REVUE MENSUELLE D'INFORMATION JURIDIQUE

DE

DROIT-NTIC

AVRIL 2003

SOMMAIRE

→ Le Peer To Peer : remise en cause des données personnelles sur l'Internet.

→ L'OCDE adapte la notion d'établissement stable au commerce électronique.

→ La sécurité intérieure et quotidienne du web : l'arsenal de règles juridiques se renforce.

→ La preuve sur Internet : les règles classiques et l'apport de la signature électronique.

→ Le droit d'utiliser une marque n'est pas sans limite

→ Internet sans fil : les nouveaux enjeux juridiques du Wi-Fi

30/04/2003

Le Peer To Peer : remise en cause des données personnelles sur l'Internet

- Auteur : **Webconseil** , *Société de conseil*
- Domaine : INFORMATIQUE_ET_LIBERTES
- Sous thème : Droit_d_auteur
- Ordre juridique :

Les services d'échange gratuits en Peer To Peer (P2P), à l'image de KaZaA, ou anciennement Napster, font l'objet d'attaques constantes de la part de l'industrie musicale et du cinéma, ainsi que des sociétés de gestion des droits d'auteur, en raison du piratage et de la contrefaçon massive des droits de propriété intellectuelle rendus possibles aux internautes utilisant ces services.

Un juge fédéral Californien vient pourtant de débouter la RIAA (Recording Industry Association of America) d'une plainte déposée contre les services P2P Grokster et Morpheus, en déclarant notamment que l'exploitation de ces services d'échange gratuits n'était pas systématiquement répréhensible, dans la mesure où ces services ne peuvent contrôler la nature et le caractère protégé ou non des fichiers échangés à l'aide de leurs logiciels, et qu'ils ne sont pas responsables des abus d'utilisation des logiciels à la base des services P2P.

Confrontés à ce type de fondement juridique, les opposants au P2P se retournent de plus en plus contre les internautes utilisateurs de ces services d'échange.

Or l'identification de ces utilisateurs repose sur l'obtention des adresses IP de ces derniers, chaque internaute possédant effectivement une adresse IP, sorte de signature de son ordinateur sur le réseau.

La CNIL (Commission Nationale Informatique et Libertés) considérant que l'adresse d'un Internaute est une donnée nominative, et donc strictement personnelle, l'internaute doit donc donner, conformément à l'article 26 de la Loi Informatiques et Libertés du 6 janvier 1978, son accord pour que son adresse IP soit collectée et éventuellement transmise à des tiers.

Ce principe est aujourd'hui malmené par le Sénat, lequel, dans le cadre du projet de réforme de la Loi du 6 janvier 1978, vient d'ouvrir par voie d'amendement la possibilité, à certaines personnes morales, de procéder à des traitements de données à caractère personnel relatives à des infractions, condamnations ou mesures de sûreté.

Dans la mesure où le téléchargement de fichiers protégés relève d'une infraction à la législation sur la propriété intellectuelle, en tant qu'acte de contrefaçon de droits d'auteur, cet amendement permet désormais aux entreprises privées, du type des sociétés de gestion collective des droits d'auteur, de mettre en place des outils collectant les adresses IP des utilisateurs des réseaux d'échanges P2P, en vue de l'engagement de poursuites judiciaires.

La question du consentement de l'internaute à la collecte et au traitement de son adresse IP, et au-delà, de la notion de données personnelles sur l'Internet, et le régime de

protection qui leur est conféré, devra donc être surveillée à l'avenir, surtout lorsque l'on considère la l'injonction faite à un fournisseur d'accès Internet, le 24 avril dernier, par la Cour du District de Columbia de transmettre les coordonnées de certains de ses abonnés utilisateurs de services P2P, en dépit de l'atteinte au droit constitutionnel à la vie privée de l'internaute invoqué par le dit fournisseur d'accès…

A suivre…

22/04/2003

L'OCDE adapte la notion d'établissement stable au commerce électronique

- Auteur : **Webconseil** , *Société de conseil*

- Domaine : COMMERCE_ELECTRONIQUE
- Sous thème : Fiscalité
- Ordre juridique :

La législation fiscale applique le principe de la taxation d'une société dans l'Etat de résidence de celle-ci, sauf lorsque l'activité est poursuivie par un établissement stable, soit un établissement fixe d'affaire, au sens de l'impôt sur les sociétés, situé dans un autre Etat.

