[740]

Les contrats

On applique en principe en matière de contrat la loi d'autonomie, c'est-à-dire la loi choisie par les parties. C'est à défaut de choix express que le problème de la loi applicable se pose. Enfin, les contrats conclus avec les consommateurs relèvent de dispositions impératives.

En ce qui concerne en premier lieu la loi applicable à la forme du contrat, on applique en droit international la loi du lieu de conclusion de l'acte[741], un critère difficile à utiliser par hypothèse en matière de réseaux informatiques.

---

[736] Paris 1er février 1989, D 1990.48.
[737] *Lex rei sitae.*
[738] Lamy informatique 1996, n°1951.
[739] Civ.1re 28 mai 1991, aff. Huston, film "Asphalt Jungle", JCP éd. G, II,21 731.
[740] Paris 19 décembre 1989, RIDA 1989, p.215.
[741] *Locus regit actum.*

Les Etats membres de la Communauté européenne se sont dotés d'une convention sur la loi applicable aux obligations contractuelles, la Convention de Rome du 19 juin 1980, entrée en vigueur le 1er avril 1991, qui sera évoquée.

Il existe d'autres conventions internationales en matière de contrats, comme la Convention de La Haye sur la loi applicable aux ventes à caractère international d'objets mobiliers du 15 juin 1955, entrée en vigueur le 1er septembre 1964 en France, mais qui ne seront pas traitées dans le cadre de cet ouvrage.[742]

La Convention de Rome du 19 avril 1980 sur la loi applicable aux obligations contractuelles prévoit en son article 9-2 que :

« Un contrat conclu entre des personnes qui se trouvent dans des pays différents est valable quant à la forme s'il satisfait aux conditions de forme de la loi qui le régit au fond en vertu de la présente convention ou de la loi de l'un de ces pays. »

Cependant, le problème de la forme du contrat n'est pas *a priori* essentiel en matière d'Internet : les contrats soumis à des règles de formes particulières (par exemple, contrat de mariage, testament, contrat de vente immobilière, donation) ne sont pas ceux qui sont couramment pratiqués sur l'Internet. Les contrats courants de la vie civile et commerciale ne posent généralement pas de problème de forme, la plupart des pays reconnaissant le principe que les contrats se forment par le seul échange des consentements, sans formalité particulière.

En ce qui concerne en second lieu la loi au fond, en l'absence de choix explicite ou implicite, les juges doivent rechercher, « d'après l'économie de la convention et les circonstances de la cause, quelle est la loi qui doit régir les rapports des contractants »[743]. Les juges recherchent des indices particuliers et se réfèrent, en l'absence ou en l'insuffisance de ces indices généraux aux deux critères suivants : lieu d'exécution ou lieu de conclusion du contrat. Ces critères sont assez inadaptés en matière d'Internet : la conclusion du contrat s'effectue à distance, l'exécution peut être réalisée dans plusieurs pays ; le paiement dans l'un, la livraison dans l'autre.

La Convention de Rome du 19 juin 1980 précise qu'en l'absence de choix, le contrat est régi par la loi du pays avec lequel il présente les liens les plus étroits[744], ce qui ne nous éclaire pas davantage.

La convention précise toutefois que :

« Il est présumé que le contrat présente les liens les plus étroits avec le pays où la partie qui doit fournir la prestation caractéristique a, au moment de la conclusion du contrat, sa résidence habituelle ou, s'il s'agit d'une société, association ou personne morale, son administration sociale. »

La prestation caractéristique, c'est celle qui permet de qualifier le contrat : loi du vendeur dans le contrat de vente, loi du donneur de licence dans le contrat de licence.

A défaut de pouvoir utiliser de manière satisfaisante les critères de rattachement habituels, le critère de la prestation caractéristique utilisé par la Convention de Rome semble être adaptable en matière de réseaux informatiques.

Le droit de la consommation

L'article 5-2 de la Convention de Rome prévoit que le choix par les parties de la loi applicable ne peut avoir pour résultat de priver le consommateur de la protection que lui assurent les

[742] le droit international est une matière complexe. L'objectif des développements qui y sont consacrés n'est pas d'être exhaustif sur l'ensemble des traités et règles de fond du droit international susceptibles de s'appliquer à l'Internet, mais de montrer les limites de règles qui n'ont pas été conçues pour un environnement informatique.

[743] Civ. 6 juillet 1959, Rev.cr.dr.int.pr. 1959.708, note Batiffol.

[744] Article 4-loi applicable à défaut de choix.

dispositions impératives de la loi du pays dans lequel il a sa résidence habituelle notamment si « la conclusion du contrat a été précédée dans ce pays d'une proposition spécialement faite ou d'une publicité, et si le consommateur a accompli dans ce pays les actes nécessaires à la conclusion du contrat ».

Or, les services Internet qui peuvent contenir offres et publicités sont consultables partout, et nécessairement dans le pays de résidence du consommateur. En outre, le consommateur accomplit depuis son pays de résidence les actes nécessaires à la conclusion du contrat, même si le lieu de conclusion du contrat est plus difficilement localisable.

De telles dispositions impliquent le respect par le vendeur des lois particulières de tous les pays de l'Union européenne dont relèvent les consommateurs auxquels il vend ses produits, et il ne peut pas y être dérogé par contrat : en droit de la consommation, beaucoup de règles sont impératives.

Il faut également savoir que de telles règles d'application de la loi du lieu de résidence habituelle existent dans d'autres pays non européens. Par exemple, l'article 21 de la loi québécoise sur la protection du consommateur applique également, en droit international privé, la loi du lieu du domicile du consommateur.[745]

Dans le même ordre d'idée, on peut citer l'article L135-1 du Code de la consommation :

« Nonobstant toute stipulation contraire, les dispositions de l'article L132-1 sont applicables lorsque la loi qui régit le contrat est celle d'un Etat n'appartenant pas à l'Union européenne, que le consommateur ou le non-professionnel a son domicile sur le territoire de l'un des Etats membres de l'Union européenne et que le contrat y est proposé, conclu ou exécuté. »

L'article L132-1 est relatif aux clauses abusives considérées comme non écrites.

Ainsi le consommateur français peut invoquer le bénéfice de ces dispositions même dans l'hypothèse où le contrat est soumis à une loi étrangère.

On peut citer comme exemple le contrat proposé par la banque américaine Mark Twain Bank pour l'ouverture d'un compte Ecash Mint[746] qui permet d'effectuer des transactions auprès des commerçants ayant adhéré à ce système[747]. Ce contrat contient plusieurs dispositions qui pourraient être qualifiées d'abusives au sens de la réglementation française[748] ou européenne[749] : clause attributive de compétence au profit de l'Association américaine d'arbitrage[750], clauses relatives à la modification unilatérale des clauses du contrat sans préciser les conditions dans lesquelles elle pourra intervenir[751], clause exonérant la banque de responsabilité en cas de demande écrite du client de corriger un virement depuis ou vers le compte e-cash effectué par erreur[752].

De même, la clause du contrat First Virtual[753] exonérant cette société de toute responsabilité même en cas de faute de First Virtual est abusive[754].

Reste la question de savoir si les juridictions étrangères saisies d'un éventuel litige accepteraient de prendre en compte le droit français.

---

[745] K. Benyerkhlef, Les transactions dématérialisées sur les voies électroniques : panorama des questions juridiques.

[746] Conditions and provisions, World Currency deposit Accounts and Ecash agreement, version du 27 octobre 1995, disponible à : <http://www.marktwain.com/ecash>.

[747] Voir supra

[748] Voir supra

[749] O. Hance, Business et Droit d'Internet, Best Of Editions 1996, p. 164.

[750] Point 1-q) de l'annexe du Code de la consommation

[751] Point 1-i) de l'annexe.

[752] Point 1-b) de l'annexe.

[753] Clause Q8.2 des conditions générales du 16 décembre 1995, disponibles à : <http://www.fv.com/pubdocs/fineprint-buyer.txt>, sur le système proposé par First Virtual voir supra

[754] Point 1 b) de l'annexe au Code de la consommation.

D'un côté, le consommateur qui achète des produits quels qu'ils soient, depuis chez lui, sans faire d'effort particulier autre que de donner l'adresse du service du fournisseur, va s'attendre à être protégé par les lois sur la consommation de son pays.

D'un autre côté, on ne peut raisonnablement exiger d'un fournisseur qu'il respecte simultanément en ce qui concerne ses produits, les lois de tous les pays connectés à l'Internet.

Va-t-on obliger par exemple des sociétés étrangères à traduire leur mode d'emploi en français ? Avant de faire une offre promotionnelle sur son site, le fournisseur devra-t-il au préalable vérifier les dispositions particulières de toutes les lois des pays de résidence de tous ses clients potentiels ?

Prenons l'exemple de la loi sur l'emploi de la langue française[755]. La Cour de cassation a indiqué que l'objectif du texte était la sauvegarde de la langue française et non la protection des consommateurs. La traduction des seules mentions essentielles pour la compréhension des caractéristiques d'un produit ou la passation d'une commande n'est donc pas suffisante : c'est l'intégralité des documents relatifs au produit qui doit être traduite[756].

Mais certains estiment que l'application de la loi française à des marchandises offertes par une entreprise d'un autre Etat membre de l'Union européenne pourrait constituer une « mesure d'effet équivalent » à des restrictions à l'importation contraire au principe de libre circulation des marchandises (article 3 du Traité de Rome)[757].

La Commission européenne a d'ailleurs souligné que :

« Un consommateur français répondant à une publicité parue dans un journal de langue anglaise ou à une émission de télévision en langue allemande ne peut s'attendre à recevoir toutes les informations dans la langue de son pays de résidence. Si le média est diffusé en dehors de sa zone linguistique, et que le consommateur décide de commander, il ne faut pas que la règle linguistique soit un obstacle à ce type de contrat transfrontière »[758].

En outre, en cas de litige, il est peu probable que ces règles assurent de manière efficace la protection des consommateurs. Même si d'un point de vue abstrait, un recours existe, sa mise en œuvre pratique est trop complexe pour qu'il soit sollicité fréquemment, ce qui revient à priver la victime d'un dommage ou d'un préjudice de chances raisonnables d'obtenir réparation.

Ainsi des acheteurs français ont intenté des procès à des sociétés de vente par correspondance allemandes. Les jugements rendus en France ne sont pas exécutés et les tribunaux allemands refusent de poursuivre ces sociétés[759].

Une réponse ministérielle a également évoqué une pratique pouvant constituer le délit d'escroquerie : des entreprises domiciliées à l'étranger envoient des cartes informant le destinataire qu'un objet est à sa disposition et lui sera livré moyennant le paiement d'une somme modique, sans rapport avec la valeur apparente dudit objet. Les objets ne sont pas livrés après versement des fonds. Le consommateur peut porter plainte auprès du procureur de la République compétent. Toutefois lorsque le contentieux résultant de ces litiges porte sur des sommes modiques (moins de 200 francs généralement), des procédures d'entraide répressive internationale sont difficiles à mettre en œuvre [760].

Il n'est en effet guère réaliste d'imaginer que le consommateur va se lancer dans un procès long et onéreux, alors que les enjeux économiques des contrats en matière de consommation restent faibles pris individuellement. Les poursuites sont en pratique difficiles, voire impos-

---

[755] Loi n°75-1349 du 31 décembre 1975 et loi nouvelle n°94-665 d'août 1994, Voir supra

[756] Crim. 20 octobre 1986, Gaz. Pal. 1987.184.

[757] Francis Delbarre, Offres de produits et services, Gaz. Pal. n° spécial sur la vente à distance, 25 février 1993,p .8

[758] Projet de directive du Conseil du 21 mai 1992 sur la protection des consommateurs en matière de contrats négociés à distance, exposé des motifs, JOCE 23 juin 1992, C 156.

[759] Lamy droit économique 1996, n°2688.

[760] Rép.min. n°54 960, JOANQ 6 avril 1992.

sibles. Des mécanismes susceptibles de prendre en compte la délocalisation des réseaux informatiques internationaux vont devoir être imaginés.[761]

Les limites de l'application des mécanismes traditionnels

Classiquement, le territoire d'un Etat délimite la sphère géographique sur laquelle cet Etat a le pouvoir d'édicter des règles et de les appliquer. Les lois d'application extra-territoriale sont rares et se heurtent en tout état de cause à des problèmes pratiques d'exécution.

En revanche avec l'Internet, les cas d'application extra-territoriale de la loi sont nombreux. Bien plus, des systèmes juridiques différents peuvent revendiquer simultanément l'application de leurs règles.

En matière de compétence juridictionnelle, le défendeur peut-il être attrait devant n'importe quelle juridiction d'un pays relié à l'Internet, et au sein de ce pays devant n'importe quel tribunal ? En outre, en application de la jurisprudence évoquée ci-dessus, le demandeur devra-t-il pour obtenir une réparation complète du dommage subi, initier des procédures dans plusieurs pays ?

Au sein de l'Europe, il existe des procédures simplifiées d'exequatur. Ne risque-t-on pas que les juridictions d'un pays donné soient choisies uniquement en raison de leur droit interne plus favorable ?

En matière de droit d'auteur ou de droit de la consommation, toutes les lois nationales ont une sorte de portée extra-territoriale.

L'éditeur d'un site pourra-t-il se voir condamné pour des faits licites au regard de sa loi nationale, mais qui ne le seraient pas dans un des pays relié à l'Internet ? Certes, une incompétence de la juridiction étrangère pourra être soulevée lors de la procédure d'exequatur en France, mais en matière délictuelle, par exemple, les critères sont sensiblement les mêmes d'un pays à l'autre. Il restera le recours à la notion d'ordre public, mais ce n'est pas évident de pouvoir l'invoquer dans toutes les hypothèses. En outre, il existe des procédures simplifiées d'exequatur.

A partir du moment où une œuvre est diffusée sur l'Internet, elle est consultable depuis n'importe quel pays relié à l'Internet. L'application du critère de territorialité des droits d'auteur en matière d'Internet aboutit à l'application cumulative de toutes les législations.

L'application des règles habituelles peut aboutir à un résultat surprenant. A quelle loi est censée se conformer la personne qui met sur place un site Internet ? Peut-on réellement lui conseiller de se renseigner sur toutes les lois nationales des pays reliés à l'Internet, au motif que les règles du droit international privé aboutissent à l'application simultanée de toutes les lois nationales ? Et que doit faire, par exemple, un négociant en vin sachant que certains pays musulmans prohibent l'alcool et certainement toute forme d'information sur le sujet ?

D'un point de vue pratique, l'application stricte de ces règles aboutirait à des situations absurdes. La probabilité d'être assigné dans un pays étranger pour ne pas avoir respecté une loi étrangère puis que la décision soit ensuite exécutée en France est heureusement faible.

De nouvelles règles vont devoir être trouvées qui prennent en compte la nature particulière des réseaux informatiques internationaux.

[761] K. Benyerkhlef, Les transactions dématérialisées sur les voies électroniques : panorama des questions juridiques.

Vers l'émergence de règles spécifiques

L'adaptation des règles classiques du droit international privé

Des règles de conflit de loi spécialement adaptées

Avec l'augmentation des litiges à caractère international, va se poser la question de l'adéquation des règles traditionnelles de conflit de loi.

Les critères de rattachement traditionnels aboutissent à doter toutes les lois d'une portée extra-territoriale absolue, ce qui ne semble pas raisonnable.

Le fait que les critères de rattachement habituels semblent inadaptés à la nature particulière des réseaux informatiques ne signifie pas qu'aucune localisation géographique ne soit envisageable : les serveurs qui hébergent les applications, les auteurs de messages et fournisseurs de service, les destinataires particuliers d'une information sont eux parfaitement localisés géographiquement.

On pourrait remplacer le critère de la loi de réception par le critère de la loi du lieu d'émission, entendu comme le lieu de localisation du serveur, du fournisseur d'accès ou de l'auteur d'un message selon les cas.

Par ailleurs, il devient également aisé de contourner une législation nationale jugée contraignante, en délocalisant le serveur d'hébergement du site. En cas de fraude à une loi nationale particulière, on reviendrait au critère de réception.

Compétence juridictionnelle

Les tribunaux américains ne sont plus unanimes sur la question de la compétence juridictionnelle fondée sur le seul constat qu'un site Web est accessible dans leur juridiction. D'autres affaires sont en cours. En pratique, le défendeur a tendance à saisir le tribunal de son domicile, ce qui réduit à néant le principe traditionnel de la compétence du tribunal du domicile du défendeur. La jurisprudence américaine montre qu'il est possible d'adapter les règles habituelles en matière de compétence pour éviter le recours abusif au forum shopping.

Une juridiction américaine a rendu une décision intéressante en matière d'application extra-territoriale du droit américain à un serveur italien non fondée sur la simple possibilité d'accéder au site depuis le territoire américain.

Une société Tattilo envisageait de publier une version américaine de son magazine pour hommes *Playmen*. La société Playboy obtient un jugement daté du 26 juin 1981 faisant interdiction à la société italienne d'imprimer, de distribuer, et de vendre ce magazine aux Etats-Unis, contrefaisant du sien. En janvier 1996, Playboy découvre que cette même société américaine a créé un site Web « Playmen » dont une partie n'est disponible que sur abonnement préalable. Elle saisit un tribunal américain au motif que la mise en œuvre de ce site Web viole l'interdiction du jugement du 26 juin 1981. Le juge fait droit à sa demande et fait injonction à la société italienne de ne plus accepter d'abonnements venus de clients résidants aux Etats-Unis et de résilier les abonnements antérieurement souscrits par des résidents américains.

A l'appui de service décision, le tribunal relève que Tattilo ne peut pas être empêché d'exploiter son site Internet au seul motif qu'il est accessible depuis un pays dans lequel ce produit est interdit. Cependant cette protection ne peut aller jusqu'à ignorer les décisions des tribunaux. Le tribunal justifie sa décision par le fait que la société italienne a activement sollicité les clients américains à venir sur son site Web, et lorsque l'abonné potentiel faxe le

formulaire adéquat à Tatillo, il reçoit en retour un mot de passe et un identifiant. En agissant ainsi, Tatillo a distribué son produit aux Etats-Unis[762].

Droits de la personnalité

La jurisprudence aurait la solution, en ce qui concerne l'Internet, de rattacher les droits de la personne à son nom, à son image ou au respect de sa vie privée à la catégorie du statut du fait personnel, qui relève en droit international privé français de la loi nationale, ou encore de faire référence à la loi du domicile.[763]

Droits d'auteur

La directive relative à la coordination de certaines règles du droit d'auteur applicables à la radiodiffusion par satellite et par câble qui prévoit le principe de l'application de la loi du territoire à partir duquel l'œuvre est émise :

« Aux fins de la présente directive, on entend par "communication au public par satellite" l'acte d'introduction, sous le contrôle et la responsabilité de l'organisme de radiodiffusion, de signaux porteurs de programmes destinés à être captés par le public dans une chaîne ininterrompue de communication conduisant au satellite et revenant vers la terre »[764].

Les autorités communautaires s'orientent donc vers l'application de la loi du lieu d'émission.

De la même manière que pour les communications par satellites, il serait souhaitable que le principe de la loi d'émission soit adopté en ce qui concerne la diffusion d'œuvres par l'intermédiaire de l'Internet. On pourrait choisir par exemple la compétence de la juridiction dans laquelle est localisé le site mettant à disposition les données incriminées, ou du fournisseur d'accès de l'auteur d'un message, ces deux nœuds de communication constituant le lieu à partir duquel sont émises les données vers le public. L'équivalent du « signal de départ » en matière de radiodiffusion.

Le gouvernement français n'est pas favorable à ce critère, en raison des risques de délocalisation vers des pays moins respectueux des droits d'auteur que cette solution comporterait[765].

Il suffirait de l'aménager pour tenir compte des cas de fraudes, et des lois nationales qui n'apporteraient pas un niveau de protection suffisant des auteurs.

Un auteur propose en matière de droits d'auteur d'appliquer la loi de réception, en limitant la réparation et la compétence du juge saisi, au dommage souffert sur son territoire[766]. Cette solution présente l'inconvénient d'obliger la victime à saisir plusieurs tribunaux si elle veut obtenir réparation de l'intégralité de son préjudice. Or les réseaux internationaux pourraient multiplier les cas de préjudice international. Par exemple, si un site Web reproduit sans autorisation une chanson d'une star mondialement connue, la star subit un préjudice dans tous les pays connectés.

Droit de la consommation

Un auteur propose de faire une distinction pour à la fois concilier la nécessité de protéger le consommateur français et le caractère international de l'Internet :

« Lorsqu'un Français est en voyage à l'étranger, la réglementation française bien évidemment ne s'applique pas. Il doit en être de même pour l'Internet. Si l'offre est à caractère international, le simple fait qu'elle puisse être accédée par des consommateur français ne devrait pas entraîner l'application des lois françaises de protection.

---

[762] Playboy Ents v. Chuckleberry Publishing, Southern Districts of New York, 19 juin 1996, disponible à :<http://www.bna.com/e-law/cases/playmen.html>.

[763] En ce sens, Loussouarn et P.Bourel, Droit international privé, précis Dalloz, 4e édition 1993,n°274-.

[764] Chapitre 1, article 1, § 2 a) de la directive 93/83/CEE du Conseil du 27 septembre 1993 relative à la coordination de certaines règles du droit d'auteur et des droits voisins du droit d'auteur applicables à la radiodiffusion par satellite et à la retransmission par câble.

[765] Pierre-Yves Gautier, Du droit applicable dans le "village planétaire", au titre de l'usage immatériel des œuvres, D 1996.131, n°4.

[766] Pierre-Yves Gautier, préc.

Au contraire, lorsque l'offre, même si elle est d'origine internationale, est faite en français ou orientée vers un consommateur français notamment, alors on pourrait considérer que les lois du for sont applicables. » L'auteur propose d'appliquer un critère de destination.[767].

Un travail d'adaptation des critères traditionnels sera certainement fait par la jurisprudence lorsqu'elle sera saisie de litiges nés sur les réseaux informatiques internationaux.

Cependant, ce processus ne sera pas immédiat. La jurisprudence se forge au fil des espèces, plusieurs années peuvent s'écouler avant que les juristes ne puissent disposer de décisions de référence.

En outre, l'Internet risque dans beaucoup d'hypothèses d'être peu contentieux : il faudra un enjeu économique suffisamment important pour que les parties ne s'engagent dans une procédure internationale.

Dans certains cas, les juges sont liés par les termes des textes qu'ils ont à appliquer et des modifications des textes existants vont se révéler nécessaires.

L'élaboration de traités internationaux

La France a proposé en avril 1996 lors d'un conseil informel de ministres de la Culture et de la Télécommunication à Bologne l'élaboration d'une convention internationale afin que les pays s'accordent sur un minimum de principes communs pouvant former le socle d'un « code de bonne conduite » sur l'Internet qui pourrait traiter des sujets suivants[768] :

- principes minimaux de déontologie applicables aux services sur l'Internet ;
- détermination des règles applicables (il serait envisageable de retenir le principe de l'applicabilité des règles du pays d'émission pour les parties signataires, et du pays de réception à défaut) ;
- principes de responsabilité communs des éditeurs et services d'hébergement ;
- principes de base d'une coopération judiciaire.

Des conventions de ce type mettront des années à être élaborées. En outre, ce qui inquiète les Etats dans l'Internet, ce n'est pas que la victime d'une contrefaçon de sa marque hésite sur le choix du tribunal et la loi qu'elle invoquera, mais les aspects de droit pénal international. Par exemple, le fait que l'on puisse accéder à des écrits illégaux en France, mais légaux dans le pays d'émission. Des domaines où justement, il va être très difficile de réaliser des conventions internationales, car l'abandon de souveraineté sera jugé trop important, le point de désaccord porte sur des éléments essentiels de la culture de chaque pays.

Même dans un domaine assez harmonisé d'un point de vue international comme le droit d'auteur, la négociation de protocoles additionnels aux conventions existantes prendra plusieurs années.

L'élaboration de directives, de règlements ou de traités se fera certainement au niveau européen. Là encore, de telles mesures n'aboutiront qu'à moyen terme, et ne régleront pas tous les problèmes dans le cadre d'un réseau par essence international, et qui donc ne se limite pas à l'Europe.

[767] Alain Bensoussan (sous la direction de), Internet, aspects juridiques, éditions Hermès 1996, p.123.
[768] Communiqué de François Fillon, ministre des Postes, des Télécommunications et de l'Espace en date du 24 avril 1996.

La création d'un droit spécifique

Certains auteurs américains font observer que le droit classique qui est fondé sur la territorialité est mis à mal par le caractère international du réseau et que le monopole de l'exécution forcée des Etats est limité par la nature du réseau lui-même.[769]

Par exemple, le droit des marques est basé sur les séparations géographiques, le même nom peut être utilisé par des entreprises différentes dès lors qu'elles n'exercent pas leurs activités dans la même zone.

Partant de ce constat, ils préconisent l'adoption de règles spécifiques pour le cyberespace.

Pour le professeur canadien Pierre Trudel :

« En raison du caractère transnational de l'Internet, on ne peut postuler que les règles édictées par les autorités nationales régiront toutes les transactions ; il est nécessaire de cerner les sortes de règles non-étatiques qui existent actuellement dans l'Internet de même que celles qui sont appelées à se développer. Il faut pour cela postuler que le droit n'est pas tout entier compris dans les décisions des autorités étatiques et qu'en conséquence, une importante part des règles concernant les transactions ne sont pas d'origine étatique. Ce sont ces règles non-étatiques qu'il faut bien comprendre afin de rendre compte, dans sa totalité, de la normativité qui s'élabore dans un environnement comme l'Internet. »[770]

En d'autre termes, ce sont les règles élaborées pour le réseau lui-même qui seraient les plus aptes à le réguler. Si le réseau est doté de règles spécifiques, le problème des frontières géographiques et de ses conflits de lois est par là même évacué.

Quelles sont les règles particulières à l'Internet identifiées par la doctrine nord américaine[771] ?