La question se pose donc de l'application de la notion d'établissement stable dans le contexte de l'Internet et du commerce électronique.

Le site web d'une entreprise française hébergé sur un serveur étranger lui assurant l'accès auprès des utilisateurs, où qu'ils soient situés, constitue-t-il un établissement stable, de cette entreprise française dans cet Etat étranger ? Et, au-delà, dans quelles conditions un serveur, en ce qu'il est un équipement matériel nécessitant un emplacement, et en ce qu'il peut être tout aussi bien passif lorsqu'il ne joue qu'un rôle de connexion à Internet, qu'actif lorsqu'il assure l'exécution de commandes, pourrait-il être considéré comme un établissement stable?
La réponse à cette question est cruciale, car dans l'affirmative, elle permettrait de « détourner » l'imposition des bénéfices d'une entreprise exploitant un site de commerce électronique, au profit de l'Etat dans lequel le serveur du site est localisé.
La question avait été confiée au comité des affaires fiscales de l'OCDE, dont le résultat des travaux a été pris en compte dans la mise à jour 2003 du modèle de convention fiscale de l'OCDE.
Le Comité a refusé d'appliquer la notion d'établissement stable aux sites Internet, considérant leur caractère immatériel.
Il en a cependant décidé autrement s'agissant des serveurs, dans la mesure où leur appréhension dans l'espace et dans un lieu donné étant susceptible d'être effectuée, il apparaît que la notion d'établissement stable peut être appliquée à l'emplacement où se trouve localisé le serveur.
Le Comité a toutefois estimé que la localisation d'un serveur ne permet pas à elle seule de retenir l'existence d'un établissement stable. Il est nécessaire, en outre, que le serveur soit à la disposition de l'entreprise et que des fonctions essentielles de cette entreprise soient réalisées par l'intermédiaire du serveur.
Seul le respect de ces trois conditions cumulatives permet en conséquence de retenir

l'existence d'un établissement stable en matière de commerce électronique et doncde déroger au principe de taxation dans l'Etat de résidence de l'entreprise.

14/04/2003

La sécurité intérieure et quotidienne du web : l'arsenal de règles juridiques se renforce.

- Auteur : **Me. Murielle-Isabelle Cahen ,** *Avocate*
- Domaine : INFORMATIQUE_ET_LIBERTES
- Sous thème : Criminalité_informatique
- Ordre juridique :

La sécurité sur Internet se trouve au centre des interventions législatives récentes : loi relative à la sécurité quotidienne, projet de loi pour la sécurité intérieure, projet de loi pour la confiance dans l'économie numérique, elles comportent tous, de manière supplétive, des dispositions ayant comme objet de permettre la mise en place de procédures sécuritaires propres aux nouvelles technologies de l'information et de la communication.

La **loi relative à la sécurité quotidienne** du 15 novembre 2001, tout d'abord, a introduit dans le droit positif français certains mesures sécuritaires spécifiques à Internet, dont notamment la conservation, pendant une période d'un an, des données relatives à une communication et ce « *pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales* » (art.29). Ces données, précise la loi, ne peuvent « *en aucun cas, porter sur le contenu des correspondances échangées ou des informations consultées sous quelque forme que ce soit* », mais concernent seulement l'identité des utilisateurs et les caractéristiques techniques des services fournis par les prestataires de communication (comme par exemple les adresses IP, les adresses de messagerie électronique envoyées ou reçues, ainsi que les adresses des sites visités).

L'article 30 de cette loi a, par ailleurs, modifié le code de procédure pénale en y insérant un chapitre concernant **la mise en clair des données chiffrées nécessaires à la manifestation de la vérité**. Ainsi, lorsque les données obtenues au cours d'une enquête ou d'une instruction ont été chiffrées, « *le procureur de la République, la juridiction d'instruction ou la juridiction de jugement saisie de l'affaire peut désigner toute personne physique ou morale qualifiée, en vue d'effectuer les opérations techniques permettant d'obtenir la version en clair de ces informations ainsi que, dans le cas où un moyen de cryptologie a été utilisé, la convention secrète de déchiffrement, si cela apparaît nécessaire* ».

Pour facilité cette procédure de déchiffrement, l'article 30 de la loi prévoit également l'insertion dans la loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications, d'un article 11-1 qui dispose que « *Les personnes physiques ou morales qui fournissent des prestations de cryptologie visant à assurer une fonction de confidentialité sont tenues de remettre aux agents autorisés dans les conditions prévues à l'article 4, sur leur demande, les conventions permettant le déchiffrement des données transformées au moyen des prestations qu'elles ont fournies…*

»

Le fait de ne pas déférer, dans ces conditions, aux demandes des autorités habilitées est puni de deux ans d'emprisonnement et de 30000 € d'amende.

Ces obligations ont été confirmées par un décret n° 2002-997 du 16 juillet 2002 relatif à l'obligation mise à la charge des fournisseurs de prestations de cryptologie en application de l'article 11-1 de la loi du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications.

En pratique, ces dispositions mettent à la charge des fournisseurs des prestations de cryptologie et des éditeurs de logiciels de chiffrement l'obligation de prévoir des portes cachées dans leurs produits, afin de pouvoir procéder au déchiffrement quand cela leur est demandé par les autorités compétentes.

Il importe de remarquer, à ce point, que le **projet de loi pour la confiance dans l'économie numérique** reproduit respectivement en ces articles 26 et 27 le texte des articles 31 et 30 de la loi relative à la sécurité quotidienne, tout en les en abrogeant, de sorte qu'une fois ce texte définitivement adopté, la LSQ ne comportera plus de dispositions sur la cryptographie.

Quant au **projet de loi sur la sécurité intérieure**, définitivement adopté par l'Assemblée nationale et le Sénat les 12 et 13 février 2003 respectivement, il vient, lui aussi, compléter la LSQ dans le domaine informatique. En effet, le texte du projet prévoit que les fournisseurs d'accès à Internet doivent mettre à la disposition de l'officier de police judiciaire, sur demande de celui-ci, les informations utiles à la manifestation de la vérité, à l'exception de celles protégées par un secret prévu par la loi, contenues dans le ou les systèmes informatiques ou traitements de données nominatives qu'ils administrent et ce par voie télématique ou informatique dans les meilleurs délais (art. 8.1).

L'officier de police judiciaire peut, en outre, intervenant sur réquisition du procureur de la République préalablement autorisé par ordonnance du juge des libertés et de la détention, requérir des opérateurs de télécommunications de prendre, sans délai, toutes mesures propres à **assurer la préservation**, pour une durée ne pouvant excéder un an, du **contenu des informations** consultées par les personnes utilisatrices des services fournis par les opérateurs.

Cette disposition vient, apparemment, compléter l'article 29 de la LSQ qui prévoyait que la conservation des données ne peut, en aucun cas, porter sur le contenu des communications.

Enfin, l'article 8 bis de la LSI permet aux officiers de police judiciaire de procéder à la perquisition en ligne, en accédant « *par un système informatique implanté sur les lieux où se déroule la perquisition à des données intéressant l'enquête en cours et stockées dans ledit système ou dans un autre système informatique, dès lors que ces données sont accessibles à partir du système initial ou disponibles pour le système initial* ».