L'éthique personnelle

L'utilisateur de l'Internet doit être responsabilisé, il est maître du choix des sites qu'il consulte, il peut recouper les informations qui lui sont données. Il n'a pas un rôle passif comme dans d'autres médias tels que la télévision.

La pression sociale non-explicitement organisée

Les premiers utilisateurs de l'Internet, chercheurs et universitaires, pratiquaient une autorégulation fondée sur le respect mutuel. Des communautés liées par les mêmes centres d'intérêt peuvent développer leurs propres règles de conduite. On peut ranger dans cette catégorie les règles de politesse de la fameuse Netiquette.

Il est vrai que ces règles seront moins suivies par des usagers venant d'horizons trop différents.

Mais elles peuvent avoir vocation à s'appliquer chaque fois que l'on rencontre un groupe d'utilisateurs liés par un même centre d'intérêts.

Le contrat :

Il constitue pour le professeur Pierre Trudel un principe régulateur central dans l'Internet.

Les relations sur l'Internet se nouent en principe de manière volontaire. L'Internet est un domaine où l'on attache beaucoup d'importance à la liberté individuelle et à son corollaire, le respect de la parole donnée.

---

[769] David R. Johnson et David Post, Law and borders-The rise of law in Cyberspace, First Monday, <http://www.firstmonday.dk>, mai 1996.

[770] P.Trudel, Introduction au droit du commerce électronique sur l'Internet, Revue du Barreau (Québec), 1995, Vol.55, p.521.

[771] P.Trudel, préc. D. Post, Anarchy, State and the Internet : an essay on law-making in Cyberspace, 1995, Journal of Online Law, article 3, <http://warthog.cc.wm.edu/law/publications/jol/>. Ces deux auteurs font référence au travail de Ellickson, Order without Law, Cambridge, Mass, Havard University Press 1991, p.132.

Il se forme entre les fournisseurs d'information et les usagers un contrat susceptible de comporter des obligations quant à la qualité, l'exactitude et la précision des informations.

L'autorégulation

L'ensemble des règles volontairement développées et acceptées par ceux qui prennent part à une activité constitue l'autoréglementation.[772]

L'Internet est constitué d'une multitude de réseaux, chacun avec ses propres règles, que l'administrateur du réseau est parfaitement à même de faire respecter. L'usager accède à l'Internet par le biais d'un fournisseur de connexion, auquel il est contractuellement lié : contrat d'abonnement, de travail, règlement de l'Université, etc.

Ces organisme et sociétés élaborent des règles, des normes de conduite auxquelles l'usager doit se conformer afin de conserver son accès à un réseau donné.

C'est ce que les Anglo-saxons appellent les « Acceptable Use Policies ».

Ces codes de bonne conduite prévoient par exemple des règles relatives au respect du caractère privé du courrier électronique, aux conditions d'utilisation des ressources, au respect de la vie privée, à l'accès illicite aux ressources des réseaux connectés, à la diffusion de matériel inapproprié, etc.[773]

Sur l'Internet, « l'autoréglementation est presque aussi inévitable que le droit des Etats ! Le droit étatique n'y possède pas une supériorité aussi manifeste que dans les autres environnements »[774].

La communauté des utilisateurs et des fournisseurs de services serait la plus apte à élaborer les règles spécifiques qui régiront le cyberespace.

L'idée de créer un droit spécifique à l'Internet ou au moins de se fonder sur l'autoréglementation comme norme de bonne conduite sur les réseaux semblera utopiste à certains.

Cependant :

- le droit prend en compte les usages. Les articles 1135, 1159 et 1160 de notre Code civil y font référence. Les usages professionnels régissent les rapports au sein d'une profession et les usages conventionnels servent à déterminer des obligations qui demeurent implicites. Ils trouvent leur fondement dans la volonté tacite des contractants et tirent leur force obligatoire de la volonté implicite[775] ;
- le droit international dispose lui-même de règles dites matérielles, c'est-à-dire de règles spécifiques. Elles se sont surtout développées dans un domaine où la méthode traditionnelle de conflits de lois était très critiquée comme ne prenant pas en compte la spécificité des règles internationales : le commerce international.[776]

Les règles d'autorégulation qui existent actuellement sur l'Internet se sont développées dans un contexte qui excluait les transactions et la publicité commerciale.

Le commerce électronique engendrera-t-il ses propres usages et pratiques ? Verra-t-on l'émergence de normes internationales en matière de commerce électronique ?[777]

---

[772] Pierre Trudel, préc.

[773] Voir la liste des comportements généralement prohibés dans : P. Trudel, Quel droit pour la cyberpresse ? La régulation de l'information sur l'Internet, Legipress, mars 1996, II, p.9.

[774] Pierre Trudel, préc., p.15.

[775] G. Cornu, Droit civil, Introduction, éditions Montchrétien, n°423 et s.

[776] Y. Loussouam et P. Bourel, Droit international privé, précis Dalloz, 4e édition 1993,n°68.

[777] S. Parisien, Un essai sur le mode de formation des normes dans le commerce électronique, Cybernews, Vol. II, n° II Hiver 1996, <http://www.droit.umontreal.ca/CRDP/Cyberews/>.

La chambre de commerce internationale de la CCI a mis en place un groupe de travail chargé d'élaborer des « Eterms Repository » — Eterms pour Electronic Terms — afin d'élaborer un répertoire de termes juridiques du commerce électronique en environnement ouvert.[778]

Les professionnels d'une même branche se dotent parfois de règles d'autodiscipline. Par exemple, le syndicat des entreprises de vente par correspondance et à distance [779] s'est doté d'un code professionnel que s'obligent à respecter les sociétés adhérentes du syndicat. Une convention européenne de la vente par correspondance et à distance transfrontière en date du 4 juin 1992 propose un certain nombre de règles déontologiques professionnelles que les entreprises adhérentes et les associations nationales s'engagent à respecter[780].

On pourrait imaginer ainsi l'élaboration de codes professionnels internationaux adaptés aux spécificités des pratiques commerciales sur l'Internet.

Une fois que les règles spécifiques au réseau ont été identifiées, reste la question de savoir qui va les appliquer.

Dans le système décentralisé que constitue l'Internet, les opérateurs du réseau sont mieux armés pour faire respecter les normes. Ils sont finalement les maîtres du réseau[781].

Mais les administrateurs des réseaux sont des techniciens, pas des juristes.

> L'autorégulation ainsi conçue va avoir besoin de ses propres mécanismes de résolution des litiges.

« Des millions de gens à travers le monde communiquent, font des affaires à travers les réseaux informatiques. Les litiges sont inévitables, et les tribunaux existants sont trop lents, trop encombrés et ont un champ d'application trop limité pour avoir un effet global. Nous devons explorer de nouvelles formes de résolution des litiges, fournir des solutions rapidement et développer des sanctions appropriées qui conviennent aux réseaux informatiques internationaux »[782].

Partant de ce constat, des organisations américaines, dont l'American Association Arbitration, ont mis sur pied un projet pilote d'arbitrage en ligne : le Virtual Magistrate Project.(VMP) [783]

Le VMP se veut une façon de fournir un moyen rapide de résoudre des litiges impliquant des utilisateurs des systèmes en ligne ; des personnes qui prétendent que des messages, ou des documents leurs sont préjudiciables, et des opérateurs systèmes.

Les systèmes opérateurs pourraient ainsi obtenir rapidement des jugements neutres sur la réponse à donner à des plaintes concernant des messages postés.

Le VMP acceptera des plaintes concernant des messages et des documents qui porteraient atteinte à des droits de propriété intellectuelle ou des marques déposées, à des secrets commerciaux, à l'honneur ou à la réputation, ou qui seraient frauduleux, constitutifs de pratiques commerciales trompeuses, inappropriés (messages obscènes), qui porteraient atteinte à la vie privée ou impliquant d'autres contenus préjudiciables.

Toute la procédure se déroule sur le réseau et par courrier électronique. Un formulaire à remplir en ligne est disponible sur le site du VMP.

Les magistrats désignés doivent en principe rendre leur décision dans un délai de 72 heures après l'acceptation de la plainte.

---

[778] Voir supra

[779] 60, rue de la Boétie 75008 Paris.

[780] Entrée en vigueur le 1er janvier 1993, Gaz. Pal.,n°spécial sur la vente à distance, 25 février 1993, annexe p.70

[781] O. Hance, Belgique, l'acceptable use policy du réseau Belnet : variations prospectives sur la notion d'autoréglementation, Droit de l'Informatique et des Télécoms 1995/3, p.53

[782] Leixner, Président du national Center for Automated Information Research, communiqué de presse du 4 mars 1996, annonçant la création du Virtual Magistrate Project.

[783] Site Web :<http://www.vmag.law.vill.edu:8080/>, « Justice assistée par ordinateur », *Planète Internet* n° 9 juin 1996, p.36.

Le VMP a rendu sa première décision le 8 mai 1996.[784] Le demandeur, un abonné d'American On Line (AOL), a saisi le Virtual Magistrate Project afin de demander le retrait d'un message publicitaire posté par Email America offrant de vendre 5 millions d'adresses e-mail pour 99 dollars. Le Virtual Magistrate a recommandé que le message incriminé soit retiré par AOL au motif qu'il était contraire aussi bien aux conditions générales du service AOL qu'aux usages Internet. L'affaire n'est néanmoins pas significative : le défendeur, Email America, n'a pas participé à l'affaire.

Les magistrats n'ont pas à appliquer le droit d'une juridiction spécifique.

Reste que des arbitres américains qui seraient saisis de plaintes en matière de messages obscènes ou violents se réfèreront nécessairement aux standards américains en la matière. Et qu'on imagine mal un fournisseur français ou allemand leur demander s'il tel message peut être qualifié de révisionniste.

Un autre projet pilote américain d'utilisation des ressources en ligne pour résoudre les litiges résultant des activités sur les réseaux informatiques est celui de l'Online Ombuds Office[785]. L'Ombudsman est une institution scandinave, un organe de protection contre les abus de l'administration, un médiateur. Les initiateurs du projet ont transposé cette institution à l'Internet. Les « ombudspersones » sont contactées en ligne, à partir du site Web du projet.

Le Centre de recherche en droit privé de l'université de Montréal a annoncé, début octobre 1996, la création d'un projet de recherche sur les modes de résolution des conflits dans le cyberespace, le Cybertribunal[786].

Si ces expériences se révélaient concluantes, de véritables instances d'arbitrage en ligne qui prennent en compte les sensibilités différentes d'un groupe de pays à un autre, pourraient être mises en place.

L'idée du Virtual Magistrate Project ne fait pas l'unanimité. Certains la trouvent prématurée, d'autres se demandent quel impact peuvent avoir des avis dépourvus de toute force exécutoire, car faute de constituer de véritables sentences arbitrales, ils ne pourront pas être revêtus de l'exequatur, et ne peuvent être exécutés que sur une base volontaire.

De telles initiatives relèvent-elles d'une vue utopiste de l'Internet ?

« Je suis convaincu que le tout judiciaire est impossible et qu'au fond il n'a pas de raison d'être. (…) La justice, parce qu'elle est lourde, formaliste, lointaine, coûteuse, lente, n'est pas vouée à régler tous les conflits dans une société. Ce qui demeure, en revanche, la fonction irremplaçable du juge, c'est de veiller au respect de la loi et à celui de la liberté individuelle. Je pense que toutes les forces de médiation sont utiles. »

Ces propos ont été tenus par Robert Badinter, ancien ministre de la Justice et ancien président du Conseil constitutionnel[787].

En matière de commerce international, l'arbitrage est un mode normal de résolution des litiges. Il n'est pas impossible que voient le jour des systèmes d'arbitrage internationaux adaptés aux réseaux informatiques.

Perspectives

L'Internet va certainement faire évoluer les règles de droit car c'est le droit qui va être obligé de s'adapter à cette nouvelle technologie et non l'inverse.

L'utilisateur actuel de l'Internet peut cependant se demander en quoi il est intéressé par ces évolutions à moyen et à long terme.

---

[784] Tierney and Email America, Docket n°96-0001, <http://vmag.law.vill.edu:8080/doksys/96-0001>.
[785] Site Web : <http://www.ombuds.org>.
[786] Site Web : <http://www.cybertribunal.org/>.
[787] « Nos sociétés sont de plus en plus soumises au contrôle de la justice », entretien accordé au journal *le Monde*, 19 mars 1996, p.14.

En réalité, il est déjà concerné dans sa pratique actuelle de l'Internet.

Prenons l'exemple du commerce électronique. Le droit classique considère le consommateur comme une personne placée en position de faiblesse face à des vendeurs tout puissants qu'il faut protéger. Des lois viennent donc fixer des obligations impératives au vendeur.

Sur l'Internet, ces lois impératives ont peu de poids pour protéger le consommateur, car elles vont n'avoir aucune efficacité sur des vendeurs situés par exemple à l'étranger.

En revanche, l'usager d'Internet doit apprendre à ne plus réagir en consommateur passif. Si par exemple, il choisit de contracter avec un serveur américain, il accepte implicitement que les modes d'emploi lui soient adressés en anglais, même si notre loi impose que ces derniers soient rédigés en français. S'il veut pouvoir passer une commande dans sa langue, il aura la possibilité, soit de s'adresser à un site qui fait des offres dans plusieurs langues, soit à un site francophone.

Il peut prendre le risque de contracter avec des sites non sécurisés, d'acheter un logiciel sans l'avoir testé alors que de nombreux vendeurs de logiciels permettent de tels tests.

Il faut aussi savoir que les usagers insatisfaits des services de telle ou telle entreprise ont la possibilité de le faire savoir *via* les forums de discussion.

Par exemple un message posté le 17 juillet 1996 dans le newsgroup <misc.consumers.frugal-living> recommandait de ne pas avoir recours aux services d'une société texane Vektron International, dont les clients seraient mécontents[788]. Le groupe de discussion français <fr.network.fournisseurs> a été créé pour discuter des prestations offertes par les différents fournisseurs de services français.

En un mot, le consommateur usager doit être responsabilisé et apprendre à utiliser les moyens d'information et de comparaison que l'Internet met à sa disposition.

Le droit français offre la possibilité à plusieurs consommateurs ayant subi des préjudices individuels causés par le fait d'un même professionnel et ayant une origine commune de donner mandat d'agir en leur nom, en réparation du préjudice, devant toute juridiction, à une association agréée[789]. Cette procédure dite action en réparation conjointe est inspirée des class-actions américaines ou encore du recours collectif du droit québécois.

Le recours aux possibilités de communication de l'Internet peut être un moyen intéressant de retrouver les consommateur qui auraient été lésés par une entreprise peu scrupuleuse, y compris à une échelle internationale.

Certains proposent même l'élaboration d'un droit de la publicité spécifique prenant en compte cette attitude interactive du consommateur[790].

Quant au vendeur, on ne peut pas raisonnablement exiger de lui qu'il connaisse les spécificités du droit de la consommation des pays de toutes les personnes qui lui achèteraient ses produits. Evidemment, il doit respecter sa loi locale, et les directives européennes qui viendraient à être prises. Il existe en revanche un principe de base du commerce qui transcende les frontières que le vendeur ne devra pas oublier : « Donner satisfaction au client ».

Prenons un autre exemple, celui de la diffamation. Un message posté dans un newsgroup porte atteinte à la réputation de votre entreprise. L'hypothèse n'est pas d'école. Il suffit de lire les newsgroups pour se rendre compte que de tels messages ne sont pas rares.

Des affaires de diffamation en ligne sont allés jusque devant les tribunaux américains.

Dans une affaire Cubby, Inc. v. Compuserve[791], une lettre d'information, à destination des journalistes et diffusée sur un des forums de Compuserve, contenait des propos diffamatoires.

---

[788] <chita@adnc.com>, "warning about Vektron", 17 juillet 1996.
[789] Articles L422-1 à L422-3 du Code de la consommation.
[790] O. Hance, Business et Droit d'Internet, Best Of Editions 1996, p. 134.

Dans une affaire Stratton Oakmont Inc. v. Prodigy[792], une personne a envoyé à un forum de Prodigy consacré aux discussions financières un message diffamatoire sur la banque d'affaires Stratton Oakmont.

Si on se place dans un contexte international, il va être difficile de faire aboutir une procédure en diffamation. Les règles régissant la diffamation sont déjà suffisamment complexes dans leurs seuls aspects de droit interne. Si en plus, il y a une incertitude sur le droit applicable et si une procédure d'exequatur s'avère nécessaire, ou des procédures multiples pour obtenir réparation de l'entier préjudice, on peut imaginer que les litiges portés devant les tribunaux seront rares.

La victime d'une diffamation est-elle totalement démunie ? Non car il ne tient qu'à elle d'utiliser la même voie que le message diffamatoire et de faire usage du droit de réponse en temps réel que lui offre l'Internet, pour défendre son honneur et sa réputation.

Or, cette possibilité n'existe pas dans les médias classiques.

Certains, du fait qu'il soit si facile de répondre pour corriger les déclarations diffamatoires, comparé au coût et à la longueur d'une procédure en diffamation, prédisent même que les procès en diffamation vont devenir marginaux[793].

Certes, cette méthode n'effacera pas l'atteinte originelle à la réputation de quelqu'un. Une réponse postée sur l'Internet n'aura jamais la portée d'une décision de justice, et ne sera peut-être pas suffisante à effacer le doute né dans l'esprit de certains. Mais c'est une possibilité qui ignore les conflits de lois et de souveraineté et qui doit donc être utilisée lorsque cela apparaît nécessaire.

Dans certains cas, une procédure devra être engagée : aucune solution amiable n'a pu être trouvée, les mécanismes de régulation de l'Internet ne sont pas suffisants.

L'enjeu économique de l'affaire va justifier qu'un procès soit fait dans un pays étranger par exemple.

Même dans ce cas de figure somme toute classique, les ressources de l'Internet pourront être utilisées à bon escient. Dans certains cas, l'entreprise ou le particulier s'adresse à son conseil habituel qui rentre ensuite en contact avec ses correspondants étrangers. Le client n'est donc pas en contact direct avec l'avocat qui traite de son dossier†: une méthode de travail qui pourrait évoluer avec l'Internet, qui facilite justement les communications entre personnes venant de pays et d'horizons différents.

De plus, la personne qui envisagerait de faire un procès dans un pays dont elle ne connaît pas bien les usages en matière judiciaire pourrait tenter d'obtenir les premières informations sur le réseau.

On peut imaginer d'autres hypothèses où des procédures sont prises en charge par des associations professionnelles. Par exemple, un syndicat d'éditeurs décide de prendre en charge les frais d'une procédure en contrefaçon contre un serveur aux Etats-Unis, afin de faire un précédent et un exemple. Ou inversement, un syndicat américain va vouloir entamer une procédure contre un serveur européen. Ces associations américaines et européennes ont intérêt à communiquer et à coopérer entre elles, car par-delà les divergences nationales, elles poursuivent le même objectif de défense des droits d'auteur sur l'Internet. L'Internet peut permettre de rendre ces échanges plus aisés et enrichissants

---

[791] 776 F., Supp. 135 (S.D.N.Y. 1991).
[792] NY Sup. Ct. n° 31063/94, May 25, 1995.
[793] Mike Godwin, Libel law : let it die, Wired magazine, mars 1996, p.116.

En conclusion, il est vrai que si l'on se place d'un point de vue judiciaire, l'Internet est une source de complication. Mais même en droit interne, toutes les situations n'aboutissent pas devant les tribunaux et des droits comme le droit de la consommation sont en réalité peu contentieux.

Par ailleurs, l'Internet offre également ses propres moyens d'autorégulation, la possibilité de s'informer, qui est un moyen de prévenir les conflits, et peut-être un jour des organismes d'arbitrage propres aux réseaux informatiques.

Annexes

Sélection de ressources Internet

Réglementation des télécommunications

- Site du Ministère des télécommunications, de la poste et de l'espace
http://www.telecom.gouv.fr

La loi sur la réglementation des télécommunications et de nombreuses informations sur le secteur des télécommunications.

Noms de domaine

- What's in a name
http://www.law.georgetown.edu/lc/internic/domain1.html

Un site américain très complet sur les noms de domaine.

- NIC France
http://www.nic.fr

Pour le dépôt des noms de domaine de la zone <fr>.

- InterNIC
http://rs.internic.net

Pour le dépôt des noms de domaine de la zone <com>.

- RIPE - Europe Network Coordination Center
http://www.ripe.net/ Ripe

Informations sur les noms de domaine en Europe.

Associations de défense des libertés publiques sur le réseau

On trouve sur les sites de ces associations de nombreuses informations sur les aspects juridiques de l'Internet.

- AUI
http://www.aui.fr

L'Association des Utilisateurs d'Internet est une association française visant à promouvoir le développement et la démocratisation de l'utilisation des réseaux électroniques de communication.

- EPIC
http://www.epic.org

L'Electronic Privacy Information Center est une association américaine qui défend plus spécifiquement le droit à la vie privée des citoyens. Informations intéressantes sur la cryptographie.

- EFF
http://www.eff.org

L'Electronic Frontier Foundation est une organisation américaine, visant à promouvoir les libertés civiles des utilisateurs des réseaux électroniques.

Sites universitaires

- Faculté de droit de Montréal
http://www.droit.umontreal.ca/

La faculté de droit de Montréal avec son Centre de Recherche en Droit Public est très active dans le domaine de l'information juridique sur l'Internet et le droit des nouvelles technologies.

Journaux électroniques

- Cybernews
http://www.droit.umontreal.ca/CRDP/CyberNews/

La lettre d'information sur le droit des technologies de l'information du Centre de Recherche en Droit Public de l'Université de Montréal.

- L'Internet Juridique
http://www.argia.fr/lij

Actualités, articles sur le droit des nouvelles technologies, ressources juridiques sur l'Internet.

Listes de diffusion

- Obiter
http://www.DROIT.UMontreal.CA/Obiter/

Forum de discussion québécois et francophone sur le droit et les nouvelles technologies.

- CYBERIA-L - Law & Policy of Computer Communications :

Forum de discussion américain sur le droit des réseaux informatiques. Pour s'abonner, envoyer le message :

SUBSCRIBE CYBERIA-L <nom>
à : LISTSERV@LISTSERV.AOL.COM

Archives :
http://www.ljextra.com/mailinglists/cyberia-l/index.html

Résolution des litiges en ligne

- Le Cybertribunal
http://www.cybertribunal.org/

Projet pilote d'arbitrage et de médiation développé à titre expérimental par le Centre de recherche en droit public (CRDP) de l'Université de Montréal s'inscrivant dans le cadre de ses recherches sur les procédés de réglementation dans le cyberespace.

- Online Ombuds Office
http://www.ombuds.org

Projet pilote américain de médiation en ligne des litiges susceptibles de survenir dans le cyberespace.

- Virtual Magistrate Project
http://vmag.law.vill.edu:8080/

Projet pilote américain d'arbitrage en ligne destiné à explorer de nouvelles méthodes de résolution des litiges adaptées aux réseaux informatiques mondiaux.

Adresses utiles

AUI

40 quai de Jemmapes
75010 Paris
tél : 01 45 52 47 99

CNIL

21, rue Saint-Guillaume
75340 Paris Cedex 07
tél : 01 53 73 22 22

NIC France

Domaine de Voluceau
BP 105
F-78153 Le Chesnay Cedex
tél : 01 39 63 56 16

SCSSI

18, rue du Docteur Zamenhof
92131 Issy-les-Moulineaux Cedex
tél : 01 40 95 37 15

TGI Paris

4 blv. du Palais
75 001 Paris
tél : 01 44 32 51 51

TGI Nanterre

6, rue Pablo Neruda
92000 Nanterre
tél : 01 40 97 10 10

Magazine Planète Internet

191 av. Aristide-Briand
94230 Cachan
tél : 01 49 08 58 30

Ministère des Télécommunications

20 av. Ségur
75007 Paris
tél : 01 43 19 20 20

Transpac

33 av. du Maine B13
75755 Paris Cedex 15
tél : 01 45 38 88 88

DGXIII

Direction Générale des Télécommunications, Industries de l'Information et Innovation de la Commission européenne

Rue de la Loi 200
B-1049 Bruxelles Wetstraat 200
tél : (32-2) 299.11.11

Abréviations

AUI : Association des Utilisateurs d'Internet

BBS : Bulletin Board Service

BRDA : Bulletin Rapide de Droit des Affaires

Bull. : Bulletin des arrêts de la Cour de cassation

CA : Cour d'appel

Cass. : Cour de cassation

CCI : Chambre de Commerce Internationale

Ch. : chambre

Civ. : civil (chambre civile de la Cour de cassation, code)

CJCE : Cour de Justice des Communautés européennes

CNCIS : Commission Nationale de Contrôle des Interceptions de Sécurité

CNIL : Commission Nationale Informatique et Libertés

Com. : commercial (chambre commerciale de la Cour de cassation, revue, code)

CPI : Code de la propriété intellectulle

CPT : Code des Postes et Télécommunications

Crim. : chambre criminelle de la Cour de cassation

CSA : Conseil supérieur de l'audiovisuel

CST : Conseil supérieur de la télématique

D : recueil Dalloz

Dr. Pénal : revue de Droit pénal

DG XIII : Direction Générale XIII de la Commission européenne

EDI : Echanges de Données Informatisées

FTP : File Transfert Protocol

Gaz. Pal. : recueil de la Gazette du Palais

IP : abréviation pour TCP/IP Internet Protocol

IRC : Internet Relay Chat

JCP éd. E : recueil de la Semaine Juridique, édition entreprises

JCP éd. G : recueil de la Semaine Juridique, édition générale

JCP éd. N : recueil de la Semaine Jurdique, édition notariale

JO : Journal Officiel

JOAN : Journal Officiel de l'Assemblée Nationale

JOCE : Journal Officiel des Communautés Européennes

NIC : Internic

NSI : Network Solutions Inc

PIBD : Propriété industrielle bulletin documentaire

PGP : Pretty Good Privacy

Préc. : précité

Rec. : recueil

Rev. : revue

Rev. cr. dr. int. pr. : revue critique de droit international privé

RIDA : revue internationale de droit d'auteur

RNIS : Réseau Numérique à Intégration de Services

RTD Civ. : revue trimestrielle de droit civil

RTD Com. : revue trimestrielle de droit commercial

S : recueil Sirey

SCSSI : Service central de la sécurité des systèmes d'information

Soc. : chambre sociale de la Cour de cassation

TCP/IP : Transmission Control Protocol/ Internet Protocol

TGI : Tribunal de Grande Instance

TI : Tribunal d'Instance

URL : Universal Resource Locator

Web : abréviation pour World Wide Web

WWW : World Wide Web

Textes de loi

Extraits de la loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications et extraits du Code pénal sur le secret des correspondances

Art. 1er - Le secret des correspondances émises par la voie des télécommunications est garanti par la loi. Il ne peut être porté atteinte à ce secret que par l'autorité publique, dans les seuls cas de nécessité d'intérêt public prévus par la loi et dans les limites fixées par celle-ci.