Dans le cas où les données accessibles seraient situées en dehors du territoire national, les autorités devront se conformer aux engagements internationaux existants. A l'heure actuelle, aucun accord international n'existe en ce domaine, la Convention du Conseil de l'Europe sur la cybercriminalité n'étant pas encore ratifiée.

10/04/2003

La preuve sur Internet : les règles classiques et l'apport de la signature électronique.

- Auteur : **Me. Murielle-Isabelle Cahen ,** *Avocate*
- Domaine : COMMERCE_ELECTRONIQUE
- Sous thème : Preuves_et_signatures
- Ordre juridique :

Comment peut-on apporter la preuve d'une transaction immatérialisée, d'un échange de consentements survenu par le biais du réseau ? Quelle est la valeur probatoire de l'écrit électronique ? La signature électronique assure-t-elle les mêmes fonctions que la signature manuscrite et dans quelles conditions ?

Ces questions constituent l'essentiel de la problématique de la preuve sur Internet, la sécurisation des échanges et la reconnaissance de la valeur juridique des outils d'une transaction sur Internet faisant partie des principaux objectifs poursuivis dès le lancement de ce nouveau monde virtuel (1) .

L'adaptation du droit de la preuve aux nouvelles technologies de l'information est intervenue, dans la plus part des Etats de l'Union Européenne, avec la transposition de la directive du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques. Aux Etats-Unis, un effort d'harmonisation des différentes lois fédéraux a été lancé avec l'entrée en vigueur de la loi fédérale intitulée "Electronic Signatures in Global and National Commerce Act", sans oublier le « Uniform Electronic Transactions Act », adopté par la commission d'uniformisation des droits étatiques américains ("National Conference of Commissioners on Uniform State Laws).

Le système légal en France est constitué par la loi du 13 mars 2000, qui reconnaît la valeur juridique de la signature électronique sous certaines conditions, complétée par le décret n° 2001-272 du 30 mars 2001, qui renvoie lui-même à un second décret du 18 avril 2002 et à un arrêté ministre de l'économie, des finances et de l'industrie du 31 mai 2002. Enfin, le projet de loi pour la confiance dans l'économie numérique comporte des dispositions concernant l'utilisation de la signature électronique dans les contrats dont l'écrit constitue une condition de validité, ce qui n'était pas prévu dans les textes actuellement en vigueur.

Avant d'examiner les différentes questions touchant la signature électronique et notamment les conditions de sa valeur probante, il convient de faire quelques remarques préliminaires sur le droit français de la preuve et son adaptation aux nouvelles technologies de l'information.

I. Les règles classiques du droit français de la preuve adaptées aux nouvelles technologies.

En droit français les règles de preuve diffèrent, selon que l'on se trouve dans le domaine commercial ou civil. En effet, l'article 109 du Code de commerce prévoit qu'« *A l'égard des commerçants, les actes de commerce peuvent se prouver par tous moyens à moins qu'il n'en soit autrement disposé par la loi* ». La règle vaut aussi bien, dans le cadre d'un acte mixte, entre un commerçant et un non-commerçant, à l'égard de la partie commerçante.

Dans les relations entre consommateurs, l'écrit est exigé pour les actes dont la valeur dépasse la somme de 800 euros (art. 1341 Code Civil et décret N° 2001-476 du 30 mai 2001)

C'est dans ce contexte de liberté que le juge français a reconnu à certaines conditions, une valeur probatoire à la signature électronique par utilisation d'un code confidentiel (affaire Créditas, 8 novembre 1989), à la production de télécopie ou encore à l'enregistrement télématique au moyen du Minitel.

Le système de la preuve libre s'applique également en droit pénal (système de l'intime conviction) et en droit administratif.

En revanche, le droit civil distingue la preuve des faits, qui relève de l'intime conviction du juge, de la preuve des actes juridiques, pour lesquels le principe est posé qu'un acte juridique ne peut se prouver que par écrit.