Titre I : Des interceptions ordonnées par l'autorité judiciaire

Art. 2 - Dans le chapitre Ier du titre III du livre Ier du code de procédure pénale :

[....]

III - Il est créé dans la même section III une sous-section intitulée "Des interceptions de correspondances émises par la voie des télécommunications" comprenant les articles 100 à 100-7 ainsi rédigés :

"Art. 100 - En matière criminelle et en matière correctionnelle, si la peine encourue est égale ou supérieure à deux ans d'emprisonnement, le juge d'instruction peut, lorsque les nécessités de l'information l'exigent, prescrire l'interception, l'enregistrement et la transcription de correspodances émises par la voie des télécommunications. Ces opérations sont effectuées sous son autorité et son contrôle.

La décision d'interception est écrite. Elle n'a pas de caractère juridictionnel et n'est suceptible d'aucun recours.

Art. 100-1 - La décision prise en application de l'article 100 doit comporter tous les éléments d'identification de la liaison à intercepter, l'infraction qui motive le recours à l'interception ainsi que la durée de celle-ci.

Art. 100-2 - Cette décision est prise pour une durée maximum de quatre mois. Elle ne peut être renouvelée que dans les mêmes conditions de forme et de durée.

Art. 100-3 - Le juge d'instruction ou l'officier de police judiciaire commis par lui peut requérir tout agent qualifié d'un service ou organisme placé sous l'autorité ou la tutelle du ministre chargé des télécommunications ou tout agent qualifié d'un exploitant de réseau du fournisseur de services de télécommunication autorisé, en vue de procéder à l'installation d'un dispositif d'interception.

Art. 100-4 - Le juge d'instruction ou l'officier de police judiciaire commis par lui dresse procès-verbal de chacune des opérations d'niterception et d'enregistrement. Ce procès-verbal mentionne la date et l'heure auxquelles l'opération a commencé et celles auxquelles elle s'est terlminée.

Les enregistrements sont placés sous scellés fermés.

Art. 100-5 - Le juge d'instruction ou l'officier de police judiciaire commis par lui transcrit la correspondance utile à la manifestation de la vérité. Il en est dressé procès-verbal. Cette transcription est versée au dossier.

Les correspondances en langue étrangère sont transcrites en français avec l'assistance d'un interprète requis à cette fin.

Art. 100-6 - Les enregistrements sont détruits, à la diligence du procureur de la République ou du procureur général, à l'expiration du délai de prescription de l'action publique.

Il est dressé procès-verbal de l'opération de destruction.

Art. 100-7 - Aucune interception ne peut avoir lieu sur une ligne dépendant du cabinet d'avocat ou de son domicile sans que le bâtonnier en soit informé par le juge d'instruction."

Titre II : Des interceptions de sécurité

Art. 3 - Peuvent être autorisées, à titre exceptionnel, dans les conditions prévues par l'article 4, les interceptions de correspondances émises par la voie des télécommunications ayant pour objet de rechercher des renseignements intéressants la sécurité nationale, la sauvegarde des éléments essentiels du potentiel scientifique et économique de la France, ou la prévention du terrorisme, de la criminalité et de la délinquance organisées et de la reconstitution ou du maintien de groupements dissous en application de la loi du 10 janvier 1936 sur les groupes de combat et les milices privées.

Art. 4 - L'autorisation est accordée par décision écrite et motivée du Premier ministre ou de l'une des deux personnes spécialement déléguées par lui. Elle est donnée sur proposition écrite et motivée du ministre de la défense, du ministre de l'intérieur ou du ministre chargé des douanes, ou de la personne que chacun d'eux aura spécialement déléguée.

Le Premier ministre organise la centralisation de l'exécution des interceptions autorisées.

Art. 5 - Le nombre maximum des interceptions susceptibles d'être pratiquées simultanément en application de l'article 4 est arrêté par le Premier ministre.

La décision fixant ce contingent et sa répartition entre les ministères mentionnés à l'article 4 est portée sans délai à la connaissance de la Commission nationale de contrôle des interceptions de sécurité.

Art. 6 - L'autorisation mentionnée à l'article 3 est donnée pour une durée maximum de quatre mois. Elle cesse de plein droit de produire effet à l'expiration de ce délai. Elle ne eput être renounelée que dans les mêmes conditions de forme et de durée.

Art. 7 - Dans les correspondances interceptées, seuls les renseignements en relation avec l'un des objectifs énumérés à l'article 3 peuvent faire l'objet d'une transcription.

Cette transcription est effectuée par les personnes habilités.

Art. 8 - Il est établi, sous l'autorité du Premier ministre, un relevé de chacune des opérations d'interception et d'enregistrement. ce relevé mentionne la date et l'heure auxquelles elle a commencé et celles auxquelles elle s'est terminée.

Art. 9 - L'enregistrement est détruit sous l'autorité du Premier ministre, à l'expiration d'un délai de dix jours au plus tard à compter de la date à laquelle il a été effectué.

Il est dressé procès-verbal de cette opération.

Art. 10 - Sans préjudice de l'application du deuxième alinéa de l'article 40 du code de procédure pénale, les renseignements recueillis ne peuvent servir à d'autres fins que celles mentionnées à l'article 3.

Art. 11 - Les opérations matérielles nécessaires à la mise en place des interceptions dans les locaux et installations des services ou organismes placés sous l'autorité ou la tutelle du ministre chargé des télécommunications ou des exploitants de réseaux ou fournisseurs de services de télécommunications autorisés ne peuvent être effectuées que sur ordre du ministre chargé des télécommunications ou sur ordre de la personne spécialement déléguée par lui, par des agents qualifiés de ces services, organismes, exploitants ou fournisseurs dans leurs installations respectives.

Art. 12 - Les transcriptions d'interceptions doivent être détruites dès que leur conservation n'est plus indispensable à la réalisation des fins mentionées à l'article 3.

Il est dressé procès-verbal de l'opération de destruction.

Les opérations mentionnées aux alinéas précédents sont effectuées sous l'autorité du Premier ministre.

Art. 13 - Il est institué une Commission nationale de contrôle des interceptions de sécurité. Cette Commission est une autorité administrative indépendante. Elle est chargée de veiller au respect des dispositions du présent titre. Elle est présidée par une personnalité désignée, pour une durée de six ans, par la Président de la République, sur une liste de quatre noms établie conjointement par le vice -président du Conseil d'Etat et le Premier président de la Cour de cassation.

Elle comprend en outre :

Un député désigné pour la durée de la législature par le président de l'Assemblée nationale ;

Un sénateur désigné après chaque renouvellement partiel du Sénat par le président du Sénat ;

La qualité de membre de la Commission est incompatible avec celle de membre du Gouvernement.

Sauf démission, il ne peut être mis fin aux fonctions de membre de la Commission qu'en cas d'empêchement constaté par celle-ci.

Le mandat des membres de la Commission n'est pas renouvelable.

En cas de partage des voix, la voix du président est prépondérante.

Les agents de la Commision sont nommés par le président.

Les membres de la Commission désignés en remplacement de ceux dont les fonctions ont pris fin avant leur terme normal achèvent le mandat de ceux qu'ils remplacent. A l'expiration de ce mandat, par dérogation au septième alinéa ci-dessus, ils peuvent être nommés comme membre de la Commission s'ils ont occupé ces fonctions de remplacement pendant moins de deux ans.

Les membres de la Commission sont astreints au respect des secrets protégés par les articles 75 et 378 du Code pénal pour les faits, actes ou renseignements dont ils ont pu avoir connaissance en raison de leurs fonctions.

La Commission établit son réglement intérieur.

Art. 14 - La décision motivée du Premier ministre mentionnée à l'article 4 est communiquée dans un délai de quarante-huit heures au plus tard au président de la Commission na tionale de contrôle des interceptions de sécurité.

Si celui-ci estime que la légalité de cette décision au regard des dispositions du présent titre n'ets pas certaine, il réunit la Commission qui statue dans les sept jours suivant la réception par son président de la communication mentionnée au premier alinéa.

Au cas où la Commission estime qu'une interception de sécurité a été autorisée en, méconnaissance des dispositions du rpésent titre, elle adresse au Premier ministre une recommandation tendant à ce que cette interception soit interrompue.

Elle porte également cette recommandation à la connaissance du ministre chargé des télécommunications.

La Commission peut adresser au Premier ministre une recommandation relative au contingent et à sa répartition visés à l'article 5.

Le Premier ministre informe sans délai la Commission des suites données à ses recommandations.

Art. 15 - De sa propre initiative ou sur réclamation de toute personne y ayant un intérêt direct et personnel, la Commission peut procéder au contrôle de toute interceptionde sécurité en vue de vérifier si elle est effectuée dans le respect des dispotions du présent titre.

Si la Commission estime que'une interception de sécurité est effectuée en violation des dispotions du présent titre, elle adresse au Premier ministre une recommandation tendant à ce que cette interception soit interrompue.

Il est alors procédé ainsi qu'il est indiqué aux quatrième et sixième alinéaq de l'article 14.

Art. 16 - Les ministres, les autorités publiques, les agents publics doivent prendre toutes mesures utiles pour faciliter l'action de la Comission.

Art. 17 - Lorsque la Commission a exercé son contrôle à la suite d'une réclamation, il est notifié à l'auteur de la réclamation qu'il a été procédé aux réclamations nécessaires.

Conformément au deuxième alinéa de l'article 40 du code de procédure pénale, la Commission donne un avis sans délai au procureur de la république de toute infraction aux dispositions de la présente loi dont elle a pu avoir connaissance à l'aoccasion du contrôle effectué en application de l'article 15.

Art; 18 - les crédits nécessaires à la Comission nationale de contrôle des interceptions de sécurité pour l'accomplissement de sa mission sont inscrits au budget des services du Premier ministre.

Le président est ordonnateur des dépenses de la commission.

Art. 19 - La Commission remet chaque année au Premier ministre un rapport sur les conditions d'exercice et les résultats de son activité, qui précise notamment le nombre de recommandations qu'elle a adressées au Premier ministre en application de l'article 14 et les suites qui leur ont été données. Ce rapport est rendu public.

Elle adresse, à tout moment, au Premier ministre les onservations qu'elle juge utile.

[....]

Article 432-9 du Code Pénal :

Le fait, par une personne dépositaire de l'autorité publique ou chargée d'une mission de service public, agissant dans l'exercice ou à l'occasion de ses fonctions ou de sa mission, d'ordonner, de commettre ou de faciliter, hors les cas prévus par la loi, le détournement, la suppression ou l'ouverture de correspondances ou la révélation du contenu de ces correspondances, est puni

de trois ans d'emprisonnement et de 300 000 francs d'amende.

Est puni des mêmes peines le fait, par une personne visée à l'alinéa précédent ou un agent d'un exploitant de réseau de télécommunications autorisé en vertu de l'article L 33-1 du Code des postes et télécommunications ou d'un fournisseur de service de télécommunications, agissant dans l'exercice de ses fonctions, d'ordonner, de commettre ou de faciliter, hors les cas prévus par la loi, l'interception ou le détournement des correspondances émises, transmises ou reçues par la voie des télécommunications, l'utilisation ou la divulgation de leur contenu.

Article 226-15 du Code pénal :

Le fait, commis de mauvaise foi, d'ouvrir, de supprimer, de retarder ou de détourner des correspondances arrivées ou non à destination et adressées à des tiers, ou d'en prendre frauduleusement connaissance, est puni d'un an d'emprisonnement et de 300 000 francs d'amende.

Est puni des mêmes peines le fait, commis de mauvaise foi, d'intercepter, de détourner, d'utiliser ou de divulguer des correspondances émises, transmises ou reçues par la voie des télécommunications ou de procéder à l'installation d'appareils conçus pour réaliser de telles interceptions.

Extraits de la loi n° 86-1067 du 30 septembre 1986 modifiée sur la réglementation de l'audiovisuel

Article 1 :

La communication audiovisuelle est libre.

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

Le Conseil supérieur de l'audiovisuel, autorité indépendante, garantit l'exercice de cette liberté dans les conditions définies par la présente loi.

Il assure l'égalité de traitement ; il garantit l'indépendance et l'impartialité du secteur public de la radiodiffusion sonore et de la télévision; il veille à favoriser la libre concurrence ; il veille à la qualité et à la diversité des programmes, au développement de la production et de la création audiovisuelles nationales ainsi qu'à la défense et à l'illustration de la langue et de la culture françaises. Il peut formuler des propositions sur l'amélioration de la qualité des programmes.

Article 2 :

On entend par télécommunication toute transmission, émission ou réception de signes, de signaux, d'écrits, d'images, de sons ou de renseignements de toute nature, par fil, optique, radio-électricité ou autres systèmes électromagnétiques.

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

Article 3 :

Le secret des choix faits par les personnes parmi les services de télécommunication et parmi les programmes offerts par ceux-ci ne peut être levé sans leur accord.

[....]

Article 37 :

Toute entreprise titulaire d'une autorisation relative à un service de communication audiovisuelle tient en permanence à la disposition du public :

1° Si elle n'est pas dotée de la personnalité morale, les nom et prénom de la ou des personnes physiques propriétaires ou copropriétaires ;

2° Si elle est dotée de la personnalité morale, sa dénomination ou sa raison sociale, son siège social, le nom de son représentant légal et des ses trois principaux associés ;

3°.Dans tous les cas, le nom du directeur de la publication et celui du responsable de la rédaction ;

4° La liste des publications éditées par l'entreprise et la liste des autres services de communication audiovisuelle qu'elle assure.

[....]

Article 43 :

Sont soumis à déclaration préalable :

1° Les services de communication audiovisuelle autres que les services prévus aux chapitres 1er et II du présent titre et aux titres III et IV de la présente loi ;

2° Par dérogation aux articles 34 et 34-1 de la présente loi :

a) l'exploitation des réseaux qui desservent moins de 100 foyers et qui ne distribuent que des services de radiodiffusion sonore et de télévision diffusés par voie hertzienne terrestre et par satellite et normalement reçus dans la zone, ainsi que l'exploitation des réseaux qui ne distribuent que des services de radiodiffusion sonore et de télévision diffusés par voie hertzienne terrestre et normalement reçus dans la zone. L'exploitation peut alors être assurée par toute personne morale.

Toutefois, lorsque ces réseaux sont situés dans une zone desservie par un réseau autorisé en application de l'article 34, ils ne peuvent faire l'objet d'une exploitation sous le régime de la déclaration préalable que dans le cas où une offre de raccordement au réseau autorisé a été précédemment rejetée soit par l'assemblée générale des copropriétaires dans les conditions prévues au j de l'article 25 de la loi No 65-557 du 10 juillet 1965 fixant le statut de la copropriété des immeubles bâtis, soit par les locataires saisis par le bailleur dans les conditions prévues à l'article 42 de la loi No 86-1290 du 23 décembre 1986 tendant à favoriser l'investissement locatif, l'accession à la propriété de logements sociaux et le développement de l'offre foncière.

L'arrêté ministériel prévu à l'article 34 fixe les conditions particulières dans lesquelles ces réseaux sont soumis aux spécifications techniques d'ensemble visées à cet article.

b) les services de communication audiovisuelle internes à une entreprise ou à un service public.

La déclaration concernant les services utilisant les réseaux de télécommunication définis au paragraphe I

de l'article L 33-1 du code des postes et télécommunications est déposée auprès du procureur de la République. Dans tous les autres cas prévus aux 1° et 2° ci-dessus du présent article, la déclaration est déposée auprès du procureur de la République et du Conseil supérieur de l'audiovisuel.

Les messages publicitaires diffusés par les services mentionnés au présent article doivent être présentés comme tels.

Le fournisseur du service est tenu de porter à la connaissance des utilisateurs :

1° Les éléments mentionnés à l'article 37 de la présente loi ;

2° Le tarif applicable lorsque le service donne lieu à rémunération.

Un décret en Conseil d'Etat détermine les règles applicables à la diffusion par ces services d'oeuvres cinématographiques.

[....]

Extrait de la décision du 23 juillet 1996 du Conseil constitutionnel relative à la loi de réglementation des télécommunications (décision n° 96-378 DC)

[....]

SUR L'ARTICLE 15 DE LA LOI :

Considérant que l'article 15 insère 3 articles, numérotés 43-1, 43-2 et 43-3, dans la loi susvisée du 30 septembre 1986 relative à la liberté de communication ; que l'article 43-1 impose à toute personne dont l'activité est d'offrir un service de connexion à un ou plusieurs services de communication audiovisuelle mentionnés au 1° de l'article 43 de ladite loi de proposer à ses clients un moyen technique leur permettant de restreindre l'accès à certains services ou de les sélectionner ; que l'article 43-2 place un Comité supérieur de la télématique auprès du Conseil supérieur de l'audiovisuel ; que son premier alinéa dispose que ce Comité élabore des recommandations qu'il propose à l'adoption du Conseil supérieur de l'audiovisuel, propres à assurer le respect, par les services de communication audiovisuelle mentionnés au 1° de l'article 43 de cette même loi, des règles déontologiques adaptées à la nature des services proposés ; que le deuxième alinéa crée au sein du Comité supérieur de la télématique une instance chargée d'émettre, dans certaines conditions de saisine, un avis sur le respect des dites recommandations par un des services de communication concernés ; que lorsque le Comité estime que le service ne respecte pas les recommandations, son avis est publié au Journal officiel de la République française ;

que le troisième et le quatrième alinéa sont relatifs respectivement, d'une part, aux conditions dans lesquelles le Comité peut être saisi de réclamations concernant un service et à l'obligation faite au président du Conseil supérieur de l'audiovisuel d'informer le procureur de la République lorsqu'à la suite de réclamations ou de demandes d'avis, il a connaissance de faits de nature à motiver des poursuites pénales, d'autre part, aux activités d'étude, de coopération internationale et de proposition du Comité concernant de tels services ;qu'en vertu du cinquième alinéa, le Comité comprend pour moitié des professionnels représentant les fournisseurs d'accès aux services, les éditeurs de services et les éditeurs de presse et pour l'autre moitié des représentants des utilisateurs et des personnalités qualifiées parmi les quelles le président est désigné par le président du Conseil supérieur de l'audiovisuel ; que le sixième alinéa confie à un décret, pris après avis du Conseil supérieur de l'audiovisuel, le soin de préciser la composition et les modalités de fonctionnement du Comité ainsi que ses attributions en matière de services offerts sur des accès télématiques anonymes ; que l'article 43-3 dispose que les personnes dont l'activité est d'offrir un service de connexion, ne sont pas pénalement responsables des infractions résultant du contenu des messages diffusés par un service de communication audiovisuelle auquel elles donnent accès si elles ont respecté les dispositions de l'article 43-1 et si ce service n'a pas fait l'objet d'un avis défavorable publié au Journal officiel en application de l'article 43-2, sauf s'il est établi que ces personnes ont, en connaissance de cause, personnellement commis l'infraction ou participé à sa commission ;

Considérant que les auteurs de la saisine soutiennent que les dispositions de l'article 15 doivent être regardées à plusieurs titres comme inconstitutionnelles ; que le Comité supérieur de la télématique se trouverait doté de pouvoirs propres en méconnaissance de l'article 34 de la Constitution et des articles 10 et 11 de la Déclaration des Droits de l'Homme et du Citoyen ; qu'ils soutiennent que l'élaboration par le Conseil supérieur de l'audiovisuel de règles déontologiques porterait ainsi atteinte à la compétence exclusive du législateur pour fixer les règles concernant les garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques ; qu'en particulier la loi ne saurait déléguer à une autorité administrative une telle compétence sans indiquer le champ d'application précis de ces règles déontologiques et qu'il appartenait au législateur de définir la composition d'un comité intervenant dans un domaine touchant aux libertés publiques et la procédure applicable devant lui ; qu'ils font valoir également que la procédure d'adoption d'avis relatifs au respect des recommandations déontologiques par les services télématiques contrevient à plusieurs règles de nature constitutionnelle ; que la définition d'une déontologie servant de base à l'adoption d'avis faisant grief, qui seraient propres à fonder des poursuites pénales, s'apparenterait à l'édiction déguisée d'une procédure d'autorisation préalable ; qu'une instance créée au sein d'une autorité dont les compositions respectives ne sont pas définies par la loi serait ainsi appelée à donner un avis susceptible de déclencher d'éventuelles poursuites pénales ; que Le Comité supérieur de la télématique serait doté d'un pouvoir d'interprétation de la loi pénale et indirectement de déclenchement des poursuites pénales et que le juge pénal serait lié par cette interprétation ; que le principe de légalité des délits et des peines serait méconnu en ce que les avis défavorables dudit Comité, qui ont des conséquences pénales, seront pris au motif de la méconnaissance de règles déontologiques dont le contenu serait "imprécis et pour tout dire inconnu" ; qu'enfin le droit au recours effectif et les droits de la défense seraient manifestement violés ;

Considérant qu'aux termes de l'article 34 de la Constitution, la loi fixe les règles concernant les droits civiques et les garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques ; qu'il appartient au législateur d'assurer la sauvegarde des droits et des libertés constitutionnellement garantis ; que s'il peut

déléguer la mise en oeuvre de cette sauvegarde au pouvoir réglementaire, il doit toutefois déterminer lui-même la nature des garanties nécessaires ; que s'agissant de la liberté de communication, il lui revient de concilier, en l'état actuel des techniques et de leur maîtrise, l'exercice de cette liberté telle qu'elle résulte de l'article 11 de la Déclaration des Droits de l'Homme et du Citoyen, avec, d'une part, les contraintes techniques inhérentes aux moyens de communication concernés et, d'autre part, les objectifs de valeur constitutionnel que sont la sauvegarde l'ordre public, le respect de la liberté d'autrui et la préservation du caractère pluraliste des courants d'expression socioculturels ;

Considérant que la loi a confié au Comité supérieur de la télématique le soin d'élaborer et de proposer à l'adoption du Conseil supérieur de l'audiovisuel, auprès duquel il est placé, des recommandations propres à assurer le respect par certains services de communication de règles déontologiques, sans fixer à la détermination de ces recommandations, au regard desquelles des avis susceptibles d'avoir des incidences pénales pourront être émis, d'autres limites que celles, de caractère très général, résultant de l'article 1er de la loi susvisée du 30 septembre 1986 ; qu'ainsi le législateur a méconnu la compétence qu'il tient de l'article 34 de la Constitution ;

que dès lors doivent être regardées comme contraires à la Constitution les dispositions du 1er alinéa de l'article 43-2 inséré dans la loi susvisée du 30 septembre 1986 ; que les dispositions des autres alinéas dudit article et celles de l'article 43-3 en sont en tout étal de cause inséparables ; que les articles 43-2 et 43-3 introduits par l'article 15 dans la loi susvisée du 30 septembre 1986 doivent par suite être déclarés contraires à la Constitution.

Extraits du Code de la propriété intellectuelle sur le droit d'auteur (Première partie, Livre premier)

TITRE I : Objet du droit d'auteur

CHAPITRE I - Nature du droit d'auteur

Art. L.111-1. L'auteur d'une oeuvre de l'esprit jouit sur cette oeuvre, du seul fait de sa création, d'un droit de propriété incorporelle exclusif et opposable à tous.

Ce droit comporte des attributs d'ordre intellectuel et moral ainsi que des attributs d'ordre patrimonial, qui sont déterminés par les livres Ier et III du présent code.

L'existence ou la conclusion d'un contrat de louage d'ouvrage ou de service par l'auteur d'une oeuvre de l'esprit n'emporte aucune dérogation à la jouissance du droit reconnu par l'alinéa 1er.

Art. L.111-2. L'oeuvre est réputée créée, indépendamment de toute divulgation publique, du seul fait de la réalisation, même inachevée, de la conception de l'auteur.

Art. L.111-3. La propriété incorporelle définie par l'article L.111-1 est indépendante de la propriété de l'objet matériel. L'acquéreur de cet objet n'est investi, du fait de cette acquisition d'aucun des droits prévus par le présent code sauf dans les cas prévus par les dispositions des deuxième et troisième alinéas de l'article L.123-4. Ces droits subsistent en la personne de l'auteur ou de ses ayants droit qui, pourtant, ne pourront exiger du propriétaire de l'objet matériel la mise à leur disposition de cet objet pour l'exercice desdits droits. Néanmoins, en cas d'abus notoire du propriétaire empêchant l'exercice du droit de divulgation, le tribunal de grande instance peut prendre toute mesure appropriée, conformément aux dispositions de l'article L.121-3.

Art. L.111-4. Sous réserve des dispositions des conventions internationales auxquelles la France est partie, dans le cas où, après consultation du ministre des affaires étrangères, il est constaté qu'un Etat n'assure pas aux oeuvres divulguées pour la première fois en France sous quelque forme que ce soit une protection suffisante et efficace, les oeuvres divulguées pour la première fois sur le territoire de cet Etat ne bénéficient pas de la protection reconnue en matière de droit d'auteur par la législation française.

Toutefois, aucune atteinte ne peut être portée à l'intégrité ni à la paternité de ces oeuvres.

Dans l'hypothèse prévue à l'alinéa 1er ci-dessus, les droits d'auteur sont versés à des organismes d'intérêt général désignés par décret.

Art.111-5. Sous réserve des conventions internationales, les droits reconnus en France aux auteurs de logiciels par le présent code sont reconnus aux étrangers sous la condition que la loi de l'Etat dont ils sont les nationaux ou sur le territoire duquel ils ont leur domicile, leur siège social ou un établissement effectif accorde sa protection aux logiciels créés par les nationaux français et par les personnes ayant en France leur domicile ou un établissement effectif.

CHAPITRE II - Oeuvres protégées

Art. L.112-1. Les dispositions du présent code protègent les droits des auteurs sur toutes les oeuvres de l'esprit, quels qu'en soient le genre, la forme d'expression, le mérite ou la destination.

Art. L.112-2. Sont considérés notamment comme oeuvres de l'esprit au sens du présent code :

1° les livres, brochures et autres écrits littéraires, artistiques et scientifiques ;

2° les conférences, allocutions, sermons, plaidoiries et autres oeuvres de même nature;

3° les oeuvres dramatiques ou dramatico-musicales ;

4° les oeuvres chorégraphiques, les numéros et tours de cirque, les pantomimes, dont la mise en oeuvre est fixée par écrit ou autrement ;

5° les compositions musicales avec ou sans paroles ;

6° les oeuvres cinématographiques et autres oeuvres consistant dans des séquences animées d'images, sonorisées ou non, dénommées ensemble oeuvres audiovisuelles ;

7° les oeuvres de dessin, de peinture, d'architecture, de sculpture, de gravure, de lithographie;

8° les oeuvres graphiques et typographiques ;

9° les oeuvres photographiques et celles réalisées à l'aide de techniques analogues à la photographie ;

10° les oeuvres des arts appliqués ;

11° les illustrations, les cartes géographiques ;

12° les plans, croquis et ouvrages plastiques relatifs à la géographie, à la topographie, à l'architecture et aux sciences ;

13° les logiciels, y compris le matériel de conception préparatoire ;

14° les créations des industries saisonnières de l'habillement et de la parure. Sont réputées industries saisonnières de l'habillement et de la parure les industries qui, en raison des exigences de la mode, renouvellent fréquemment la forme de leurs produits, et notamment la couture, la fourrure, la lingerie, la broderie, la mode, la chaussure, la ganterie, la maroquinerie, la fabrique de tissus de haute nouveauté ou spéciaux à la haute couture, les productions des paruriers et des bottiers et les fabriques de tissus d'ameublement.

Art. L.112-3. Les auteurs de traductions, d'adaptations, transformations ou arrangements des oeuvres de l'esprit jouissent de la protection instituée par le présent code sans préjudice des droits de l'auteur de l'oeuvre originale. Il en est de même des auteurs d'anthologies ou recueils d'oeuvres diverses qui, par le choix et la disposition des matières, constituent des créations intellectuelles.

Art. L.112-4. Le titre d'une oeuvre de l'esprit, dès lors qu'il présente un caractère original, est protégé comme l'oeuvre elle-même.

Nul ne peut, même si l'oeuvre n'est plus protégée dans les termes des articles L.123-1 à L.123-3, utiliser ce titre pour individualiser une oeuvre du même genre, dans des conditions susceptibles de provoquer une confusion.

CHAPITRE III - Titulaires du droit d'auteur

Art. L.113-1. La qualité d'auteur appartient, sauf preuve contraire, à celui ou à ceux sous le nom de qui l'oeuvre est divulguée.

Art. L.113-2. Est dite de collaboration l'oeuvre à la création de laquelle ont concouru plusieurs personnes physiques.

Est dite composite l'oeuvre nouvelle à laquelle est incorporée une oeuvre préexistante sans la collaboration de l'auteur de cette dernière.

Est dite collective l'oeuvre créée sur l'initiative d'une personne physique ou morale qui l'édite, la publie et la divulgue sous sa direction et son nom et dans laquelle la contribution personnelle des divers auteurs participant à son élaboration se fond dans l'ensemble en vue duquel elle est conçue, sans qu'il soit possible d'attribuer à chacun d'eux un droit distinct sur l'ensemble réalisé.

Art. L.113-3. L'oeuvre de collaboration est la propriété commune des coauteurs.

Les coauteurs doivent exercer leurs droits d'un commun accord.

En cas de désaccord, il appartient à la juridiction civile de statuer.

Lorsque la participation de chacun des coauteurs relève de genres différents, chacun peut, sauf convention contraire, exploiter séparément sa contribution personnelle, sans toutefois porter préjudice à l'exploitation de l'oeuvre commune.

Art. L.113-4. L'oeuvre composite est la propriété de l'auteur qui l'a réalisée, sous réserve des droits de l'auteur de l'oeuvre préexistante.

Art. L.113-5. L'oeuvre collective est, sauf preuve contraire, la propriété de la personne physique ou morale sous le nom de laquelle elle est divulguée.

Cette personne est investie des droits de l'auteur.

Art. L.113-6. Les auteurs des oeuvres pseudonymes et anonymes jouissent sur celles-ci des droits reconnus par l'article L.111-1.

Ils sont représentés dans l'exercice de ces droits par l'éditeur ou le publicateur originaire, tant qu'ils n'ont pas fait connaître leur identité civile et justifié de leur qualité.

La déclaration prévue à l'alinéa précédent peut être faite par testament ; toutefois, sont maintenus les droits qui auraient pu être acquis par des tiers antérieurement.

Les dispositions des deuxième et troisième alinéas ne sont pas applicables lorsque le pseudonyme adopté par l'auteur ne laisse aucun doute sur son identité civile.

Art. L.113-7. Ont la qualité d'auteur d'une oeuvre audiovisuelle la ou les personnes physiques qui réalisent la création intellectuelle de cette oeuvre.

Sont présumés, sauf preuve contraire, coauteurs d'une oeuvre audiovisuelle réalisée en collaboration:

1° l'auteur du scénario ;

2° l'auteur de l'adaptation ;

3° l'auteur du texte parlé ;

4° l'auteur des compositions musicales avec ou sans paroles spécialement réalisées pour l'oeuvre ;

5° le réalisateur.

Lorsque l'oeuvre audiovisuelle est tirée d'une oeuvre ou d'un scénario préexistants encore protégés, les auteurs de l'oeuvre originaire sont assimilés aux auteurs de l'oeuvre nouvelle.

Art. L.113-8. Ont la qualité d'auteur d'une oeuvre radiophonique la ou les personnes physiques qui assurent la création intellectuelle de cette oeuvre.

Les dispositions du dernier alinéa de l'article L.113-7 et celles de l'article L.121-6 sont applicables aux oeuvres radiophoniques.

Art. L.113-9. Sauf dispositions statutaires ou stipulations contraires, les droits patrimoniaux sur les logiciels et leur documentation créés par un ou plusieurs employés dans l'exercice de leurs fonctions ou d'après les instructions de leur employeur sont dévolus à l'employeur qui est seul habilité à les exercer.

Toute contestation sur l'application du présent article est soumise au tribunal de grande instance du siège social de l'employeur.

Les dispositions du premier alinéa du présent article sont également applicables aux agents de l'Etat, des collectivités publiques et des établissements publics à caractère administratif.

TITRE II : Droit des auteurs

CHAPITRE Ier - Droits moraux

Art. L.121-1. L'auteur jouit du droit au respect de son nom, de sa qualité et de son oeuvre.

Ce droit est attaché à sa personne.

Il est perpétuel, inaliénable et imprescriptible.

Il est transmissible à cause de mort aux héritiers de l'auteur.

L'exercice peut être conféré à un tiers en vertu de dispositions testamentaires.

Art. L.121-2. L'auteur a seul le droit de divulguer son oeuvre. Sous réserve des dispositions de l'article L.132-24, il détermine le procédé de divulgation et fixe les conditions de celle-ci.

Après sa mort, le droit de divulgation de ses oeuvres posthumes est exercé leur vie durant par le ou les exécuteurs testamentaires désignés par l'auteur. A leur défaut, ou après leur décès, et sauf volonté contraire de l'auteur, ce droit est exercé dans l'ordre suivant : par les descendants, par le conjoint contre lequel n'existe pas un

jugement passé en force de chose jugée de séparation de corps ou qui n'a pas contracté un nouveau mariage, par les héritiers autres que les descendants qui recueillent tout ou partie de la succession et par les légataires universels ou donataires de l'universalité des biens à venir.

Ce droit peut s'exercer même après l'expiration du droit exclusif d'exploitation déterminé à l'article L.123-1.

Art. L.121-3. En cas d'abus notoire dans l'usage ou le non-usage du droit de divulgation de la part des représentants de l'auteur décédé visés à l'article L.121-2, le tribunal de grande instance peut ordonner toute mesure appropriée. Il en est de même s'il y a conflit entre lesdits représentants, s'il n'y a pas d'ayant droit connu ou en cas de vacance ou de déshérence.

Le tribunal peut être saisi notamment par le ministre chargé de la culture.

Art. L.121-4. Nonobstant la cession de son droit d'exploitation, l'auteur, même postérieurement à la publication de son oeuvre, jouit d'un droit de repentir ou de retrait vis-à-vis du cessionnaire. Il ne peut toutefois exercer ce droit qu'à charge d'indemniser préalablement le cessionnaire du préjudice que ce repentir ou ce retrait peut lui causer. Lorsque, postérieurement à l'exercice de son droit de repentir ou de retrait, l'auteur décide de faire publier son oeuvre, il est tenu d'offrir par priorité ses droits d'exploitation au cessionnaire qu'il avait originairement choisi et aux conditions originairement déterminées.

Art. L.121-5. L'oeuvre audiovisuelle est réputée achevée lorsque la version définitive a été établie d'un commun accord entre, d'une part, le réalisateur ou, éventuellement les coauteurs et, d'autre part, le producteur.

Il est interdit de détruire la matrice de cette version.

Toute modification de cette version par addition, suppression ou changement d'un élément quelconque exige l'accord des personnes mentionnées au premier alinéa.

Tout transfert de l'oeuvre audiovisuelle sur un autre type de support en vue d'un autre mode d'exploitation doit être précédé de la consultation du réalisateur.

Les droits propres des auteurs, tels qu'ils sont définis à l'article L.121-1, ne peuvent être exercés par eux que sur l'oeuvre audiovisuelle achevée.

Art. L.121-6. Si l'un des auteurs refuse d'achever sa contribution à l'oeuvre audiovisuelle ou se trouve dans l'impossibilité d'achever cette contribution par suite de force majeure, il ne pourra s'opposer à l'utilisation, en vue de l'achèvement de l'oeuvre, de la partie de cette contribution déjà réalisée. Il aura, pour cette contribution, la qualité d'auteur et jouira des droits qui en découlent.

Art. L.121-7. Sauf stipulation contraire plus favorable à l'auteur d'un logiciel, celui-ci ne peut :

1°. S'opposer à la modification du logiciel par le cessionnaire des droits mentionnés au 2°. de l'article L.122-6, lorsqu'elle n'est préjudiciable ni à son honneur, ni à sa réputation ;

2°. Exercer son droit de repentir ou de retrait.

Art. L.121-8. L'auteur seul a le droit de réunir ses articles et ses discours en recueil et de les publier ou d'en autoriser la publication sous cette forme.

Pour toutes les oeuvres publiées ainsi dans un journal ou recueil périodique l'auteur conserve, sauf stipulation contraire, le droit de les faire reproduire et de les exploiter, sous quelque forme que ce soit, pourvu que cette reproduction ou cette exploitation ne soit pas de nature à faire concurrence à ce journal ou à ce recueil périodique.

[....]

CHAPITRE II - Droits patrimoniaux

Art. L.122-1. Le droit d'exploitation appartenant à l'auteur comprend le droit de représentation et le droit de reproduction.

Art. L.122-2. La représentation consiste dans la communication de l'oeuvre au public par un procédé quelconque, et notamment :

1° par récitation publique, exécution lyrique, représentation dramatique, présentation publique, projection publique et transmission dans un lieu public de l'oeuvre télédiffusée ;

2° par télédiffusion.

La télédiffusion s'entend de la diffusion par tout procédé de télécommunication de sons, d'images, de documents, de données et de messages de toute nature.

Est assimilée à une représentation l'émission d'une oeuvre vers un satellite.

Art. L.122-3. La reproduction consiste dans la fixation matérielle de l'oeuvre par tous procédés qui permettent de la communiquer au public d'une manière indirecte.

Elle peut s'effectuer notamment par imprimerie, dessin, gravure, photographie, moulage et tout procédé des arts graphiques et plastiques, enregistrement mécanique, cinématographique ou magnétique.

Pour les oeuvres d'architecture, la reproduction consiste également dans l'exécution répétée d'un plan ou d'un projet type.

Art. L.122-4. Toute représentation ou reproduction intégrale ou partielle faite sans le consentement de l'auteur ou de ses ayants droit ou ayants cause est illicite. Il en est de même pour la traduction, l'adaptation ou la transformation, l'arrangement ou la reproduction par un art ou un procédé quelconque.

Art. L.122-5. Lorsque l'oeuvre a été divulguée, l'auteur ne peut interdire :

1° les représentations privées et gratuites effectuées exclusivement dans un cercle de famille ;

2° les copies ou reproductions strictement réservées à l'usage privé du copiste et non destinées à une utilisation collective, à l'exception des copies des oeuvres d'art destinées à être utilisées pour des fins identiques à celles pour lesquelles l'oeuvre originale a été créée et des copies d'un logiciel autres que la copie de sauvegarde établie dans les conditions prévues au II de l'article L.122-6-1 ;

3°. Sous réserve que soient indiqués clairement le nom de l'auteur et la source :

a) les analyses et courtes citations[13] justifiées par le caractère critique, polémique, pédagogique, scientifique ou d'information de l'oeuvre à laquelle elles sont incorporées;

b) les revues de presse ;

c) la diffusion, même intégrale, par la voie de presse ou de télédiffusion, à titre d'information d'actualité, des discours destinés au public prononcés dans les assemblées politiques, administratives, judiciaires ou académiques, ainsi que dans les réunions publiques d'ordre politique et les cérémonies officielles ;

4° la parodie, le pastiche et la caricature, compte tenu des lois du genre.

Art. L.122-6. Sous réserve des dispositions de l'article L.122-6-1, le droit d'exploitation appartenant à l'auteur d'un logiciel comprend le droit d'effectuer et d'autoriser :

1° La reproduction permanente ou provisoire d'un logiciel en tout ou partie par tout moyen et sous toute forme. Dans la mesure où le chargement, l'affichage, l'exécution, la transmission ou le stockage de ce logiciel nécessitent une reproduction, ces actes ne sont possibles qu'avec l'autorisation de l'auteur ;

2° La traduction, l'adaptation, l'arrangement ou toute autre modification d'un logiciel et la reproduction du logiciel en résultant ;

3° La mise sur le marché à titre onéreux ou gratuit, y compris la location, du ou des exemplaires d'un logiciel par tout procédé. Toutefois, la première vente d'un exemplaire d'un logiciel dans le territoire d'un Etat membre de la Communauté européenne ou d'un Etat partie à l'accord sur l'Espace économique européen par l'auteur ou avec son consentement épuise le droit de mise sur le marché de cet exemplaire dans tous les Etats membres à l'exception du droit d'autoriser la location ultérieure d'un exemplaire.

Art. L.122-6-1. I. Les actes prévus aux 1° et 2° de l'article L.122-6 ne sont pas soumis à l'autorisation de l'auteur lorsqu'ils sont nécessaires pour permettre l'utilisation du logiciel, conformément à sa destination, par la personne ayant le droit de l'utiliser, y compris pour corriger des erreurs.

Toutefois, l'auteur est habilité à se réserver par contrat le droit de corriger les erreurs et de déterminer les modalités particulières auxquelles seront soumis les actes prévus aux 1° et 2° de l'article L.122-6, nécessaires pour permettre l'utilisation du logiciel, conformément à sa destination, par la personne ayant le droit de l'utiliser.

II. La personne ayant le droit d'utiliser le logiciel peut faire une copie de sauvegarde lorsque celle-ci est nécessaire pour préserver l'utilisation du logiciel.

III. La personne ayant le droit d'utiliser le logiciel peut sans l'autorisation de l'auteur observer, étudier ou tester le fonctionnement de ce logiciel afin de déterminer les idées et principes qui sont à la base de n'importe quel élément du logiciel lorsqu'elle effectue toute opération de chargement, d'affichage, d'exécution, de transmission ou de stockage du logiciel qu'elle est en droit d'effectuer.

IV. La reproduction du code du logiciel ou la traduction de la forme de ce code n'est pas soumise à l'autorisation de l'auteur lorsque la reproduction ou la traduction au sens du 1° ou du 2° de l'article L.122-6 est indispensable pour obtenir les informations nécessaires à l'interopérabilité d'un logiciel créé de façon indépendante avec d'autres logiciels, sous réserve que soient réunies les conditions suivantes:

1° ces actes sont accomplis par la personne ayant le droit d'utiliser un exemplaire du logiciel ou pour son compte par une personne habilitée à cette fin ;

2° les informations nécessaires à l'interopérabilité n'ont pas déjà été rendues facilement et rapidement accessibles aux personnes mentionnées au 1deg. ci-dessus;

3° et ces actes sont limités aux parties du logiciel d'origine nécessaires à cette interopérabilité.

Les informations ainsi obtenues ne peuvent être :

1° ni utilisées à des fins autres que la réalisation de l'interopérabilité du logiciel créé de façon indépendante;

2° ni communiquées à des tiers sauf si cela est nécessaire à l'interopérabilité du logiciel créé de façon indépendante ;

3° ni utilisées pour la mise au point, la production ou la commercialisation d'un logiciel dont l'expression est substantiellement similaire ou pour tout autre acte portant atteinte au droit d'auteur.

V. Le présent article ne saurait être interprété comme permettant de porter atteinte à l'exploitation normale du logiciel ou de causer un préjudice injustifié aux intérêts légitimes de l'auteur.

Toute stipulation contraire aux dispositions prévues aux II, III et IV du présent article est nulle et non avenue.

Art. L.122-6-2. Toute publicité ou notice d'utilisation relative aux moyens permettant la suppression ou la neutralisation de tout dispositif technique protégeant un logiciel doit mentionner que l'utilisation illicite de ces moyens est passible des sanctions prévues en cas de contrefaçon.

Un décret en Conseil d'Etat fixera les conditions d'application du présent article.

Art. L.122-7. Le droit de représentation et le droit de reproduction sont cessibles à titre gratuit ou à titre onéreux.

La cession du droit de représentation n'emporte pas celle du droit de reproduction.

La cession du droit de reproduction n'emporte pas celle du droit de représentation.

Lorsqu'un contrat comporte cession totale de l'un des deux droits visés au présent article, la portée en est limitée aux modes d'exploitation prévus au contrat.

[....]

Art. L.122-10. La publication d'une oeuvre emporte cession du droit de reproduction par reprographie à une société régie par le titre II du livre III et agréée à cet effet par le ministre chargé de la culture. Les sociétés agréées peuvent seules conclure toute convention avec les utilisateurs aux fins de gestion du droit ainsi cédé, sous réserve, pour les stipulations autorisant les copies aux fins de vente, de location, de publicité ou de promotion, de l'accord de l'auteur ou de ses ayants droit. A défaut de désignation par l'auteur ou son ayant droit à la date de la publication de l'oeuvre, une des sociétés agréées est réputée cessionnaire de ce droit.

La reprographie s'entend de la reproduction sous forme de copie sur papier ou support assimilé par une technique photographique ou d'effet équivalent permettant une lecture directe.

Les dispositions du premier alinéa ne font pas obstacle au droit de l'auteur ou de ses ayants droit de réaliser des copies aux fins de vente, de location, de publicité ou de promotion.

Nonobstant toute stipulation contraire, les dispositions du présent article s'appliquent à toutes les oeuvres protégées quelle que soit la date de leur publication.

Art. L.122-11. Les conventions mentionnées au premier alinéa de l'article L.122-10 peuvent prévoir une rémunération forfaitaire dans les cas définis aux 1° à 3° de l'article L.131-4.

Art. L.122-12. L'agrément des sociétés mentionnées au premier alinéa de l'article L.122-10 est délivré en considération :

- de la diversité des associés ;

- de la qualification professionnelle des dirigeants ;

- des moyens humains et matériels qu'ils proposent de mettre en oeuvre pour assurer la gestion du droit de reproduction par reprographie ;

- du caractère équitable des modalités prévues pour la répartition des sommes perçues.

Un décret en Conseil d'Etat fixe les modalités de la délivrance et du retrait de cet agrément ainsi que du choix des sociétés cessionnaires en application de la dernière phrase du premier alinéa de l'article L.122-10.

CHAPITRE III - Durée de la protection

Art. L.123-1. L'auteur jouit, sa vie durant, du droit exclusif d'exploiter son oeuvre sous quelque forme que ce soit et d'en tirer un profit pécuniaire.

Au décès de l'auteur, ce droit persiste au bénéfice de ses ayants droit pendant l'année civile en cours et les cinquante années qui suivent. Toutefois, pour les compositions musicales avec ou sans paroles, cette durée est de soixante-dix années.

[....]

Titre III : exploitation des droits

Chapitre premier : dispositions générales

Art. L.131-1. La cession globale des oeuvres futures est nulle.

Art. L.131-2. Les contrats de représentation, d'édition et de production audiovisuelle définis au présent titre doivent être constatés par écrit. Il en est de même pour les autorisations gratuites d'exécution.

Dans tous les autres cas les dispositions des articles 1341 à 1348 du code civil sont applicables.

Art. L.131-3. La transmission des droits de l'auteur est subordonnée à la condition que chacun des droits cédés fasse l'objet d'une mention distincte dans l'acte de cession et que le domaine d'exploitation des droits cédés soit délimité quant à son étendue et à sa destination, quant au lieu et quant à la durée.

Lorsque des circonstances spéciales l'exigent, le contrat peut être valablement conclu par échange de télégrammes, à condition que le domaine d'exploitation des droits cédés soit délimité conformément aux termes du premier alinéa du présent article. Les cessions portant sur les droits d'adaptation audiovisuelle doivent faire l'objet d'un contrat écrit sur un document distinct du contrat relatif à l'édition proprement dite de l'oeuvre imprimée.

Le bénéficiaire de la cession s'engage par ce contrat à rechercher une exploitation du droit cédé conformément aux usages de la profession et à verser à l'auteur, en cas d'adaptation, une rémunération proportionnelle aux recettes perçues.

Art. L.131-4. La cession par l'auteur de ses droits sur son oeuvre peut être totale ou partielle. Elle doit comporter au profit de l'auteur la participation proportionnelle aux recettes provenant de la vente ou de l'exploitation.

Toutefois, la rémunération de l'auteur peut être évaluée forfaitairement dans les cas suivants :

1° la base de calcul de la participation proportionnelle ne peut être pratiquement déterminée ;

2° les moyens de contrôler l'application de la participation font défaut ;

3° les frais des opérations de calcul et de contrôle seraient hors de proportion avec les résultats à atteindre;

4° la nature ou les conditions de l'exploitation rendent impossible l'application de la règle de la rémunération proportionnelle, soit que la contribution de l'auteur ne constitue pas l'un des éléments essentiels de la création intellectuelle de l'oeuvre, soit que l'utilisation de l'oeuvre ne présente qu'un caractère accessoire par rapport à

l'objet exploité ;

5° en cas de cession des droits portant sur un logiciel ;

6° dans les autres cas prévus au présent code.

Est également licite la conversion entre les parties, à la demande de l'auteur, des droits provenant des contrats en vigueur en annuités forfaitaires pour des durées à déterminer entre les parties.

Art. L.131-6. La clause d'une cession qui tend à conférer le droit d'exploiter l'oeuvre sous une forme non prévisible ou non prévue à la date du contrat doit être expresse et stipuler une participation corrélative aux profits d'exploitation.

[....]