Dans le système de la preuve légale, les différents moyens de preuve n'ont pas la même force probante. L'écrit, sous forme d'acte authentique ou d'acte sous seing privé, c'est à dire signé par les parties l'importe sur les autres moyens de preuve (témoignage, présomption, aveu de la partie et serment).

La loi du 13 mars 2000 a modifié le droit français de la preuve, en admettant tout d'abord l'écrite électronique au rang des preuves littérales : "Lorsque la preuve est littérale, elle résulte d'une suite de lettres, de caractères, de chiffres ou de tout autre signe ou symbole doté d'une signification intelligible quel que soit leur support et leurs modalités de transmission" (art. 1316-1 C.Civ).

L'article 1316-3 prévoit que l'écrit sur support électronique est admis comme preuve au même rang et à la même force probante que l'écrit sur papier. S'il existe un conflit entre papier et immatériel, la loi prévoit que le juge doit trancher et régler les conflits de preuve, en déterminant le titre le plus vraisemblable, quel qu'en soit le support (article

1316-2 C.Civ). Le législateur affirme donc l'équivalence entre le papier et l'électronique.

L'art. 1317 du C.Civ modifié énonce, encore, que « Les actes authentiques peuvent désormais être établis par voie électronique ».

Pourtant, la loi du 13 mars 2000 ne concerne pas les actes juridiques pour lesquels l'écrit est requis à titre de validité. Ainsi, seuls les contrats dont l'écrit est une condition de preuve peuvent aujourd'hui être conclus sur Internet. Ceci va changer, avec l'adoption du projet de loi pour la confiance dans l'économie numérique, qui vient, avec son article 14, modifier à nouveau le code civil, en insérant un article 1369-1 qui prévoit que « lorsqu'un écrit est exigé pour la validité d'un acte juridique, celui-ci peut être établi, conservé sous forme électronique dans les conditions prévues aux articles 1316-1 et 1316-4 et, lorsqu'un acte authentique est requis, au second alinéa de l'article 1317 ». Certaines exceptions sont prévues, notamment en matière du droit de la famille et des successions ou encore en droit des sûretés.

Or, que l'écrit soit une condition de preuve ou de validité, celui-ci doit comporter des éléments qui servent à assurer la réalité du consentement des parties qui pourraient se trouver liées par cet écrit. Ces éléments ne sont d'autres que la signature des parties.

II. La signature électronique : conditions et modalités de sa valeur probante.

L'article 1316-4 de la loi du 13 mars 2000 dispose que « *La signature nécessaire à la perfection d'un acte juridique identifie celui qui l'appose. Elle manifeste le consentement des parties aux obligations qui découlent de cet acte. Quand elle est apposée par un officier public, elle confère l'authenticité à l'acte.* »

Cet article définit les deux fonctions essentielles de la signature : l'identification de l'auteur de l'acte et la manifestation de son adhésion au contenu de cet acte.

Le second alinéa du même article prévoit que "*Lorsqu'elle [la signature] est électronique, elle consiste en l'usage d'un****procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache****. La fiabilité de ce procédé est présumée jusqu'à preuve contraire, lorsque la signature électronique est créée, l'identité du signataire assurée et l'intégrité de l'acte garantie, dans des conditions fixées en Conseil d'Etat*".

La fiabilité du procédé de signature électronique est présumée jusqu'à preuve contraire, dès lors que **la signature est sécurisée**, qu'elle est établie à l'aide d'un **dispositif de création sécurisé** et que **le certificat est qualifié** (article 2 du décret du 30 mars 2001).

Si les conditions nécessaires à la présomption de fiabilité ne sont pas réalisées, la fiabilité du procédé devra être démontrée à la charge du signataire.