Décision rendue dans l'affaire UEJF c/ Calvacom et autres, TGI Paris, ordonnance de référé, 12 juin 1996

L'Union des Etudiants Juifs de France/ Calvacom (Calvanet réseau Calvacom), la société Eunet France, Axone, (Apysoft)Oléane, Compuserve France (Information service, Francenet, Internet Way, Imaginet Sa (RG Finance), GIP RENATER

Attendu que l'Union des Etudiants Juifs de France a, le 5 mars 1996, fait assigner les sociétés Calvacom (Calvanet réseau Calvacom), Eunet France, Axone -IBM Global Network, Apysoft -Oléane, Compuserve France, Francenet, Internet Way, Imaginet SA (RG Finance) & le GIP RENATER, pour qu'il leur soit ordonné, sous astreinte, d'empêcher toute connexion, à partir de leur serveur d'accès et plus généralement par leur intermédiaire direct ou indirect, à tout service ou message diffusé sur le réseau Internet quelle qu'en soit la provenance, méconnaissant ostensiblement pas sa présentation, son objet ou son contenu, les dispositions de l'article 24 bis de la loi du 24 juillet 1881;

Attendu que les parties se sont expliquées relativement à cette présentation, lors de l'audience du 15 mars 1996, à l'issue de laquelle elles ont été invitées à se rapprocher; qu'afin de favoriser la recherche d'un accord, une nouvelle audience a été tenue le 3 avril 1996; qu'elle a été suivie de l'envoi de notes en délibéré faisant apparaître une évolution du litige; que le respect des droits de la défense et du principe de la contradiction a conduit à ordonner le 22 mais 1996 la réouverture des débats au 29 mai 1996;

Attendu que la demande récapitulative présentée par l'Union des Etudiants Juifs de France pour cette audience est la suivante :

A TITRE PRINCIPAL

Constater que la diffusion publique auprès d'un nombre indéterminé d'utilisateurs du réseau Internet(ou sous-réseau) et sur le territoire de la République, de messages ou d'informations à caractère raciste, antisémite ou négationniste, par l'intermédiaire direct ou indirect des sociétés défenderesses, est constitutive d'un trouble manifestement illicite autant que d'un dommage immi-

nent, et ce quelle que soit la provenance de ces messages ou informations;

Décerner les actes requis par Internet Way, Calvacom, Imaginet, Francenet, Axone, Oléane & le GIP RENATER, en ce qui concerne la régulation des informations & messages disponibles sur leurs propres sites;

Donner acte à l'Union des Etudiants Juifs de France de ce qu'elle s'estime sur ce point, en l'état et jusqu'à plus ample informé, remplie de ses droits à l'égard de toutes les défenderesses;

Surseoir à statuer sur les exceptions de procédures soulevées par le GIP RENATER et les sociétés Compuserve, Oléane, Eunet ou autres dans l'intérêt d'une bonne administration de la Justice, par l'application de l'article 378 du Nouveau Code de Procédure Civile, et subsidiairement les en débouter;

Désigner en qualité de consultant de l'Institut de Recherche Criminelle de la Gendarmerie Nationale avec pour mission de fournir tout élément d'appréciation utile sur les mesures ou remèdes d'ordre technique de nature à empêcher ou restreindre la diffusion ou la réception sur le territoire de la République de certains messages ou informations disponibles sur le réseau Internet ou sous-réseau, et réputés contraires à la loi réprimant les infractions commises pas voie de communication au public, et en l'occurrence à caractère raciste, antisémite ou négationniste;

SUBSIDIAIREMENT

Statuer dans les termes de l'acte introductif d'instance;

Débouter les défenderesses de toutes leurs exceptions et demandes reconventionnelles;

Attendu que rien ne fait obstacle à ce que soient décernés les actes requis tant en demande qu'en défense;

Attendu que l'Union des Etudiants Juifs de France s'estime, en considération de ces derniers, remplie de ses droits à l'égard des sociétés Internet Way, Calvacom, Imaginet, Francenet, Axone, Oléane et du GIP RENATER, pour ce qui se rapporte à la régularisation des informations & messages disponibles sur leurs propres sites; qu'elle ne peut donc, tout en adoptant une telle position, solliciter qu'il soit sursis à statuer sur les exceptions de procédure de la société Oléane et du GIP RENATER, alors surtout que rien n'indique que, eu égard à l'évolution du litige, ces moyens trouvent encore leur place dans le présent débat;

Attendu que la bonne administration de la Justice ne commande pas de suspendre l'instance relativement aux moyens de procédure soulevés par les sociétés Compuserve & Eunet car le sort de ceux-ci conditionne l'examen des autres prétentions en l'espèce soumises;

Attendu que l'Union des Etudiants Juifs de France justifie de son droit d'agir en la présente cause, en sorte que les fins de non-recevoir qui lui sont à cet égard opposées doivent être écartées;

Attendu, en revanche, que les demandes maintenues par cette association, en sus de celles ci-avant examinées, ne peuvent être accueillies;

Attendu, en effet, qu'il est défendu aux juges de prononcer par voie de disposition générale et réglementaire sur les causes qui leur sont soumises; que, par ailleurs, la liberté d'expression constitue une valeur fondamentale, dont les juridictions de l'ordre judiciaire sont gardiennes, et qui n'est susceptible de trouver de limites, que dans des hypothèses particulières, selon des modalités strictement déterminées;

Attendu que la mesure d'instruction sollicitée, si elle serait certes de nature à permettre la collecte d'informations intéressantes, en particulier sur un plan technique, ne présenterait cependant pas d'utilité dans le cadre de la présente instance, dont l'issue ne saurait être marquée par l'institution d'un système global de prohibition et de censure préalable, qui au demeurant, eu égard à l'effet relatif de cette décision, ne concernerait qu'une partie des membres de la profession, et encore de manière provisoire; que s'il est bien certain, et les codéfendeurs se sont dans l'ensemble accordés à le reconnaître, que les craintes manifestées par l'Union des Etudiants Juifs de France sont hautement respectables, elles ne peuvent cependant conduire à des constatations générales,

dépourvues de surcroît de conséquences pratiques, ou encore à des interdictions que seule la démonstration de manquements précis pourrait le cas échéant légitimer; qu'il ne peut en l'état être considéré qu'une telle preuve se trouve apportée, car force est de constater que le procès-verbal de constat dressé les 20 & 21 mai 1996 par Maître Couchoud, Huissier de Justice à Paris, et produit par la réclamante au soutien de ses prétentions, renferme un certain nombre d'imprécisions, et que sans qu'il soit le moins du monde question de suspecter la bonne foi des intervenants, diverses incertitudes existent, notamment en ce qui concerne le processus exact de la démonstration opérée devant le constatant, manifestement profane en la matière, par un étudiant dont l'identité n'est d'ailleurs point fournie;

Attendu que n'est pas établie l'existence d'une obligation non sérieusement contestable au paiement des dommages-intérêts reconventionnellement réclamés;

Attendu que des raisons tirées de considérations d'équité conduisent à écarter l'application de l'article 700 du Nouveau Code de Procédure Civile;

PAR CES MOTIFS,

Donnons acte aux sociétés Calvacom, Internet Way, Imaginet & Francenet de ce qu'elles déclarent:

- qu'elles ne peuvent que s'engager à développer leurs meilleurs efforts pour, dans l'hypothèse où l'un de leurs abonnés ou l'un de leurs annonceurs contreviendrait aux dispositions de la loi du 29 juillet 1881 de manière suffisamment évidente :

- soit obtenir qu'il cesse ses agissements,

- soit rompre le contrat de prestation qui les lient à cet abonné ou à cet annonceur, dans le respect des conditions générales dudit contrat, qui sont, à ce jour, spécifiques à chacune des quatre sociétés, et ce, afin de tenter d'empêcher, autant que faire se peut, la promotion et la diffusion involontaires, à partir de leurs pages "WEB" et Forums de Discussions propres, de tout message ou propos contraire à la loi du 29 juillet 1881 et notamment raciste, antisémite ou négationniste;

- qu'elles considèrent que la seule éventuelle responsabilité qui serait susceptible d'être recherchée à leur encontre, devrait être limitée aux seules pages "WEB" et Forums de Discussion dont elles sont les concepteurs, les animateurs, et/ou qu'elles hébergent volontairement pour les diffuser, soit pour leur propre compte, soit pour le compte de tiers, abonnés ou annonceurs, auxquels elles sont contractuellement liées;

- qu'elles ont déjà mis en oeuvre des moyens d'information et de sensibilisation et que notamment elles imposent et imposeront à leurs abonnés et annonceurs, l'obligation formelle de se conformer aux dispositions de la loi du 29 juillet 1881, à peine de rupture immédiate et à leurs seuls torts du contrat les liant à elles, sauf à ce qu'il soit remédié immédiatement à toute violation constatée;

- qu'en ce qui concerne les Forums de Discussion étrangers aux leurs et dont le contenu violerait les dispositions de la loi du 29 juillet 1881, elles considèrent qu'elles ne seraient susceptibles d'en supprimer le référencement et l'accès simplifié, que dans la mesure où la demande leur en serait faite pas une autorité institutionnelle légalement habilitée et qui aurait seule la charge d'identifier lesdits forums et la responsabilité d'en décider la fermeture;

- qu'elles estiment n'avoir en aucun cas le moyen d'empêcher l'un ou l'autre de leurs abonnés de se connecter à leur insu à ces Forums de Discussion;

Donnons acte à la société Axone qu'elle déclare:

- qu'elle n'a pas encore été confrontée à des situations dans lesquelles le problème de la "régulation" évoqué par l'UEJF se trouverait posé;

- que compte tenu des spécificités du réseau Internet et de son rôle de fournisseur d'accès, elle estime qu'aucune responsabilité juridique ne pèse sur elle d'avoir à réguler les informations disponibles sur le réseau, que ces informations puissent être consultées pas ses clients, ou qu'elles soient émises pas eux, cette responsabilité ne pouvant reposer que sur les auteurs des informations;

- qu'en conséquence, dans le cadre actuel de la législation, elle estime ne pas avoir à se substituer, ni aux auteurs dans l'appréciation de cette responsabilité, ni au Juge dans la qualification juridique que la diffusion des informations peut mériter; qu'il revient donc normalement aux victimes ou au ministère public de se pourvoir en Justice à l'encontre des auteurs, éventuellement en requérant dans ce cadre des fournisseurs d'accès une action

particulière dans la mesure où celle-ci serait envisageable et efficace ;

- qu'elle estime néanmoins pouvoir appliquer certaines règles déontologiques, ci-après précisées, sous les réserves expresses de principe suivantes:

- son action déontologique ne peut s'exercer qu'auprès des personnes avec lesquelles elle est liée contractuellement pour l'hébergement des services Internet, et dans la mesure où ces personnes seraient auteurs d'informations tombant sous le coup de la législation française réprimant pénalement des délits commis par voie de communication au public,

- elle ne peut agir que dans les cas où de toute évidence et sans excuse possible lesdites informations tombent sous le coup de la loi, sous peine pour elle, en se substituant au juge, de ne plus fournir à ses clients le service qu'ils sont en droit d'attendre,

- un contrôle systématique à son initiative des informations disponibles sur le réseau, y compris celles provenant de ses propres clients, est tout à fait exclu,

- s'agissant de l'application d'une règle déontologique qu'elle se fixe elle-même, et non d'une obligation légale, elle ne peut qu'exercer son meilleur jugement et le faire en toute liberté, et son action comme son inaction ne sauraient engager sa responsabilité,

- en considération de ce qui précède, son action déontologique s'exercera lorsqu'elle aura effectivement connaissance qu'en provenance apparente d'une même personne identifiable liée contractuellement à elle pour l'hébergement de services Internet, des informations sont mises sur le réseau de façon répétée et que ces informations tombent de toute évidence et sans excuse possible sous le coup de la législation susvisée; cette action consistera pour elle à se mettre en rapport avec cette personne à l'effet de provoquer ses explications et l'avertir le cas échéant que le renouvellement de tels agissements la conduira à résilier son contrat ou à lui interdire, de façon temporaire ou définitive, l'accès au réseau;

- elle adaptera ses contrats-types à l'effet de prévoir expressément une clause à l'effet ci-dessus;

Donnons acte à la Société Oléane de ce qu'elle déclare:

- qu'en sa qualité de fournisseur de services et d'accès Internet elle a plusieurs activités; qu'en sa qualité d'hébergeur de pages "WEB" et de "user group" sa politique est clairement d'éviter que les services hébergés sur ses serveurs et avec lesquels elle a signé un contrat d'hébergement, ne diffusent des informations contraires à la loi;

- qu'elle se réserve à cet égard la possibilité de déconnecter, après avertissements préalables non suivis d'effet, tout client publiant de telles informations;

- qu'elle ne se considère pas comme tenue et ne s'engage à aucune obligation de vérification systématique de l'ensemble des informations publiée sur le réseau;

- qu'au cas où son attention serait attirée sur le fait que certaines informations publiées sur son serveur seraient contraires à la loi, elle se réserve de prendre les mesures susvisées;

Donnons acte au GIP RENATER de ce qu'il déclare:

- qu'il est destiné au monde de la recherche, du développement technologique, de l'enseignement supérieur, de la diffusion de l'information scientifique & technique; qu'il a élaboré une "charte d'usage et de sécurité" (disponible sur le site WWW RENATER) destinée à responsabiliser chaque site utilisateur au respect d'un code de bonne conduite applicable à tous les sites utilisateurs;

- qu'en application de cette charte, chaque site utilisateur signataire désigne un responsable de site qui doit s'engager vis-à-vis du GIP à respecter les dispositions qui y sont définies et à les faire respecter par tous les utilisateurs relevant de son autorité;

- qu'en cas de manquement aux règles d'usage et de sécurité, il peut être amené à suspendre l'accès du site concerné à son réseau;

Donnons acte à l'Union des Etudiants Juifs de France de ce qu'en considération des actes qui précèdent, décernés aux sociétés Internet Way, Calvacom, Imaginet, Francenet, Axone, Oléane & au GIP RENATER, relativement à la régulation des informations et messages disponibles sur leurs propres sites, elle s'estime, en l'état et jusqu'à plus ample informé, remplie de ses droits à l'égard de toutes les défenderesses;

Et rejetant toute autre demande, laissons à chacune des parties la charge de ses propres dépens.

Extraits de la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et à la libre circulation de ces données

[....]

CHAPITRE I - DISPOSITIONS GENERALES

Article premier - Objet de la directive

1. Les Etats membres assurent, conformément aux dispositions de la présente directive, la protection des libertés et des droits fondamentaux des personnes physiques, et en particulier du droit à la vie privée, à l'égard du traitement des données à caractère personnel.

2. Les Etats membres ne peuvent restreindre ni interdire la libre circulation des données à caractère personnel entre Etats membres pour des raisons relatives à la protection assurée en vertu du paragraphe 1.

Article 2 - Définitions

Aux fins de la présente directive, on entend par :

a) "données à caractère personnel", toute information concernant une personne physique identifiée ou identifiable ("personne concernée"); est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale ;

b) "traitement de données à caractère personnel" ("traitement"), toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés, et appliquées à des données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou interconnexion, ainsi que le verrouillage, l'effacement ou la destruction ;

c) "fichier de données à caractère personnel" ("fichier"), tout ensemble structuré de données à caractère personnel accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique ;

d) "responsable du traitement", la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel; lorsque les finalités et les moyens du traitement sont déterminées par des dispositions législatives ou réglementaires nationales ou communautaires, le responsable du traitement ou les critères spécifiques pour le désigner peuvent être fixés par le droit national ou communautaire ;

e) "sous-traitement", la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement ;

f) "tiers", la personne physique ou morale, l'autorité publique, le service ou tout autre organisme autre que la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui, placées sous l'autorité directe du responsable du traitement ou du sous-traitant, sont habilitées à traiter les données ;

g) "destinataire" : la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication de données, qu'il s'agisse ou non d'un tiers; les autorités qui sont susceptibles de recevoir communication de données dans le cadre d'une mission d'enquête particulière ne sont toutefois pas considérées comme des destinataires ;

h) "consentement de la personne concernée", toute manifestation de volonté, libre, spécifique et informée par laquelle la personne concernée accepte que des données à caractère personnel la concernant fassent l'objet d'un traitement.

Article 3 - Champ d'application

1. La présente directive s'applique au traitement de données à caractère personnel automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier.

2. La présente directive ne s'applique pas au traitement de données à caractère personnel :

- mis en oeuvre pour l'exercice d'activités qui ne relèvent pas du champ d'application du droit communautaire, telles que celles prévues aux titres V et VI du traité sur l'Union européenne et, en tout état de cause, aux traitements ayant pour objet la sécurité publique, la défense, la sûreté de l'Etat (y compris le bien-être économique de l'Etat lorsque ces traitements sont liés à des questions de sûreté de l'Etat) et les activités de l'Etat relatives à des domaines du droit pénal ;

- effectué par une personne physique pour l'exercice d'activités exclusivement personnelles ou domestiques.

Article 4 - Droit national applicable

1. Chaque Etat membre applique les dispositions nationales qu'il arrête en vertu de la présente directive aux traitements de données à caractère personnel lorsque:

a) le traitement est effectué dans le cadre des activités d'un établissement du responsable du traitement sur le territoire de l'Etat membre; si un même responsable du traitement est établi sur le territoire de plusieurs Etats membres, il doit prendre les mesures nécessaires pour assurer le respect, par chacun de ses établissements, des obligations prévues par le droit national applicable ;

b) le responsable du traitement n'est pas établi sur le territoire de l'Etat membre mais en un lieu où sa loi nationale s'applique en vertu du droit international public ;

c) le responsable du traitement n'est pas établi sur le territoire de la Communauté et recourt, à des fins de traitement de données à caractère personnel, à des moyens, automatisés ou non, situés sur le territoire dudit Etat membre, sauf si ces moyens ne sont utilisés qu'à des fins de transit sur le territoire de la Communauté.

2. Dans le cas visé au paragraphe 1 point c), le responsable du traitement doit désigner un représentant établi sur le territoire dudit Etat membre, sans préjudice d'actions qui pourraient être introduites contre le responsable du traitement lui-même.

CHAPITRE II - LES CONDITIONS GENERALES DE LICEITE DES TRAITEMENTS DE DONNEES A CARACTERE PERSONNEL

Article 5

Les Etats membres précisent, dans les limites des dispositions du présent chapitre, les conditions dans

lesquelles les traitements de données à caractère personnel sont licites.

SECTION I - PRINCIPES RELATIFS A LA QUALITE DES DONNEES

Article 6

1. Les Etats membres prévoient que les données à caractère personnel doivent être:

a) traitées loyalement et licitement ;

b) collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités. Un traitement ultérieur à des fins historiques, statistiques ou scientifiques n'est pas réputé incompatible pour autant que les Etats membres prévoient des garanties appropriées ;

c) adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement ;

d) exactes et, si nécessaire, mises à jour; toutes les mesures raisonnables doivent être prises pour que les données inexactes ou incomplètes, au regard des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement, soient effacées ou rectifiées ;

e) conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement. Les Etats membres prévoient des garanties appropriées pour les données à caractère personnel qui sont conservées au-delà de la période précitée, à des fins historiques, statistiques ou scientifiques.

2. Il incombe au responsable du traitement d'assurer le respect du paragraphe 1.

SECTION II - PRINCIPES RELATIFS AUX FONDEMENTS DES TRAITEMENTS DE DONNEES

Article 7

Les Etats membres prévoient que le traitement de données à caractère personnel ne peut être effectué que si :

a) la personne concernée a donné son consentement ou ;

b) il est nécessaire à l'exécution du contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci ou ;

c) il est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis ou ;

d) il est nécessaire à la sauvegarde de l'intérêt vital de la personne concernée ou ;

e) il est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique, dont est investi le responsable du traitement ou le tiers auquel les données sont communiquées ou ;

f) il est nécessaire à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le ou les tiers auxquels les données sont communiquées, à condition que ne prévale pas l'intérêt ou les droits et libertés fondamentaux de la personne concernée qui appellent une protection au titre de l'article 1er paragraphe 1.

SECTION III - CATEGORIES PARTICULIERES DE TRAITEMENTS

Article 8 - Traitements portant sur des catégories particulières de données

1. Les Etats membres interdisent le traitement des données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que le traitement des données relatives à la santé et à la vie sexuelle.

2. Le paragraphe 1 ne s'applique pas, lorsque :

a) la personne concernée a donné son consentement explicite à un tel traitement, sauf dans le cas où la législation de l'Etat membre prévoit que l'interdiction visée au paragraphe 1 ne peut être levée par le consentement de la personne concernée ou ;

b) le traitement est nécessaire aux fins de respecter les obligations et les droits spécifiques du responsable du traitement en matière de droit du travail, dans la mesure où il est autorisé par une législation nationale prévoyant des garanties adéquates ou ;

c) le traitement est nécessaire à la défense des intérêts vitaux de la personne concernée ou d'une autre personne dans le cas où la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement ou ;

d) le traitement est effectué dans le cadre de leurs activités légitimes et avec des garanties appropriées par une fondation, une association ou tout autre organisme à but non lucratif, à finalité politique, philosophique, religieuse ou syndicale, à condition que le traitement se rapporte aux seuls membres de cet organisme ou aux

personnes entretenant avec lui des contacts réguliers liés à sa finalité et que les données ne soient pas communiquées à des tiers sans le consentement des personnes concernées ou ;

e) le traitement porte sur des données manifestement publiques par la personne concernée ou est nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice.

3) Le paragraphe 1 ne s'applique pas lorsque le traitement des données est nécessaire aux fins de la médecine préventive, des diagnostics médicaux, de l'administration de soins ou de traitements ou de la gestion de services de santé et que le traitement de ces données est effectué par un praticien de la santé soumis à l'obligation du secret professionnel sanctionné par le droit national, ou par des réglementations arrêtées par les autorités nationales compétentes au secret professionnel, ou par une autre personne également soumise à une obligation de secret équivalente.

4. Sous réserve de garanties appropriées, les Etats membres peuvent prévoir, pour un motif d'intérêt public important, des dérogations autres que celles prévues au paragraphe 2, soit par leur législation nationale, soit sur décision de l'autorité de contrôle.

5. Le traitement de données relatives aux infractions, aux condamnations pénales ou aux mesures de sécurité ne peut être effectué que sous le contrôle de l'autorité publique ou si des garanties appropriées et spécifiques sont prévues par le droit national, sous réserve des dérogations qui peuvent être accordées par l'Etat membre sur la base de dispositions nationales prévoyant des garanties appropriées et spécifiques. Toutefois, un recueil des condamnations pénales ne peut être tenu que sous le contrôle de l'autorité publique.

Les Etats membres peuvent prévoir que les données relatives aux sanctions administratives ou aux jugements civils sont également traitées sous le contrôle de l'autorité publique.

6. Les dérogations au paragraphe 1 prévues aux paragraphes 4 et 5 sont notifiées à la Commission.

7. Les Etats membres déterminent les conditions dans lesquelles un numéro national d'identification ou tout autre identifiant de portée générale peut faire l'objet d'un traitement.

Article 9 - Traitements de données à caractère personnel et liberté d'expression

Les Etats membres prévoient pour les traitements de données à caractère personnel effectués aux seules fins de journalisme ou d'expression artistique ou littéraire, des exemptions et dérogations au présent chapitre, au chapitre IV et au chapitre VI dans la seule mesure où elles s'avèrent nécessaires pour concilier le droit à la vie

privée avec les règles régissant la liberté d'expression.

SECTION IV - INFORMATION DE LA PERSONNE CONCERNEE

Article 10 - Information en cas de collecte de données auprès de la personne concernée

Les Etats membres prévoient que le responsable du traitement ou son représentant doit fournir à la personne auprès de laquelle il collecte des données la concernant, au moins les informations énumérées ci-dessous, sauf si la personne en est déjà informée :

a) l'identité du responsable du traitement et, le cas échéant, de son représentant ;

b) les finalités du traitement auquel les données sont destinées ;

c) toute information supplémentaire telle que:

- les destinataires ou les catégories de destinataires des données ;-

- le fait de savoir si la réponse aux questions est obligatoire ou facultative ainsi que les conséquences éventuelles d'un défaut de réponse ;

- l'existence de droits d'accès aux données la concernant et de rectification de ces données, dans la mesure où, compte tenu des circonstances particulières dans lesquelles les données sont collectées, ces informations supplémentaires sont nécessaires pour assurer à l'égard de la personne concernée un traitement loyal des données.

Article 11 - Informations lorsque les données n'ont pas été collectées auprès de la personne concernée

1. Lorsque les données n'ont pas été collectées auprès de la personne concernée, les Etats membres prévoient que le responsable du traitement ou son représentant doit, dès l'enregistrement des données ou, si une communication de données à un tiers est envisagée, au plus tard lors de la première communication de données, fournir à la personne concernée au moins les informations énumérées ci-dessous, sauf si la personne en est déjà informée :

a) l'identité du responsable du traitement, et le cas échéant de son représentant ;

b) les finalités du traitement ;

c) toute information supplémentaire telle que:

- les catégories de données concernées ;

- les destinataires ou les catégories de destinataires des données ;

- l'existence d'un droit d'accès aux données la concernant et de rectification de ces données, dans la mesure où, compte tenu des circonstances particulières dans lesquelles les données sont collectées, ces informations supplémentaires sont nécessaires pour assurer à l'égard de la personne concernée un traitement loyal des données.

2. Le paragraphe 1 ne s'appliquent pas lorsque, en particulier pour un traitement à finalité statistique ou de recherche historique ou scientifique, l'information de la personne concernée se révèle impossible ou implique des efforts disproportionnés, ou si la législation prévoit expressément l'enregistrement ou la communication des

données. Dans ces cas, les Etats membres prévoient des garanties appropriées.

SECTION V: DROIT D'ACCES DE LA PERSONNE CONCERNEE AUX DONNEES

Article 12 - Droit d'accès

Les Etats membres garantissent à toute personne concernée le droit d'obtenir du responsable du traitement :

a) sans contrainte, à des intervalles raisonnables et sans délai ou frais excessifs:

- la confirmation que des données la concernant sont ou ne sont pas traitées, ainsi que des information portant au moins sur les finalités du traitement, les catégories de données sur lesquelles il porte et les destinataires ou les catégories de destinataires auxquels les données sont communiquées ;

- la communication sous une forme intelligible, des données faisant l'objet des traitements, ainsi que de toute information disponible sur l'origine des données ;

- la connaissance de la logique qui sous-tend tout traitement automatisé des données la concernant, au moins dans le cas des décisions automatisées visées à l'article 15 paragraphe 1 ;

b) selon le cas, la rectification, l'effacement ou le verrouillage des données dont le traitement n'est pas conforme à la présente directive, notamment en raison du caractère incomplet ou inexact des données ;

c) la notification aux tiers auxquels les données ont été communiquées de toute rectification, tout effacement ou tout verrouillage effectué conformément au point b), si cela ne s'avère pas impossible ou ne suppose pas un effort disproportionné.

SECTION VI - EXCEPTIONS ET LIMITATIONS

Article 13 - Exceptions et limitations

1. Les Etats membres peuvent prendre des mesures législatives visant à limiter la portée des obligations et des droits prévus à l'article 6 paragraphe 1, à l'article 10, à l'article 11 paragraphe 1 et aux articles 12 et 21, lorsqu'une telle limitation constitue une mesure nécessaire pour sauvegarder:

a) la sûreté de l'Etat ;

b) la défense ;

c) la sécurité publique ;

d) la prévention, la recherche, la détection et la poursuite d'infractions pénales ou de manquements à la déontologie dans le cas des professions réglementées ;

e) un intérêt économique et financier important d'un Etat membre ou de l'Union européenne, y compris dans les domaines monétaire, budgétaire et fiscal ;

f) une mission de contrôle, d'inspection ou de réglementation relevant, même à titre occasionnel, de l'exercice de l'autorité publique, dans les cas visés aux points c), d) et e) ;

g) la protection de la personne concernée et des droits et libertés d'autrui.

2. Sous réserve de garanties légales appropriées, excluant notamment que les données puissent être utilisées aux fins de mesures ou de décisions se rapportant à des personnes précises, les Etats membres peuvent, dans le cas où il n'existe manifestement aucun risque d'atteinte à la vie privée de la personne concernée, limiter par une mesure législative les droits prévus à l'article 12 lorsque les données sont traitées exclusivement aux fins de la recherche scientifique ou sont stockées sous la forme de données à caractère personnel pendant une durée n'excédant pas celle nécessaire à la seule finalité d'établissement de statistiques.

SECTION VII : DROIT D'OPPOSITION DE LA PERSONNE CONCERNEE

Article 14 - Droit d'opposition de la personne concernée

Les Etats membres reconnaissent à la personne concernée le droit:

a) au moins dans les cas visés à l'article 7 points e) et f), de s'opposer à tout moment, pour des raisons prépondérantes et légitimes tenant à sa situation particulière, à ce que des données la concernant fassent l'objet d'un traitement, sauf en cas de disposition contraire du droit national. En cas d'opposition justifiée, le traitement mis en oeuvre par le responsable du traitement ne peut plus porter sur ces données ;

b) de s'opposer, sur demande et gratuitement, au traitement des données à caractère personnel la concernant envisagé par le responsable du traitement à des fins de prospection; ou d'être informée avant que des données à caractère personnel ne soient pour la première fois communiquées à des tiers ou utilisées pour le compte de tiers à des fins de prospection et de se voir expressément offrir le droit de s'opposer, gratuitement, à ladite communication ou utilisation.

Les Etats membres prennent les mesures nécessaires pour garantir que les personnes concernées ont connaissance de l'existence du droit visé au point b) premier alinéa.

Article 15 - Décisions individuelles automatisées

1. Les Etats membres reconnaissent à toute personne le droit de ne pas être soumise à une décision produisant des effets juridiques à son égard ou l'affectant de manière significative, prise sur le seul fondement d'un traitement automatisé de données destiné à évaluer certains aspects de sa personnalité, tels que son rendement

professionnel, son crédit, sa fiabilité, son comportement, etc.

2. Les Etats membres prévoient, sous réserve des autres dispositions de la présente directive, qu'une personne peut être soumise à une décision telle que celle visée au paragraphe 1 si une telle décision :

a) est prise dans le cadre de la conclusion ou de l'exécution d'un contrat, à condition que la demande de conclusion ou d'exécution du contrat, introduite par la personne concernée, ait été satisfaite ou que des mesures appropriées, telles que la possibilité de faire valoir son point de vue, garantissent la sauvegarde de son intérêt légitime ou ;

b) est autorisée par une loi qui précise les mesures garantissant la sauvegarde de l'intérêt légitime de la personne concernée.

SECTION VIII : CONFIDENTIALITE ET SECURITE DES TRAITEMENTS

Article 16 - Confidentialité des traitements

Toute personne agissant sous l'autorité du responsable du traitement ou de celle du sous-traitant, ainsi que le sous-traitant lui-même, qui accède à des données à caractère personnel, ne peut les traiter que sur instruction du responsable du traitement, sauf en vertu d'obligations légales.

Article 17 - Sécurité des traitements

1. Les Etats membres prévoient que le responsable du traitement doit mettre en oeuvre les mesures techniques et d'organisation appropriées pour protéger les données à caractère personnel contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisés, notamment lorsque le traitement comporte des transmissions de données dans un réseau, ainsi que contre toute autre forme de traitement illicite. Ces mesures doivent assurer, compte tenu de l'état de l'art et des coûts liés à leur mise en oeuvre, un niveau de sécurité approprié au regard des risques présentés par le traitement et de la nature des données à protéger.

2. Les Etats membres prévoient que le responsable du traitement, lorsque le traitement est effectué pour son compte, doit choisir un sous-traitant qui apporte des garanties suffisantes au regard des mesures de sécurité technique et d'organisation relatives aux traitements à effectuer et qu'il doit veiller au respect de ces mesures.

3. La réalisation de traitements en sous-traitance doit être régie par un contrat ou un acte juridique qui lie le sous-traitant au responsable du traitement et qui prévoit notamment que :

- le sous-traitant n'agit que sur la seule instruction du responsable du traitement ;

- les obligations visées au paragraphe 1, telles que définies par la législation de l'Etat membre dans lequel le sous-traitant est établi, incombent également à celui-ci.

4. Aux fins de la conservation des preuves, les éléments du contrat ou de l'acte juridique relatifs à la protection des données et les exigences portant sur les mesures visées au paragraphe 1 sont consignées par écrit ou sous une autre forme équivalente.

SECTION IX : NOTIFICATION

Article 18 - Obligation de notification à l'autorité de contrôle

1. Les Etats membres prévoient que le responsable du traitement, ou le cas échéant, son représentant, doit adresser une notification à l'autorité de contrôle visée à l'article 28 préalablement à la mise en oeuvre d'un traitement entièrement ou partiellement automatisé ou d'un ensemble de tels traitements ayant une même finalité ou des finalités liées.

2. Les Etats membres ne peuvent prévoir de simplification de la notification ou de dérogation à cette obligation que dans les cas et aux conditions suivants :

- lorsque, pour les catégories de traitement qui, compte tenu des données à traiter, ne sont pas susceptibles de porter atteinte aux droits et libertés des personnes concernées, ils précisent les finalités des traitements, les données ou catégories de données traitées, la ou les

catégories de personnes concernées, les destinataires ou catégories de destinataires auxquels les données sont communiquées et la durée de conservation des données et/ou ;

- lorsque le responsable du traitement désigne, conformément au droit national auquel il est soumis, 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, contenant les informations visées à l'article 21 paragraphe 2, et garantissant de la sorte que les traitements ne sont pas susceptibles de porter atteinte faux droits et libertés des personnes concernées.

3. Les Etats membres peuvent prévoir que le paragraphe 1 ne s'applique pas aux traitements ayant pour seul objet la tenue d'un registre qui, en vertu de dispositions législatives ou réglementaires, est destiné à l'information du public et est ouvert à la consultation du public ou de toute personne justifiant d'un intérêt légitime.

4. Les Etats membres peuvent prévoir une dérogation à l'obligation de notification ou une simplification de la notification pour les traitements visés à l'article 8 paragraphe 2 point d).

5. Les Etats membres peuvent prévoir que les traitements non autorisés de données à caractère personnel, ou certains d'entre eux, font l'objet d'une notification, éventuellement simplifiée.

Article 19 - Contenu de la notification

1. Les Etats membres précisent les informations qui doivent figurer dans la notification. Elles comprennent au minimum:

a) le nom et l'adresse du responsable du traitement et, le cas échéant, de son représentant ;

b) la ou les finalités du traitement ;

c) une description de la ou des catégories de personnes concernées et des données ou des catégories de données s'y rapportant ;

d) les destinataires ou les catégories de destinataires auxquels les données sont susceptibles d'être communiquées ;

e) les transferts de données envisagés à destination de pays tiers ;

f) une description générale permettant d'apprécier de façon préliminaire le caractère approprié des mesures prises pour assurer la sécurité du traitement en application de l'article 17.

2. Les Etats membres précisent les modalités de notification à l'autorité de contrôle des changements affectant les informations visées au paragraphe 1.

Article 20 Contrôles préalables

1. Les Etats membres précisent les traitements susceptibles de présenter des risques particuliers au regard des droits et libertés des personnes concernées et veillent à ce que ces traitements soient examinés avant leur mise en oeuvre.

2. De tels examens préalables sont effectués par l'autorité de contrôle après réception de la notification du responsable du traitement ou par le détaché à la protection des données, qui, en cas de doute, doit consulter l'autorité de contrôle.

3. Les Etats membres peuvent aussi procéder à un tel examen dans le cadre de l'élaboration soit d'une mesure du Parlement national, soit d'une mesure fondée sur une telle mesure législative, qui définisse la nature du traitement et fixe des garanties appropriées.

Article 21 - Publicité des traitements

1. Les Etats membres prennent des mesures pour assurer la publicité des traitements.

2. Les Etats membres prévoient que l'autorité de contrôle tient un registre des traitements notifiés en vertu de l'article 18. Le registre contient au minimum les informations énumérées à l'article 19 paragraphe 1 points a) à e).

Le registre peut être consulté par toute personne.

3. En ce qui concerne les traitements non soumis à notification, les Etats membres prévoient que le responsable du traitement ou une autre instance qu'ils désignent communique sous une forme appropriée à toute personne qui en fait la demande au moins les informations visées à l'article 19 paragraphe 1 points a) à e).

Les Etats membres peuvent prévoir que la présente disposition ne s'applique pas aux traitements ayant pour seul objet la tenue d'un registre qui, en vertu de dispositions législatives ou réglementaires, est destiné à l'information du public et est ouvert à la consultation du public ou de toute personne justifiant d'un intérêt égitime.

[....]

CHAPITRE IV - TRANSFERT DE DONNEES A CARACTERE PERSONNEL VERS DES PAYS TIERS

Article 25 - Principes

1. Les Etats membres prévoient que le transfert vers un pays tiers de données à caractère personnel faisant l'objet d'un traitement, ou destinées à faire l'objet d'un traitement après leur transfert, ne peut avoir lieu que si, sous réserve du respect des dispositions nationales prises en application des autres dispositions de la présente directive, le pays tiers en question assure un niveau de protection adéquat.

2. Le caractère adéquat du niveau de protection offert par un pays tiers s'apprécie au regard de toutes les circonstances relatives à un transfert ou à une catégorie de transferts de données; en particulier, sont prises en considération la nature des données, la finalité et la durée du ou des traitements envisagés, les pays d'origine et de destination finale, les règles de droit, générales ou sectorielles, en vigueur dans le pays tiers en cause, ainsi que les règles professionnelles et les mesures de sécurité qui y sont respectées.

3. Les Etats membres et la Commission s'informent mutuellement des cas dans lesquels ils estiment qu'un pays tiers n'assure pas un niveau de protection adéquat au sens du paragraphe 2.

4. Lorsque la Commission constate, conformément à la procédure prévue à l'article 31 paragraphe 2, qu'un pays tiers n'assure pas un niveau de protection adéquat au sens du paragraphe 2 du présent article, les Etats membres prennent les mesures nécessaires en vue d'empêcher tout transfert de même nature vers le pays tiers en cause.

5. La Commission engage, au moment opportun, des négociations en vue de remédier à la situation résultant de la constatation faite en application du paragraphe 4.

6. La Commission peut constater, conformément à la procédure prévue à l'article 31 paragraphe 2, qu'un pays

tiers assure un niveau de protection adéquat au sens du paragraphe 2 du présent article, en raison de sa législation interne ou de ses engagements internationaux, souscrits notamment à l'issue des négociations visées au paragraphe 5, en vue de la protection de la vie privée et des libertés et droits fondamentaux des personnes.

Les Etats membres prennent les mesures nécessaires pour se conformer à la décision de la Commission.

Article 26 - Dérogations

1. Par dérogations à l'article 25 et sous réserve de dispositions contraires de leur droit national régissant des cas particuliers, les Etats membres prévoient qu'un transfert de données à caractère personnel vers un pays tiers n'assurant pas un niveau de protection adéquat au sens de l'article 25 paragraphe 2, peut être effectué, à condition que:

a) la personne concernée ait indubitablement donné son consentement au transfert envisagé ou ;

b) le transfert soit nécessaire à l'exécution d'un contrat entre la personne concernée et le responsable du traitement ou à l'exécution de mesures précontractuelles prises à la demande de la personne concernée ou ;

c) le transfert soit nécessaire à la conclusion ou à l'exécution d'un contrat conclu ou à conclure, dans l'intérêt de la personne concernée, entre le responsable du traitement et un tiers ou ;

d) le transfert soit nécessaire ou rendu juridiquement obligatoire pour la sauvegarde d'un intérêt public important, ou pour la constatation, l'exercice ou la défense d'un droit en justice ou ;

e) le transfert soit nécessaire à la sauvegarde de l'intérêt vital de la personne concernée ou ;

f) le transfert intervienne au départ d'un registre public qui, en vertu de dispositions législatives ou réglementaires, est destiné à l'information du public et est ouvert à la consultation du public ou de toute personne justifiant d'un intérêt légitime, dans la mesure où les conditions légales pour la consultation sont remplies dans le cas particulier.

2. Sans préjudice du paragraphe 1, un Etat membre peut autoriser un transfert, ou un ensemble de transferts, de données à caractère personnel vers un pays tiers n'assurant pas un niveau de protection adéquat au sens de l'article 25 paragraphe 2, lorsque le responsable du traitement offre des garanties suffisantes au regard de la protection de la vie privée et des libertés et droits fondamentaux des personnes, ainsi qu'à l'égard de l'exercice des droits correspondants ; ces garanties peuvent notamment résulter de clauses contractuelles appropriées.

3. L'Etat membre informe la Commission et les autres Etats membres des autorisations qu'il accorde en application du paragraphe 2. En cas d'opposition exprimée par un autre Etat membre ou par la Commission et dûment justifiée au regard de la protection de la vie privée et des libertés et droits fondamentaux des personnes, la Commission arrête les mesures appropriées, conformément à la procédure prévue à l'article 31 paragraphe 2.

Les Etats membres prennent les mesures nécessaires pour se conformer à la décision de la Commission.

4. Lorsque la Commission décide, conformément à la procédure prévue à l'article 31 paragraphe 2, que certaines clauses contractuelles types présentent les garanties suffisantes visées au paragraphe 2, les Etats membres prennent les mesures nécessaires pour se conformer à la décision de la Commission.

[....]

Loi sur la cryptographie (Article 28 de la loi du 29 décembre 1990, modifiée par la loi n° 91-648 du 11 juillet 1991 et la loi n° 96-659 du 26 juillet 1996)

I- On entend par prestations de cryptologie toutes prestations visant à transformer à l'aide de conventions secrètes des informations ou signaux clairs en information ou signaux inintelligibles pour des tiers, ou à réaliser l'opération inverse, grâce à des moyens, matériels ou logiciels conçus à cet effet. On entend par moyen de cryptologie tout matériel ou logiciel conçu ou modifié dans le même objectif.

Pour préserver les intérêts de la défense nationale et de la sécurité intérieure ou extérieure de l'Etat, tout en permettant la protection des informations et le développement des communications et des transactions sécurisées :

1°) L'utilisation d'un moyen ou d'une prestation de cryptologie est :

a) Libre :

- si le moyen ou la prestation de cryptologie ne permet pas d'assurer des fonctions de confidentialité, notamment lorsqu'il ne peut avoir comme objet que d'authentifier une communication ou d'assurer l'intégrité du message transmis,

- ou si le moyen ou la prestation assure des fonctions de confidentialité et n'utilise que des conventions secrètes gérées selon les procédures et par un organisme agréés dans les conditions définies au II ;

b) Soumise à autorisation du Premier ministre dans les autres cas.

2°) La fourniture, l'importation de pays n'appartenant pas à la Communauté européenne et l'exportation tant d'un moyen que d'une prestation de cryptologie :

a) sont soumises à autorisation préalable du Premier ministre lorsqu'ils assurent des fonctions de confidentialité ; l'autorisation peut être subordonnée à l'obligation pour le fournisseur de communiquer l'identité de l'acquéreur ;

b) Sont soumises à la déclaration auprès du Premier ministre dans les autres cas.

3°) Un décret fixe les conditions dans lesquelles sont souscrites les déclarations et accordées les autorisations. Ce décret prévoit :

a) Un régime simplifié de déclaration ou d'autorisation pour certains types de moyens ou de prestations ou pour certaines catégories d'utilisateurs ;

b) La substitution de la déclaration à l'autorisation pour les opérations portant sur des moyens ou des prestations de cryptologie, dont les caractéristiques techniques ou les conditions d'utilisation, tout en justifiant, au regard des intérêts susmentionnés, un suivi particulier, n'exigent pas l'autorisation préalable de ces opérations ;

c) La dispense de toute formalité préalable pour les opérations portant sur des moyens ou des prestations de

cryptologie, dont les caractéristiques techniques ou les conditions d'utilisation sont telles que ces opérations ne sont pas susceptibles de porter atteinte aux intérêts mentionnés au deuxième alinéa.

d) Les délais de réponse aux demandes d'autorisation.

II. - Les organismes chargés de gérer pour le compte d'autrui les conventions secrètes de moyens ou prestations de cryptologie permettant d'assurer des fonctions de confidentialité doivent être préalablement agréés par le Premier ministre.

Ils sont assujettis au secret professionnel dans l'exercice de leurs activités agréées.

L'agrément précise les moyens ou prestations qu'ils peuvent utiliser ou fournir.

Ils sont tenus de conserver les conventions secrètes qu'ils gèrent. Dans le cadre de l'application de la loi n°91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications ainsi que dans le cadre des enquêtes menées au titre des chapitres premier et II du titre II du livre premier du code de procédure pénale, ils doivent les remettre aux autorités judiciaires ou aux autorités habilitées, ou les mettre en oeuvre selon leur demande.

Lorsque ces organismes remettent les convention secrètes qu'ils gèrent dans le cadre des enquêtes menées au titre des chapitres premier et II du titre II du livre premier du code de procédure pénale, suite aux réquisitions du procureur de la République, ils informent les utilisateurs de cette remise.

Ils doivent exercer leurs activités agréées sur le territoire national.

Un décret en Conseil d'Etat fixe les conditions dans lesquelles ces organismes sont agréés ainsi que les garanties auxquelles est subordonné l'agrément ; il précise les procédures et les dispositions techniques permettant la mise en oeuvre des obligations indiquées ci-dessus.

III. - a) Sans préjudice de l'application du code des douanes, le fait de fournir, d'importer de pays n'appartenant pas à la Communauté européenne ou d'exporter un moyen ou une prestation de cryptologie sans avoir obtenu l'autorisation préalable mentionnée au I ou en dehors des conditions de l'autorisation délivrée est puni de six mois d'emprisonnement et de 200 000 F d'amende.

Le fait de gérer, pour le compte d'autrui, des conventions secrètes de moyens ou de prestations de cryptologie permettant d'assurer des fonctions de confidentialité sans avoir obtenu l'agrément mentionné au II ou en dehors des conditions de cet agrément est puni de deux ans d'emprisonnement et de 300 000 F d'amende.

Le fait de fournir, d'importer de pays n'appartenant pas à la Communauté Européenne, d'exporter ou d'utiliser un moyen ou une prestation de cryptologie en vue de faciliter la préparation ou la commission d'un crime ou d'un délit est puni de trois ans d'emprisonnement et de 500 000 F d'amende.

La tentative des infractions prévues aux alinéas précédents est punie des mêmes peines.

b) Les personnes physiques coupables des infractions prévues au a) encourent les peines complémentaires prévues aux articles 131-19, 131-21 et 131-27 et, à titre définitif ou pour une durée de cinq ans au plus, les peines prévues aux articles 131-33 et 131-34 du code pénal.

IV- Outre les officiers et agents de police judiciaire agissant conformément au Code de procédure pénale et, dans leur domaine de compétence, les agents des douanes agissant conformément au Code des douanes, les agents habilités à cet effet par le Premier ministre et assermentés dans des conditions fixées par décret en Conseil d'Etat peuvent rechercher et constater par procès-verbal les infractions aux dispositions du présent article et des textes pris pour son application. Les agents habilités par le Premier ministre visés à l'alinéa précédent peuvent accéder aux locaux, terrains ou moyens de transport à usage professionnel, en vue de rechercher et de constater les infractions, demander la communication de tous documents professionnels et en prendre copie, recueillir, sur convocation ou sur place, les renseignements et justifications. Les agents ne peuvent accéder à ces locaux que pendant leurs heures d'ouverture lorsqu'ils sont ouverts au public, et dans les autres cas, qu'entre 8 heures et 20 heures. Ils ne peuvent accéder aux locaux qui servent pour partie de domicile aux intéressés.

Le procureur de la république est préalablement informé des opérations envisagées en vue de la recherche des infractions, par les agents visés au deuxième alinéa. Il peut s'opposer à ces opérations. Les procès-verbaux lui sont transmis dans les cinq jours suivant leur établissement. Une copie en est également remise à l'intéressé.

Les agents habilités par le Premier ministre visé au deuxième alinéa peuvent, dans les mêmes lieux et les mêmes temps que ceux visés au même alinéa du présent paragraphe, procéder à la saisie des matériels visés au paragraphe I sur autorisation judiciaire donnée par ordonnance du président du tribunal de grande instance dans le ressort duquel sont situés les matériels, ou d'un juge délégué par lui.

La demande doit comporter tous les éléments d'information de nature à justifier la saisie. Celle-ci s'effectue sous le l'autorité et le contrôle du juge qui l'a autorisée.

Les matériels saisis sont immédiatement inventoriés. L'inventaire est annexé au procès-verbal dressé sur les lieux. Les originaux du procès-verbal et de l'inventaire sont transmis, dans les cinq jours suivant leur établissement, au juge qui a ordonné la saisie.

Le président du tribunal de grande instance ou le juge délégué par lui pourra d'office à tout moment ou sur la demande de l'intéressé ordonner mainlevée de la saisie.

Est puni d'un emprisonnement de six mois et d'une amende de 200 000 F le fait de refuser de fournir les informations ou documents ou de faire obstacle au déroulement des enquêtes mentionnées au présent paragraphe.

V- Les autorisations et déclarations de fourniture, d'exportation ou d'utilisation de moyens ou de prestations de cryptologie délivrés avant la date de publication de la présente loi conservent leurs effets jusqu'à l'expiration du terme prévu.

VI. - Les dispositions du présent article ne font pas obstacle à l'application du décret du 18 avril 1939 fixant le régime des matériels de guerre, armes et munitions, à ceux des moyens de cryptologie qui sont spécialement conçus ou modifiés pour permettre ou faciliter l'utilisation ou la mise en oeuvre des armes.

VII. - Le présent article est applicable aux territoires d'outre-mer et à la collectivité territoriale de Mayotte.

Extraits du Code de la Consommation (livre premier : information des consommateurs et formation des contrats)

Obligation générale d'information

Article L 111-1

Tout professionnel vendeur de biens ou prestataire de services doit, avant la conclusion du contrat, mettre le consommateur en mesure de connaître les caractéristiques essentielles du bien ou du service.

Article L 111-2

Le professionnel vendeur de biens meubles doit, en outre, indiquer au consommateur la période pendant laquelle il est prévisible que les pièces indispensables à l'utilisation du bien seront disponibles sur le marché. Cette période est obligatoirement portée à la connaissance du professionnel par le fabricant ou l'importateur.

Article L 111-3

Les dispositions des deux articles précédents s'appliquent sans préjudice des dispositions plus favorables aux consommateurs qui soumettent certaines activités à des règles particulières en ce qui concerne l'information du consommateur.

Prix et conditions de vente

Article L 113-3

Tout vendeur de produit ou tout prestataire de services doit par voie de marquage, d'étiquetage, d'affichage ou par tout autre procédé approprié, informer le consommateur sur les prix, les limitations éventuelles de la responsabilité contractuelle et les conditions particulières de la vente, selon des modalités fixées par arrêtés du ministre chargé de l'économie, après consultation du Conseil national de la consommation.

Cette disposition s'applique à toutes les activités visées au dernier alinéa de l'article L 113-2.

Information sur les délais de livraison

Article L 114-1

Dans tout contrat ayant pour objet la vente d'un bien meuble ou la fourniture d'une prestation de services à un consommateur, le professionnel doit, lorsque la livraison du bien ou la fourniture de la prestation n'est pas immédiate et si le prix convenu excède des seuils fixés par voie réglementaire, indiquer la date limite à laquelle il s'engage à livrer le bien ou à exécuter la prestation.

Le consommateur peut dénoncer le contrat de vente d'un bien meuble ou de fourniture d'une prestation de services par lettre recommandée avec demande d'avis de réception en cas de dépassement de la date de livraison du bien ou d'exécution de la prestation excédant sept jours et non dû à un cas de force majeure.

Ce contrat est, le cas échéant, considéré comme rompu à la réception, par le vendeur ou par le prestataire de services, de la lettre par laquelle le consommateur l'informe de sa décision, si la livraison n'est pas intervenue ou si la prestation n'a pas été exécutée entre l'envoi et la réception de cette lettre. Le consommateur exerce ce droit dans un délai de soixante jours ouvrés à compter de la date indiquée pour la livraison du bien ou l'exécution de la prestation.

Sauf stipulation contraire du contrat, les sommes versées d'avance sont des arrhes, ce qui a pour effet que chacun des contractants peut revenir sur son engagement, le consommateur en perdant les arrhes, le professionnel en les restituant au double.

[....]

Publicité

Article L 121-1

Est interdite toute publicité comportant, sous quelque forme que ce soit des allégations, indications ou présentations fausses ou de nature à induire en erreur, lorsque celles-ci portent sur un ou plusieurs des éléments ci-après: existence, nature, composition, qualités substantielles, teneur en principes utiles, espèce, origine, quantité, mode et date de fabrication, propriétés, prix et conditions de vente de biens ou services qui font l'objet de la publicité, conditions de leur utilisation, résultats qui peuvent être attendus de leur utilisation, motifs ou procédés de la vente ou de la prestation de services, portée des engagements pris par l'annonceur, identité, qualités ou aptitudes du fabricant, des revendeurs, des promoteurs ou des prestataires.

Article L 121-2

Les agents de la direction générale de la concurrence, de la consommation et de la répression des fraudes, ceux de la direction générale de l'alimentation du ministère de l'agriculture et ceux du service de métrologie au ministère de l'industrie, sont habilités a constater, au moyen de procès-verbaux, les infractions aux dispositions de l'article L 121-1. Ils peuvent exiger de l'annonceur la mise à leur disposition de tous les éléments propres à justifier les allégations, indications ou présentations publicitaires. Ils peuvent également exiger de l'annonceur, de l'agence de publicité ou du responsable du support la mise à leur disposition des messages publicitaires diffusés.

Les procès-verbaux dressés en application du présent article sont transmis au procureur de la République.-

[....]

Article L 121-5

L'annonceur, pour le compte duquel la publicité est diffusée, est responsable, à titre principal, de l'infraction commise. Si le contrevenant est une personne morale, la responsabilité incombe à ses dirigeants. La complicité est punissable dans les conditions de droit commun.

Le délit est constitué dès lors que la publicité est faite, reçue ou perçue en France.

[....]

Article L 121-8

La publicité qui met en comparaison des biens ou services en utilisant soit la citation ou la représentation de la marque de fabrique, de commerce ou de service d'autrui, soit la citation ou la représentation de la raison sociale ou de la dénomination sociale, du nom commercial ou de l'enseigne d'autrui n'est autorisée que si elle est loyale, véridique et qu'elle n'est pas de nature à induire en erreur le consommateur. Elle doit être limitée à une comparaison objective qui ne peut porter que sur des caractéristiques essentielles, significatives, pertinentes et vérifiables de biens ou services de même nature et disponibles sur le marché. Lorsque la comparaison porte sur les prix, elle doit concerner des produits identiques vendus dans les mêmes conditions et indiquer la durée pendant laquelle sont maintenus les prix mentionnés comme siens par l'annonceur. La publicité comparative ne peut pas s'appuyer sur des opinions ou des appréciations individuelles ou collectives.

Article L 121-9

Aucune comparaison ne peut avoir pour objet principal de tirer avantage de la notoriété attachée à une marque. Aucune comparaison ne peut présenter des produits ou des services comme l'imitation ou la réplique de produits ou services revêtus d'une marque préalablement déposée.

Article L 121-10

Pour les produits qui bénéficient d'une appellation d'origine contrôlée, la comparaison n'est autorisée que si elle porte sur des produits bénéficiant chacun de la même appellation.

Article L 121-11

Il est interdit de faire figurer des annonces comparatives telles que définies aux articles L 121-8 et L 121-9 sur des emballages, des factures, des titres de transport, des moyens de paiement ou des billets d'accès à des spectacles ou à des lieux ouverts au public.

Article L 121-12

L'annonceur pour le compte duquel la publicité définie aux articles L 121-8 et L 121-9 est diffusée doit être en mesure de prouver l'exactitude de ses allégations, indications ou présentations. Avant toute diffusion, il communique l'annonce comparative aux professionnels visés, dans un délai au moins égal à celui exigé, selon le type de support retenu, pour l'annulation d'un ordre de publicité.

Article L 121-13

Les insertions réalisées dans la presse pour une publicité définie aux articles L 121-8 et L 121-9 ne donnent pas lieu à l'application de l'article 13 de la loi du 29 juillet 1881 sur la liberté de la presse et de l'article 6 de la loi n° 82-652 du 29 juillet 1982 sur la communication audiovisuelle (droit de réponse).

[....]

Ventes à distance

Article L 121-16

Pour toutes les opérations de vente à distance, l'acheteur d'un produit dispose d'un délai de sept jours francs à compter de la livraison de sa commande pour faire retour de ce produit au vendeur pour échange ou remboursement, sans pénalités à l'exception des frais de retour.

Si ce délai expire normalement un samedi, un dimanche ou un jour férié ou chômé, il est prorogé jusqu'au premier jour ouvrable suivant.

Article L 121-17

Les règles relatives à la responsabilité du dirigeant de droit ou de fait d'un service de radiodiffusion sonore ou de télévision sont définies par le II de l'article 3 de la loi n° 88-21 du 6 janvier 1988 relative aux opérations de télé-promotion avec offre de vente dites de "télé-achat" reproduit ci après:

"II: Le dirigeant de droit ou de fait d'un service de radiodiffusion sonore ou de télévision défini à l'article 2 de la présente loi qui aura programmé et fait diffuser ou distribuer une émission en violation des règles fixées en vertu du même article sera puni d'une amende de 6 000 F à 500 000 F.

Dans le cas de récidive, l'auteur de l'infraction pourra être puni d'une amende de 100 000 F à 1 000 000 F."

Article L 121-18

Dans toute offre de vente d'un bien ou de fourniture d'une prestation de services qui est faite à distance à un consommateur, le professionnel est tenu d'indiquer le nom de son entreprise, ses coordonnées téléphoniques ainsi que l'adresse de son siège et, si elle est différente, celle de l'établissement responsable de l'offre.

Article L 121-19

Les infractions aux dispositions de l'article L 121-18, ainsi que le refus du vendeur de changer ou de rembourser un produit retourné par l'acheteur dans les conditions visées à l'article L 121-16 son constatés et poursuivis conformément aux dispositions du titre VI de l'ordonnance n° 86-1243 du Ier décembre 1986 relative à la liberté des prix et de la concurrence.

Article L 121-20

Les règles relatives à la fixation des règles de programmation des émissions sont définies par l'article 2 de la loi du n° 88-21 du 6 janvier 1988 précitée reproduit ci après:

"Art. 2: Le Conseil supérieur de l'audiovisuel fixe les règles de programmation des émissions consacrées en tout ou partie à la présentation ou à la promotion d'objets, de produits ou de services offerts directement à la vente par des services de radiodiffusion sonore et de télévision autorisés en vertu de la loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication."

[....]

Extraits de la décision rendue dans l'affaire Yves Rocher c/ BNP et BANEXI, TGI Paris, ordonnance de référé, 16 avril 1996

BANQUE NATIONALE DE PARIS dite BNP, BANQUE POUR L'EXPANSION INDUSTRIELLE dite BANEXI, Monsieur Michel BOUISSOU c/ Monsieur Yves ROCHER

[....]

A la suite de l'acquisition en 1988 par la société Laboratoires de Biologie Végétale Yves Rocher de la majorité des titres de la société Petit Bateau Valton (PBV), une polémique s'est engagée entre Yves Rocher et le groupe BNP-Banexi, titulaire d'une partie du capital de l'entreprise dont les titres ont été cédés, au sujet de la situation financière de cette entreprise à l'époque de la cession;

[....]

Au mois de février et mars 1996 ont été diffusées, notamment auprès de nombreux chefs d'entreprises, des brochures, intitulées par les demandeurs « libellés n° 1 et 2 », exposant les griefs d'Yves Rocher à l'encontre du groupe BNP- Banexi ;

Les mêmes informations ont fait l'objet d'une reproduction sur le réseau informatique Internet ;

Des plaintes avec constitution de partie civile ont été déposées par le groupe BNP-Banexi entre les mains du doyen des juges d'instruction du Tribunal de Grande Instance de Troyes les 4 et 25 mars 1996, lesdites plaintes visant les imputations contenues dans les fascicules diffusés par Yves Rocher ;

Par l'assignation introductive de la présente instance, signifiée le 28 mars 1996, les requérants nous deman-

dent, sur le fondement des articles 491, 808 et 809 du Nouveau Code de procédure civile :

- de dire qu'Yves Rocher sera tenu, dans un délai de 24 heures à compter de la signification de l'ordonnance à intervenir et sous astreinte de 1 000 000 francs par jour de retard, de prendre toutes dispositions pour faire disparaître du réseau Internet toute mention du texte de ses « libellés n°1 et 2 » des mois de février et mars 1996, comme celle de tout texte en résumant la teneur ;

- d'interdire au défendeur le renouvellement, par quelque vois publique que ce soit, de l'une quelconque des allégations contenues dans ces libellés, sous astreinte de 10 000 000 francs par infraction constatée ;

- d'ordonner la publication sur le réseau Internet et dans quinze journaux d'un communiqué faisant état de la condamnation prononcée en référé contre Yves Rocher ;

- de condamner celui-ci à payer à chacun des demandeurs une indemnité de 20 000 francs par application de l'article 700 du Nouveau Code de procédure civile ;

Selon les demandeurs, les mesures sollicitées doivent être prononcées pour empêcher le renouvellement des graves accusations proférées par le défendeur et pour faire cesser le trouble manifestement illicite déjà causé par la campagne de déstabilisation et de dénigrement qu'il a entreprise ;

Yves Rocher conclut à titre principal à notre incompétence au profit du tribunal de grande instance de Vanves, subsidiairement au rejet des demandes ;

Sur la compétence, il fait valoir qu'il est domicilié dans le ressort du tribunal de grande instance de Vannes et que les demandeurs n'expliquent aucunement sur quelle base ils fondent la compétence du tribunal de grande instance de Paris ;

Sur le fond, Yves Rocher soutient, d'une part que les demandes sont impossibles à satisfaire compte tenu des principes de fonctionnement du réseau Internet, d'autre part que ces demandes sont incompatibles avec le droit à la liberté d'expression dont soit jouir tout citoyen, le juge des référés ne devant pas au surplus préjuger de la décision qui sera prise par les juges saisis des actions en diffamation ;

Yves Rocher a néanmoins demandé qu'en tant que de besoin il lui soit donné acte de ce que les « libellés n°1 et 2 » ne feront plus l'objet d'une diffusion publique et ajouté, par note en délibéré, que les messages critiqués par le groupe BNP-Banexi n'étaient plus diffusés sur le réseau Internet ;

SUR LA COMPETENCE

Attendu que les requérants se plaignent de la diffusion publique de propos les mettant en cause, toute juridiction dans le ressort de la quelle les informations incriminées ont été divulguées et reçues est compétente pour statuer sur la demande ;

Attendu qu'il résulte des pièces versées aux débats que les brochures contenant les accusations portées par Yves Rocher contre le groupe BNP-Banexi ont é té diffusées en différents points du territoire national, notamment à Paris, et ont été reproduites sur le réseau Internet, accessible également pour tout intéressé à paris ; qu'à ce titre les requérants étaient en droit de saisir le juge des référés du tribunal de grande instance de cette ville ;

SUR LE BIEN FONDE DE LA DEMANDE

Attendu que les brochures incriminées, qui mentionnent pour celles du mois de mars 1996 Yves Rocher comme directeur de la publication, comportent en première page, sous le titre « rebondissement dans l'affaire Petit Bateau Yves Rocher - BNP », les indications suivantes :

« conséquences d'une expertise judiciaire :

- le tribunal arbitral a été abusé

- le groupe Yves Rocher a été escroqué par le BNP-Banexi. »

Qu'elles relatent ensuite, dans un texte de douze pages, les accusations formulées par Yves Rocher contre le groupe BNP-Banexi à propos des conditions dans lesquelles celui-ci l'aurait déterminé à acquérir les titres de la société PBV [....]

Attendu que ces brochures, manifestement publiées à l'initiative et sous la responsabilité d'Yves Rocher, ont fait l'objet d'une importante diffusion auprès des chefs d'entreprises français, -la presse faisant même état, pour celle du mois de mars 1996, de 500 000 exemplaires mis en circulation sur le territoire national -, et étaient accompagnées d'une lettre de présentation expliquant le souhait d'Yves Rocher de dénoncer « après d'autres scandales (...) celui de la BNP-Banexi » et les agissements de ces requins ; qu'elles ont aussi été reproduites sur le réseau informatique international Internet dans des circonstances auxquelles Yves Rocher ne peut sérieusement prétendre être étranger dès lors que les fascicules du mois de mars 1996 renvoient les lecteurs à ce réseau par l'avertissement suivant publié en page de couverture :

« dans tous les pays du monde on peut consulter ce document sur le réseau Internet et questionner la BNP. », complété par la mention d'une « adresse Internet » permettant d'accéder à ces informations ;

Attendu que, sans préjuger de l'appréciation qui sera faite par les juges du fond des actions engagées par chacune des parties contre l'autre, la publicité tapageuse et réitérée donnée par le défendeur à des propos outranciers, divulguant des informations contenues dans une procédure judiciaire ouverte sur constitution de partie civile et relevant à ce titre de l'interdiction de publication prévue par l'article 2 de la loi du 2 juillet 1931, portant de surcroît sans aucune restriction ou nuance des accusations graves à l'encontre de personnes actuellement étrangères à cette procédure, constitue pour les personnes visées un trouble manifestement illicite qu'elles sont en droit de faire cesser ;

Attendu à cet égard, s'il peut être donné acte à Yves Rocher de ce qu'il s'engage à ne plus procéder à la diffusion publique de ses « libellés n°1 et 2 », il convient aussi, en tant que de besoin, compte tenu des circonstances ci-dessus relevées et en application de l'article 809 alinéa 1er du Nouveau Code de procédure civile, de lui faire injonction de ne plus les diffuser ;

Attendu, quant à la reproduction des documents incriminés sur les écrans du réseau Internet, qu'Yves Rocher a fait valoir par conclusions qu'aucun contrôle de l'accès et de la diffusion des informations sur le réseau ne peut être exercé ;

Attendu cependant que toute personnes ayant pris la responsabilité de faire diffuser publiquement, par quelque mode de communication que ce soit, des propos mettant en cause la réputation d'un tiers doit être au moins en mesure, lorsque comme en l'espèce cette divulgation est constitutive d'un trouble manifestement illicite, de justifier des efforts et démarches accomplies pour faire cesser l'atteinte aux droits d'autrui ou en limiter les effets ;

Attendu qu'Yves Rocher a produit, en cours de délibéré, une lettre du 11 avril 1996 émanant, selon ses dires, d'un « organisme serveur » et indiquant que « les écrans Web concernant l'affaire Petit-Bateau/BNP ont été retirés définitivement du réseau Internet ; qu'il y a lieu

de commettre un huissier-audiencier aux fins de vérification de ces allégations par constat contradictoire, l'huissier désigné recevant également pour mission, aux frais avancés des demandeurs, de constater les éventuelles infractions à l'injonction faite à Yves Rocher de ne plus diffuser les « libelles n° 1 et 2 » ;

[....]

Instruction du 16 février 1996 du SLF et de la DGI relative à la TVA. Régime applicable aux opérations portant sur des logiciels (BOI 3 A-1-96, 26 février 1996)

Les règles de TVA applicables aux logiciels dépendent de la nature du logiciel (standard ou spécifique) et de la nature de la transaction.

1. Cette instruction a pour objet de préciser les règles de TVA applicables aux cessions de logiciels et à certaines autres opérations portant sur les logiciels.

A. LES CESSIONS DE LOGICIELS

2. Le régime de TVA applicable à une cession de logiciel diffère suivant qu'il s'agit d'une livraison de bien meuble corporel ou d'une prestation de services. En effet, de cette qualification découlent notamment les règles de territorialité et d'exigibilité applicables. Elles reposent sur la distinction entre les logiciels « standards » et les logiciels « spécifiques » et sur la nature de la transaction.

I. Définition des logiciels standards et spécifiques

3. Les produits standards sont des articles fabriqués en série qui peuvent être acquis par tous les clients et être utilisés par eux après leur installation et une formation limitée, pour la réalisation des mêmes applications ou fonctions. Ils sont constitués d'un ensemble cohérent de programmation et de matériels d'appui et comportent souvent des services d'installation, de formation et de maintenance. La plupart des logiciels pour micro-ordinateurs, les logiciels pour ordinateur domestique et les logiciels de jeux appartiennent à cette catégorie. Tel est le cas également des logiciels standards adaptés à l'initiative des fournisseurs, par incorporation d'un dispositif de sécurité ou de dispositifs analogues.

Les logiciels qui ne répondent pas à cette définition sont des logiciels spécifiques.

II. Nature de la transaction

4. Les logiciels sont des oeuvres de l'esprit protégées par le Code de la propriété intellectuelle. La reproduction et la mise sur le marché d'un logiciel (nécessaires en particulier à la distribution des logiciels standards) si elles ne sont pas réalisées par l'auteur lui-même, sont donc subordonnées à la cession par l'auteur de son droit d'exploitation.

Les exemplaires du logiciel sont ensuite commercialisés.

III. Conséquences en ce qui concerne la qualification des opérations

a) La cession de logiciels standards, pour un prix déterminé à la date de l'opération, est toujours considérée comme une livraison de biens sauf lorsque :

5. Le contrat s'analyse en une cession de droits d'auteur. Tel est le cas par exemple du contrat conclu entre l'auteur (développeur) et l'éditeur en vue de la fabrication et de la commercialisation d'exemplaires conformément aux dispositions de l'article L 122-6 du Code de la propriété intellectuelle.

6. Précision : dans le cas de la commercialisation d'un exemplaire d'un logiciel standard, pour un prix forfaitaire et définitif, les clauses du contrat qui limitent les prérogatives de l'acheteur afin de protéger les droits de l'auteur n'ont pas pour effet de déqualifier fiscalement l'opération en cession de droits (quelle que soit la terminologie employée dans le contrat : convention de droits d'utilisation, d'usage,...). En effet, il y a bien cession des exemplaires qui constituent des biens meubles corporels.

7. La cession intervient en l'absence de support matériel (transmission par voie télématique par exemple).

Dans ces deux hypothèses (cession de droits portant sur un logiciel standard ou absence de support matériel), l'opération constitue une prestation de services.

8. b) La cession d'un logiciel spécifique est toujours considérée comme une prestation de services.

IV. Les règles de TVA applicables

1° La cession du logiciel constitue une livraison de bien meuble corporel.

9. La livraison du logiciel est imposable à la TVA au taux de 20,6% selon les règles de droit commun applicables aux livraisons de biens.

Le lieu des livraisons de biens meubles corporels est déterminé par les articles 258 à 258 B du CGI.

Il est précisé que lorsque le contrat de vente dispose que la cession du logiciel intervient après son installation chez le client, l'opération s'analyse en une livraison après installation (CGI, article 258-I-b).

10. Par ailleurs, le régime particulier des ventes à distance, précisé aux articles 258 A et 258 B du CGI, s'applique, le cas échéant, aux cessions de logiciels standards expédiés ou transportés dans ou à partir d'un Etat membre de la Communauté européenne par le vendeur ou pour son compte à destination d'une personne bénéficiant du régime dérogatoire ou d'une personne physique non assujettie.

11. Le régime des acquisitions intra-communautaires s'applique, le cas échéant, aux acquisitions de logiciels standards.

2) La cession du logiciel constitue une prestation de services.

12. La cession du logiciel est imposable à la TVA au taux de 20,6% selon les règles de droit commun applicables aux prestations de services.

13. En matière de territorialité, la cession de logiciels spécifiques et la cession de logiciels standards transmis en l'absence de support matériel relèvent de l'article 259 B du CGI.

14. Les prestations de services de cette nature sont imposables à la TVA en France lorsque :

- le prestataire et le preneur sont établis en France ;

- le prestataire est établi en France et le preneur est établi dans un autre Etat membre de la Communauté européenne sans y être assujetti à la TVA ;

- le prestataire est établi dans un autre Etat membre de la Communauté européenne et le preneur est assujetti à la TVA en France ;

- le prestataire est établi hors de la Communauté européenne et le preneur est assujetti à la TVA en France, ou

une personne établie ou domiciliée en France sans y être assujettie qui utilise le logiciel en France (article 259 C).

15. Ces prestations ne sont pas imposables à la TVA en France lorsqu'elles sont rendues par une entreprise française à un preneur assujetti à la TVA dans un autre Etat membre de la Communauté européenne ou à un client établi hors de la Communauté européenne.

16. Nota : les opérations portant sur des logiciels , qu'il s'agisse de livraison de biens ou de prestations de services, bénéficient de la franchise en base de 70 000 F. La franchise en base de 245 000 F. ne s'applique pas à ces opérations (CGI, article 293 B-III-2°).

B. AUTRES OPERATIONS PORTANT SUR LES LOGICIELS

I. Les importations de logiciels

17. Les modalités d'imposition à la TVA des logiciels importés varient selon leur nature.

1° Importation de logiciels standards.

18. L'importation de tels logiciels constitue une importation de biens. La base d'imposition à l'importation est la valeur totale (support et données).

19. Lorsqu'une entreprise acquiert des droits d'exploitation sur un logiciel, l'opération s'analyse comme une prestation de services taxable à la TVA dans les conditions prévues à l'article 259 B du CGI (cf. supra, point 5). Si elle importe un support comportant les données nécessaires à cette exploitation (logiciel matrice), la base d'imposition à la TVA de cette importation est alors constituée de la valeur du support (à l'exclusion du prix de la cession des droits d'exploitation généralement acquitté sous forme de redevances) augmenté du montant de tous les autres frais accessoires.

2° Importation de logiciels spécifiques.

20. Lorsque les logiciels spécifiques sont importés sur un support physique (bande magnétique, disque optique, disquette,...), la valeur en douane est établie en ne retenant que le prix du support, à l'exclusion du coût des données, à condition que ces valeurs soient connues distinctement.

21. En outre, la fourniture des données constitue une prestation de services imposable à la TVA en France en application des articles 259 B ou 259 C du CGI si le logiciel a fait l'objet d'une cession à titre onéreux. Selon le cas, la taxe est due :

- par le preneur du service s'il est assujetti à la TVA en France (CGI, article 283-2) ;

- par le prestataire si le preneur du service n'est pas assujetti à la TVA et que le service est utilisé en France (CGI, article 259 C). Conformément à l'article 289 A du CGI, le prestataire étranger doit, s'il n'est pas établi en France, désigner un représentant fiscal qui s'engage à accomplir les formalités et à acquitter la taxe exigible.

3° Importation de logiciels en l'absence de support matériel.

22. La fourniture par une entreprise établie hors de la Communauté européenne à un client français de logiciels standards ou spécifiques qui sont transmis en l'absence de support matériel (au moyen d'une ligne téléphonique, d'un réseau spécialisé,...) constitue une prestation de services de l'article 259 B du CGI.

23. Cette prestation est imposable à la TVA en France, dès lors que le preneur du service est assujetti à la TVA en France (CGI, article 259 B) ou qu'il est établi ou domicilié en France sans y être assujetti dès lors que le logiciel est utilisé en France (CGI, article 259 C). La taxe est due par le preneur ou par le prestataire comme indiqué au point 21 ci-dessus.

La réalisation d'une telle prestation n'est soumise à aucune formalité douanière.

II. Les locations de logiciels

24. La location de logiciels (mise à disposition moyennant une redevance périodique) constitue une prestation de services (article 259 B du CGI).

III. Les opérations d'installation

25. Les opérations d'installation de logiciels constituent des prestations de services imposables dans les conditions de droit commun lorsque leur prix n'est pas inclus dans le prix du logiciel.

26. 1. Lorsque l'opération d'installation de logiciels consiste en une intervention matérielle sur le site d'implantation, elle s'analyse comme une prestation de l'article 259 A-4°-bis du CGI issu de l'article 19 de la loi n°95-1347 du 30 décembre 1995 (Dr. Fisc. 1996, n°1-2, comm.1).

En application des dispositions de cet article, la prestation d'installation de logiciels qui demeurent implantés sur un site français est imposable à la TVA en France.

27. 2. Lorsque le logiciel est installé à distance (téléchargement) ou que l'intervention du fournisseur se limite à une assistance téléphonique, l'opération constitue une prestation de l'article 259 B du CGI.

28. Les prestations de cette nature sont situées en France :

- lorsqu'elles sont rendues par un prestataire français à un preneur établi en France ou établi ou domicilié dans un autre Etat membre de la Communauté européenne sans y être assujetti à la TVA (CGI, article 259 et 259 B) ;

- lorsque le prestataire est établi dans un autre Etat membre et que le preneur est assujetti à la TVA en France (CGI, article 259 C) ;

- lorsque le prestataire est établi hors de la Communauté européenne et que le logiciel est installé en France pour le compte d'un preneur non assujetti à la TVA (CGI, article 259 C).

29. Les mêmes prestations ne sont pas situées en France lorsqu'elles sont rendues par un prestataire français à un preneur assujetti à la TVA dans un autre Etat membre de la Communauté européenne ou à un client établi hors de la Communauté européenne (CGI, article 259 B).

IV. Les opérations de formation

30. Des services de formation peuvent être fournis à l'occasion de la cession de logiciels, standards ou spécifiques.

31. Ces opérations constituent des prestations imposables dans les conditions de droit commun lorsqu'elles font l'objet d'un prix distinct de la cession du logiciel.

32. Elles sont situées en France lorsqu'elles y sont matériellement exécutées (CGI, article 259 A-4°).

33. Elles peuvent éventuellement bénéficier des dispositions de l'article 261-4-4°-a du CGI qui exonèrent les opérations de formation professionnelle continue si les conditions d'exonération posées par ce texte sont remplies.

V. Les opérations de maintenance

34. Les opérations de maintenance dont le prix est distinct de celui de la fourniture du logiciel constituent

des prestations de services imposables selon les règles habituelles.

Ces opérations peuvent être exécutées selon des modalités diverses : déplacement chez le client, dépannage à distance.

35. 1. Les opérations de maintenance qui se traduisent par une intervention à distance (dépannage à distance, assistance téléphonique,...), et les opérations réalisées en exécution d'un contrat d'assistance par abonnement constituent des prestations de l'article 259 B du CGI.

La réalisation occasionnelle, dans le cadre du contrat d'assistance, d'une prestation sur site qui ne donne pas lieu à la facturation d'un supplément de prix, ne remet pas en cause cette analyse.

36. Les prestations de cette nature sont situées en France :

- lorsqu'elles sont rendues par un prestataire français à un preneur établi en France ou qui est établi ou domicilié dans un autre Etat membre de la Communauté européenne sans y être assujetti à la TVA (CGI, article 259 et 259 B) ;

- lorsque le prestataire est établi dans un autre Etat membre et que le preneur est assujetti à la TVA en France (CGI, article 259 B) ;

- lorsque le prestataire est établi hors de la Communauté européenne et que la maintenance se rapporte à un logiciel installé en France chez un preneur non assujetti à la TVA (CGI, article 259 C).

37. Les mêmes prestations ne sont pas situées en France lorsqu'elles sont rendues par un prestataire français à un preneur assujetti à la TVA dans un autre Etat membre de la Communauté européenne ou à un client établi hors de la Communauté européenne (CGI, article 259B).

38. 2. Les opérations de maintenance qui consistent en une intervention matérielle chez le client ou qui résultent d'un contrat d'assistance sur site s'analysent comme des prestations relevant de l'article 259 A-4°-bis du CGI issu de l'article 19 de la loi n°95-1347 du 30 décembre 1995 précitée. Le lieu des prestations de cette nature est situé dans l'Etat où le service est matériellement exécuté.

Par dérogation à ce principe, le lieu de ces opérations rendues par un preneur identifié à la TVA dans un autre Etat membre de la Communauté européenne est situé sur le territoire de l'Etat membre qui a attribué au preneur le numéro d'identification sous lequel le service lui est rendu, à condition que les biens quittent le territoire après la réalisation de la prestation.

Dès lors, les opérations de maintenance effectuées en France sur des logiciels qui demeurent implantés en France constituent des prestations imposables en France.

VI. La fourniture d'adaptations

39. Lorsque l'adaptation d'un logiciel standard est effectuée en fonction des besoins spécifiques d'un client, les opérations d'adaptation de ce logiciel constituent des prestations de services.

Lorsque l'adaptation est elle-même un standard, le régime des livraisons de biens s'applique.

Les opérations d'adaptation de logiciels spécifiques constituent toujours des prestations de services.

VII. La fourniture de mises à jour

40. La qualification de cette opération doit s'opérer selon les critères définis au A.

En règle générale, la qualification de l'opération de fourniture de mises à jour sera identique à celle retenue pour le logiciel initial.

C. REGLEMENT DU PASSE

41. Les dispositions de la présente instruction sont applicables aux contrôles en cours et, sur demande des intéressés, aux impositions non définitives à la date de sa publication.

Extraits de la décision de la Cour de Justice des communautés européennes du 7 mars 1995, en matière de diffamation internationale et de compétence des juridictions nationales (Shevill C/ Presse Alliance, aff. C-68-93)

[....]

3- Il ressort du dossier que Presse Alliance SA, qui édite le journal France-Soir, a publié le 23 septembre 1989 un article relatif à une opération que des agents de la brigade antidrogue de la police française avaient effectué dans un des locaux de change exploités à Paris par Chequepoint SARL. Cet article, qui était fondé sur des renseignements fournis par l'agence France Presse, mentionnait la Société Chequepoint ainsi qu'une jeune femme du nom de Fiona Shevill-Avril.

4- Chequepoint SARL, société de droit français établie à Paris, exploite des bureaux de change en France depuis 1988. Il n'est pas allégué qu'elle exerce des activités en Angleterre ou au Pays de Galles.

5- Madame Fiona Shevill a été employée à titre temporaire, pendant trois mois au cours de l'été 1989, par Chequepoint SARL à Paris. Elle est retournée en Angleterre le 26 septembre 1989.

6- Ixora Trading Inc., qui n'est pas une société de droit anglais, exploite depuis 1974 des bureaux de change en Angleterre sous le nom de "Chequepoint".

7- Chequepoint International Limited, société holding de droit belge établie à Bruxelles, contrôle Chequepoint SARL et Ixora Trading Inc.

8- Estimant que l'article susmentionné était diffamatoire en ce qu'il suggérait qu'elles faisaient partie d'un réseau de trafic de drogue pour lequel elles avaient effectué des opérations de blanchiment d'argent, Madame Shevill, Chequepoint SARL, Ixora Trading Inc. et Chequepoint International Limited ont, le 17 octobre 1989, assigné Presse Alliance SA en diffamation devant la High Court of England and Wales, en demandant réparation en ce qui concerne les exemplaires de France-Soir distribués tant en France que dans les autres pays européens, y compris ceux vendus en Angleterre et au Pays de Galles. Ultérieurement, les demandeurs ont modifié leurs conclusions en abandonnant toute référence aux exemplaires vendus en dehors de l'Angleterre et du Pays de Galles. Le droit anglais prévoyant en matière de diffamation une présomption de préjudice, les demandeurs n'ont pas eu à apporter la preuve du préjudice résultant de la publication de l'article litigieux.

9- Il est constant que France Soir est distribué principalement en France, la diffusion de ce journal, assurée par des distributeurs indépendants, étant très faible au Royaume-Uni. On estime à plus de 237 000 le nombre d'exemplaires de l'édition litigieuse qui ont été vendus en France et à près de 15 500 le nombre d'exemplaires distribués dans les autres pays européens, dont 230 exemplaires vendus en Angleterre et au Pays de Galles (5 dans le Yorkshire).

10- Le 23 novembre 1989, France Soir a publié un texte d'excuses précisant qu'il n'avait pas eu l'intention d'affirmer qu'un des propriétaires des bureaux de change Chequepoint ou Madame Shevill avaient été impliqués dans un trafic de drogue ou des opérations de blanchiment d'argent.

11- Le 7 décembre 1989, Presse Alliance Sa a contesté la compétence de la High Court of England and Wales pour connaître du litige, au motif qu'aucun fait dommageable, au sens de l'article 5, point 3, de la convention, ne s'était produit en Angleterre.

12- Cette exception a été rejetée par ordonnance du 10 avril 1990. L'appel interjeté contre cette décision a été rejeté par ordonnance du 14 mai 1990.

13- Le 12 mars 1991, la Court of appeal a, d'une part, rejeté le recours que Presse Alliance Sa avait formé contre cette dernière décision et, d'autre part, sursis à statuer sur la demande de Chequepoint International Limited.

14- Presse Alliance SA a introduit un pourvoi contre cette décision devant la House of Lords, avec l'autorisation préalable de celle-ci.

15- Presse Alliance SA a soutenu en substance que conformément à l'article 2 de la convention, les juridictions françaises étaient compétentes pour connaître du litige et que les tribunaux anglais n'avaient pas compétence au titre de l'article 5, point 3, de cette convention, puisque le « lieu où le fait dommageable s'est produit au sens de cette disposition, était en France et qu'aucun fait dommageable ne s'était produit en Angleterre ».

16- Estimant que le litige soulevait des problèmes d'interprétation de la convention, la House of Lords a, par ordonnance du 1er mars 1993, décidé de surseoir à statuer jusqu'à ce que la Cour se soit prononcée à titre préjudiciel ;

[....]

Sur les première, deuxième, troisième et sixième questions ;

17- Par ses première, deuxième, troisième et sixième questions, qu'il y a lieu d'examiner ensemble, la juridiction de renvoi interroge en substance la Cour sur l'interprétation de la notion de « lieu où le fait dommageable s'est produit » utilisé par l'article 5, point 3, de la convention, afin de déterminer quelles juridictions sont compétentes pour statuer sur une action en réparation des préjudices causés à la victime à la suite de la diffusion d'un article de presse diffamatoire dans plusieurs Etats contractants.

18- En vue de répondre à ces questions, il convient de rappeler d'abord que, par dérogation au principe général consacré par l'article 2, alinéa 1er, de la convention, à savoir celui de la compétence des juridictions de l'Etat contactant du domicile du défendeur, l'article 5, point 3 de la convention dispose :

« Le défendeur domicilié sur le territoire d'un Etat contractant peut être attrait, dans un autre Etat contractant [....]

3) en matière délictuelle ou quasi délictuelle, devant le tribunal du lieu où le fait dommageable s'est produit » ;

[....]

20- Il y a lieu de souligner ensuite que, dans l'arrêt Mines de potasse d'Alsace (V. arrêts du 30 novembre 1976, Mines de potasse d'Alsace, 21/76, Rec. CJCE, p. 1735, point 11, et du 11 janvier 1990, Dumez-France et Tracoba, C-220/88, Rec. CJCE, p. 1-49, point 17), la Cour a dit pour droit que, dans le cas où le lieu où se situe le fait susceptible d'entraîner une responsabilité délictuelle ou quasi délictuelle et le lieu où ce fait a entraîné un dommage ne sont pas identique, l'expression « lieu où le fait dommageable s'est produit », figurant dans l'article 5, point 3 de la convention doit être entendue en ce sens qu'elle vise à la fois le lieu où le dommage est survenu et le lieu de l'événement causal qui est à l'origine de ce dommage.

21- Dans cet arrêt, la Cour a en effet considéré (points 15 et 17) que le lieu de l'événement causal non moins que celui de la matérialisation du dommage peut constituer un rattachement significatif du point de vue de la compétence judiciaire, chacun d'entre eux étant susceptible, selon les circonstances, de fournir une indication particulièrement utile en ce qui concerne la preuve et l'organisation du procès.

[....]

23- Ces constatations, faites à propos de dommages matériels, doivent valoir également, pour les mêmes motif, dans le cas de préjudices non patrimoniaux, notamment ceux causés à la réputation et à la considération d'une personne physique ou morale par une publication diffamatoire.

24- Dans l'hypothèse d'une diffamation au moyen d'un article de presse diffusé sur le territoire de plusieurs Etats contractants, le lieu de l'événement causal, au sens de cette jurisprudence, ne peut être que le lieu d'établissement de l'éditeur de la publication litigieuse, en tant qu'il constitue le lieu d'origine du fait dommageable, à partir duquel la diffamation a été exprimée et mise en circulation.

25- Le tribunal du lieu d'établissement de l'éditeur de la publication diffamatoire doit dès lors avoir compétence pour connaître de l'action en réparation de l'intégralité du préjudice causé par l'acte illicite.

26- Ce for coïncide toutefois, en règle générale avec le chef de compétence de principe consacré par l'article 2 alinéa 1er de la convention.

27- Ainsi que la Cour l'a jugé dans l'arrêt Mines de potasse d'Alsace, précité, il convient en conséquence de reconnaître au demandeur la faculté d'introduire son action également au lieu où le préjudice a été matérialisé sous peine de vider de sa substance l'article 5, point 3 de la convention.

28- Le lieu de matérialisation du préjudice est l'endroit où le fait générateur, engageant la responsabilité délictuelle ou quasi délictuelle de son auteur, a produit ses effets dommageables à l'égard de la victime.

29- Dans le cas d'une diffamation internationale par voie de presse, l'atteinte portée par une publication diffamatoire à l'honneur, à la réputation et à la considération d'une personne physique ou morale se manifeste dans les lieux où la publication est diffusée, lorsque la victime y est connue.

30- Il en résulte que les juridictions de chaque Etat contractant dans lequel la publication diffamatoire a été diffusée et où la victime prétend avoir subi une atteinte à sa réputation sont compétentes pour connaître des

dommages causés dans cet Etat à la réputation de la victime.

31- En effet, conformément à l'impératif d'une bonne administration de la justice, fondement de la règle de compétence spéciale de l'article 5, point 3, le tribunal de chaque Etat dans lequel la publication diffamatoire a été diffusée et où la victime prétend avoir subi une atteinte à sa réputation est territorialement le plus qualifié pour apprécier la diffamation commise dans cet Etat et déterminer l'étendue du préjudice correspondant.

32- S'il est vrai que le jugement des divers aspects d'un même litige par des tribunaux différents présente des inconvénients, le demandeur a cependant toujours la faculté de porter l'ensemble de sa demande devant le tribunal soit du domicile du défendeur, soit du lieu d'établissement de l'éditeur de la publication diffamatoire.

33- Compte tenu de l'ensemble des considérations qui précèdent, il y a lieu de répondre aux première, deuxième, troisième et sixième questions posées par la House of Lords que l'expression « lieu où le fait dommageable s'est produit », utilisée à l'article 5, point 3 de la convention, doit, en cas de diffamation au moyen d'un article de presse diffusé dans plusieurs Etats contractants, être interprété en ce sens que la victime peut intenter contre l'éditeur une action en réparation soit devant les juridictions de l'Etat contractant du lieu d'établissement de l'éditeur de la publication diffamatoire, compétentes pour réparer l'intégralité des dommages résultant de la diffamation, soit devant les juridictions de chaque Etat contractant dans lequel la publication a été diffusée et où la victime prétend avoir subi une atteinte à sa réputation, compétentes pour connaître des seuls dommages causés dans l'Etat de la juridiction saisie.

Extraits de la Convention de Rome du 19 juin 1980 sur la loi applicable aux obligations contractuelles

[....]

Titre Ier : Champ d'application

Article 1er : Champ d'application

1. Les dispositions de la présente Convention sont applicables, dans les situations comportant un conflit de lois, aux obligations contractuelles.

[....]

Article 2 : Caractère universel

La loi désignée par la présente Convention s'applique même si cette loi est celle d'un Etat non contractant.

Titre II : Règles uniformes

Article 3 : Liberté de choix

1. Le contrat est régi par la loi choisie par les parties. ce choix doit être exprès ou résulter de façon certaine des dispositions du contrat ou des circonstances de la cause. par ce choix, les parties peuvent désigner la loi applicable à la totalité ou à une partie seulement de leur contrat.

2. Les parties peuvent convenir, à tout moment, de faire régir le contrat par une loi autre que celle qui le régissait auparavant soit en vertu d'un choix antérieur selon le présent article, soit en vertu d'autres dispositions de la présente Convention. Toute modification quant à la détermination de la loi applicable, intervenue postérieurement à la conclusion du contrat, n'affecte pas la validité formelle du contrat au sens de l'article 9 et ne porte pas atteinte aux droits des tiers.

3. Le choix par les parties d'une loi étrangère, assortie ou non de celui d'un tribunal étranger ne peut , lorsque tous les autres éléments de la situation sont localisés au moment de ce choix dans un seul pays, porter atteinte aux dispositions auxquelles la loi de ce pays ne permet pas de déroger par contrat, ci-après dénommées « Dispositions impératives ».

[....]

Article 4 : Loi applicable à défaut de choix

1. Dans la mesure où la loi applicable au contrat n'a pas été choisie conformément aux dispositions de l'article 3, le contrat est régi par la loi du pays avec lequel il présente les liens les plus étroits. Toutefois, si une partie de contrat est séparable du reste du contrat et présente un lien plus étroit avec un autre pays, il pourra être fait application, à titre exceptionnel, à cette partie du contrat de la loi de cet autre pays.

2. Sous réserve du paragraphe 5, il est présumé que le contrat présente les liens les plus étroits avec le pays où la partie qui doit fournir la prestation caractéristique a, au moment de la conclusion du contrat, sa résidence habituelle ou, s'il s'agit d'une société, association ou personne morale, son administration centrale. Toutefois, Si le contrat est conclu dans l'exercice de l'activité professionnelle de cette partie, ce pays est celui où est situé son principal établissement ou, si, selon le contrat, la prestation doit être fournie par un établissement autre que l'établissement principal, celui où est situé cet autre établissement.

3. Nonobstant les dispositions du paragraphe 2, dans la mesure où le contrat a pour objet un droit réel immobilier ou un droit d'utilisation d'un immeuble, il est présumé que le contrat présente les liens les plus étroits avec le pays où est situé l'immeuble.

[....]

5. L'application du paragraphe 2 est écartée lorsque la prestation caractéristique ne peut être déterminée. Les présomptions des paragraphes 2, 3 et 4 sont écartées lorsqu'il résulte de l'ensemble des circonstances que le contrat présente des liens plus étroits avec un autre pays.

Article 5 : Contrats conclus par les consommateurs

1. Le présent article s'applique aux contrats ayant pour objet la fourniture d'objets mobiliers corporels ou de services à une personne, le consommateur, pour un usage pouvant être considéré comme étranger à son activité professionnelle, ainsi qu'aux contrats destinés au financement d'une telle fourniture.

2. Nonobstant les dispositions de l'article 3, le choix par les parties de la loi applicable ne peut avoir pour résultat de priver le consommateur de la protection que lui assurent les dispositions impératives de la loi du pays dans lequel il a sa résidence habituelle :

- si la conclusion du contrat a été précédée dans ce pays d'une proposition spécialement faite ou d'une publicité, et si le consommateur a accompli dans ce pays les actes nécessaires à la conclusion du contrat, ou

- si le cocontractant du consommateur ou son représentant a reçu la commande du consommateur dans ce pays, ou

- si le contrat est une vente de marchandises et que le consommateur se soit rendu de ce pays dans un pays étranger et y ait passé la commande, à la condition que

la voyage ait été organisé par le vendeur dans le but d'inciter le consommateur à conclure une vente.

3. Nonobstant les dispositions de l'article 4 et à défaut de choix exercé conformément à l'article 3, ces contrats sont régis par la loi du pays dans lequel le consommateur a sa résidence habituelle, s'ils sont intervenus dans les circonstances décrites au paragraphe 2 du présent article.

4. Le présent article ne s'applique pas :

a) Au contrat de transport ;

b) Au contrat de fourniture de services lorsque les services dus au consommateur doivent être fournis exclusivement dans un pays autre que celui dans lequel il a sa résidence habituelle.

5. Nonobstant les dispositions du paragraphe 4, le présent article s'applique au contrat offrant pour un prix global des prestations combinées de transport et de logement.

[....]

Article 7 : Lois de police

1. Lors de l'application en vertu de la présente Convention, de la loi d'un pays déterminé, il pourra être donné effet aux dispositions impératives de la loi d'un autre pays avec lequel la situation présente un lien étroit, si et dans la mesure où, selon le droit de ce dernier pays, ces dispositions sont applicables quelle que soit la loi régissant le contrat. Pour décider si effet doit être donné à ces dispositions impératives, il sera tenu compte de leur nature et de leur objet ainsi que des conséquences qui découleraient de leurrât application ou de leur non-application.

2. Les dispositions de la présente Convention ne pourront porter atteinte à l'application des règles de la loi du pays du juge qui régissent impérativement la situation quelle que soit la loi applicable au contrat.

[....]

Extraits de la Convention de Bruxelles du 27 septembre 1968 concernant la compétence judiciaire et l'exécution des décisions en matière civile et commerciale

[....]

Titre II : Compétence

Section 1 : Dispositions générales

Art. 2. Sous réserve des dispositions de la présente convention, les personnes domiciliées sur le territoire d'un Etat contractant sont atttraites, quelle que soit leur nationalité, devant les juridictions de cet Etat.

Les personnes qui ne possèdent pas la nationalité de l'Etat dans lequel elles sont domiciliées y sont soumises aux règles de compétence applicables aux nationaux.

Art. 3. Les personnes domiciliées sur le territoire d'un Etat contractant ne peuvent être atttraites devant les tribunaux d'un autre Etat contractant qu'en vertu des règles énoncées aux sections 2 à 6 du présent titre.

[....]

Section 2 : Compétences spéciales

Art. 5. Le défendeur domicilié sur le territoire d'un Etat contractant peut être attrait, dans un autre Etat contractant :

1. en matière contractuelle, devant le tribunal du lieu où l'obligation qui sert de base à la demande a été ou doit être exécutée ;

2. en matière d'obligation alimentaire, devant le tribunal du lieu où le créancier d'aliments a son domicile ou sa résidence habituelle ou, s'il s'agit d'une demande accessoire à une action relative à l'état des personnes, devant le tribunal compétent selon la loi du for pour en connaître, sauf si cette compétence est uniquement fondée sur la nationalité d'une des parties ;

3. en matière délictuelle ou quasi-délictuelle, devant le tribunal du lieu où le fait dommageable s'est produit ;

4. S'il s'agit d'une action en réparation de dommage ou d'une action en restitution fondées sur une infraction, devant le tribunal saisi de l'action publique, dans la mesure où, selon sa loi, ce tribunal peut connaître de l'action civile ;

5. s'il s'agit d'une contestation relative à l'exploitation d'une succursale, d'une agence ou de tout autre établissement, devant le tribunal du lieu de leur situation ;

[....]

Art. 6. Ce même défendeur peut aussi être attrait :

1. s'il y a plusieurs défendeurs devant le tribunal du domicile de l'un d'eux ;

2. s'il s'agit d'une demande en garantie ou en intervention, devant le tribunal saisi de la demande originaire, à moins qu'elle n'ai été formée que pour traduire hors de son tribunal celui qui a été appelé ;

3. s'il s'agit d'une demande reconventionnelle qui dérive du contrat ou du fait sur lequel est fondé la demande originaire, devant le tribunal saisi de celle-ci.

[....]

Section 4 : Compétence en matière de contrats conclus par des consommateurs

13. En matière de contrats conclu par une personne pour un usage pouvant être considéré comme étranger à son activité professionnelle, ci-après dénommée « le consommateur », la compétence est déterminée par la présente section, sans préjudice des dispositions de l'article 4 et de l'article 5 point 5 ;

1. lorsqu'il s'agit d'une vente à tempérament d'objets mobiliers corporels ;

2. lorsqu'il s'agit d'un prêt à tempérament ou d'une autre opération de crédit liés au financement d'une vente de tels objets ;

3. pour tout autre contrat ayant pour objet une fourniture de services ou d'objets mobiliers corporels si :

a) la conclusion du contrat a été précédée dans l'Etat du domicile du consommateur d'une proposition spécialement faite ou d'une publicité

et que

b) le consommateur a accompli dans cet Etat les actes nécessaires à la conclusion de ce contrat.

Lorsque le cocontractant du consommateur n'est pas domicilié sur le territoire d'un Etat contractant, mais possède une succursale, une agence ou tout autre établissement dans un Etat contractant, il est considéré pour les contestations relatives à leur exploitation comme ayant son domicile sur le territoire de cet Etat.

la présente section ne s'applique pas au contrat de transport.

Art. 14. L'action intentée par un consommateur contre l'autre partie au contrat peut être portée soit devant les tribunaux de l'Etat contractant sur le territoire duquel est domicilié cette partie soit devant les tribunaux de l'Etat contractant sur le territoire duquel est domicilié le consommateur.

L'action intentée contre le consommateur par l'autre partie au contrat ne peut être portée que devant les tribunaux de l'Etat contractant sur le territoire duquel est domicilié le consommateur.

Ces dispositions ne portent pas atteinte au droit d'introduire une demande reconventionnelle devant le tribunal saisi d'une demande originaire conformément à la présente section.

Art. 15. Il ne peut être dérogé aux dispositions de la présente section que par des conventions :

1. postérieures à la naissance du différend

ou

2. qui permettent au consommateur de saisir d'autres tribunaux que ceux indiqués à la présente section

ou

3. qui, passés entre le consommateur et son cocontractant ayant, au moment de la conclusion du contrat, leur domicile ou leur résidence habituelle dans un même Etat contractant, attribuent compétence aux tribunaux de cet Etat sauf si la loi de celui-ci interdit de telles conventions.

Section 5 : Compétences exclusives

Art. 16. Sont seuls compétents, sans considération de domicile :

1. en matière de droits réels immobiliers et de baux d'immeubles, les tribunaux de l'Etat contractant où l'immeuble est situé ;

2. en matière de validité, de nullité ou de dissolution des sociétés ou personnes morales ayant leur siège sur le territoire d'un Etat contractant, ou des décisions de leurs organes, les tribunaux de cet Etat ;

3. en matière d'inscription ou de validité des brevets, marques, dessins et modèles, et autres droits analogues donnant lieu à un dépôt ou à un enregistrement, les juridictions de l'Etat contractant sur le territoire duquel le dépôt ou l'enregistrement a été demandé, a été effectué ou est réputé avoir été effectué aux termes d'une convention internationale ;

5. en matière d'exécution des décision, les tribunaux de l'Etat contractant du lieu de l'exécution.

Section 6 : Prorogation de compétence

Art. 17. Si les parties, dont l'une au moins a son domicile sur le territoire d'un Etat contractant, sont convenues d'un tribunal ou de tribunaux d'un Etat contractant pour connaître de différends nés ou à naître à l'occasion d'un rapport de droit déterminé, ce tribunal ou les tribunaux de cet Etat sont seuls compétents. Cette convention attributive de juridiction doit être conclue soit pat écrit , soit verbalement avec confirmation écrite, soit dans le commerce international, en une forme admise par les usages dans ce domaine et que les parties connaissent ou sont censées connaître. Lorsqu'une telle convention est conclue par des parties dont aucune n'a son domicile sur le territoire d'un Etat contractant, les tribunaux des autres Etats contractants ne peuvent pas connaître du différend tant que le tribunal ou les tribunaux désignés n'ont pas décliné leur compétence.

[....]

Les conventions attributives de juridiction ainsi que les stipulations similaires d'actes constitutifs de trust sont sans effet si elles sont contraires aux dispositions des articles 12 et 15 ou si les tribunaux à la compétence desquels elles dérogent sont exclusivement compétents en vertu de l'article 16.

Si une convention attributive de juridiction n'a été stipulée qu'en faveur de l'une des parties, celle-ci conserve le droit de saisir tout autre tribunal compétent en vertu de la présente convention.

[....]

Titre III : Reconnaissance et exécution

Art. 25. On entend par décision, au sens de la présente convention, toute décision rendue par une juridiction d'un Etat contractant quelle que soit la dénomination qui lui est donnée telle qu'arrêt, jugement, ordonnance ou mandat d'exécution, ainsi que la fixation par le greffier des montants des frais du procès.

Section 1 : Reconnaissance

Les décisions rendues dans un Etat contractant sont reconnues dans les autres Etats contractants, sans qu'il soit nécessaire de recourir à aucune procédure.

En cas de contestation, toute partie intéressée qui invoque la reconnaissance à titre principal peut faire constater, selon la procédure prévue aux sections 2 et 3 du présent titre, que la décision doit être reconnue.

Si la reconnaissance est invoquée de façon incidente devant une juridiction d'un Etat contractant, celle-ci est compétente pour en connaître.

Art. 27. Les décisions ne sont pas reconnues :

1. si la reconnaissance est contraire à l'ordre public de l'Etat requis ;

2. si l'acte introductif d'instance ou un acte équivalent n'a pas été signifié ou notifié au défendeur défaillant, régulièrement et en temps utile, pour qu'il puisse se défendre ;

3. si la décision est inconciliable avec une décision rendue entre les mêmes parties dans l'Etat requis;

[....]

5. si la décision est inconciliable avec une décision rendue antérieurement dans un Etat non contractant entre les mêmes parties dans un litige ayant le même objet et la même cause, lorsque cette dernière décision réunit les conditions nécessaires à sa reconnaissance dans l'Etat requis.

[....]

Art. 29. En aucun cas, la décision étrangère ne peut faire l'objet d'une révision au fond.

[....]

Section 2 : Exécution

Art. 31. Les décisions rendues dans un Etat contractant et qui y sont exécutoires sont mises à exécution dans un autre Etat contractant après y avoir été revêtues de la formule exécutoire sur requête de toute partie intéressée.

[....]

Index

R

S

T

U

V

W

Valérie Sédallian
sedallian@argia.fr
http://www.argia.fr/lij

Collection AUI
Association des Utilisateurs d'Internet
40 quai de Jemmapes 75010 Paris
http://www.aui.fr

Éditions Net Press
191 avenue Aristide-Briand 94230 Cachan
http://www.netpress.fr

Imprimé en France par Jouve
Dépôt légal : janvier 1997
ISBN : 2-9510901-0-2