L'article 3 du décret du 30 mars 2001 présente les exigences que doit remplir le dispositif de création de signature électronique pour être présumé sécurisé. Il doit notamment :

- garantir que la signature électronique est liée au signataire ;

- permettre de créer la signature électronique par des moyens que le signataire puisse garder sous son contrôle exclusif ;

- garantir que la signature électronique lie les données auxquelles elle se rapporte de telle sorte que toute modification ultérieure de celles-ci soit détectable;

- garantir par les moyens techniques et procédures appropriées que les données utilisées pour la création de la signature électronique :

a. ne puissent se rencontrer qu'une seule fois et que leur confidentialité soit assurée,

b. ne puissent être trouvées par déduction et que la signature soit protégée contre toute falsification par les moyens techniques conformes à l'état de l'art,

c. puissent être protégées de manière fiables par le signataire légitime contre leur utilisation par des tiers ;

- ne doit pas modifier les données à signer ni empêcher que ces données soient soumises au signataire avant le processus de signature.

Les dispositifs sécurisés de création de signature électronique devront être certifiés conformes, soit par la DCSSI (Direction Centrale de la Sécurité des Systèmes d'Information) dans les conditions fixées par le décret n° 2002-535 du 18 avril 2002, soit par un organisme européen reconnu équivalent.

Enfin, le certificat électronique, quant à lui, ne peut être regardé comme qualifié que si :

- il comporte les éléments mentionnés à l'article 6-I du décret du 30 mars 2001 (2) ;

- et il est délivré par un prestataire de services de certification électronique répondant aux exigences de l'article 6-II du 30 mars 2001 (3)

(1) Voir notamment le rapport du Conseil d'Etat, Internet et les réseaux numériques, 1998.

(2) - Un certificat électronique qualifié doit comporter :

a) Une mention indiquant que ce certificat est délivré à titre de certificat électronique qualifié ;

b) L'identité du prestataire de services de certification électronique ainsi que l'Etat dans lequel il est établi ;

c) Le nom du signataire ou un pseudonyme, celui-ci devant alors être identifié comme tel ;

d) Le cas échéant, l'indication de la qualité du signataire en fonction de l'usage auquel le certificat électronique est destiné ;

e) Les données de vérification de signature électronique qui correspondent aux données de création de signature électronique ;

f) L'indication du début et de la fin de la période de validité du certificat électronique ;

g) Le code d'identité du certificat électronique ;

h) La signature électronique sécurisée du prestataire de services de certification électronique qui délivre le certificat électronique ;

i) Le cas échéant, les conditions d'utilisation du certificat électronique, notamment le montant maximum des transactions pour lesquelles

ce certificat peut être utilisé.

(3) Un prestataire de services de certification électronique doit satisfaire aux exigences suivantes :

a) Faire preuve de la fiabilité des services de certification électronique qu'il fournit ;

b) Assurer le fonctionnement, au profit des personnes auxquelles le certificat électronique est délivré, d'un service d'annuaire recensant les certificats électroniques des personnes qui en font la demande ;

c) Assurer le fonctionnement d'un service permettant à la personne à qui le certificat électronique a été délivré de révoquer sans délai et avec certitude ce certificat ;

d) Veiller à ce que la date et l'heure de délivrance et de révocation d'un certificat électronique puissent être déterminées avec précision ;

e) Employer du personnel ayant les connaissances, l'expérience et les qualifications nécessaires à la fourniture de services de certification électronique ;

f) Appliquer des procédures de sécurité appropriées ;

Pour la liste exhaustive voir art. 6-II du décret du 30 mars 2001.

10/04/2003

Le droit d'utiliser une marque n'est pas sans limite

- Auteur : **Webconseil** , *Société de conseil*
- Domaine : PROPRIETE_INTELLECTUELLE
- Sous thème : Droit_des_marques_et_des_brevets
- Ordre juridique :

Lorsqu'une entreprise bénéficie de l'autorisation d'utiliser une marque, cette entreprise dispose sur cette marque des prérogatives convenues avec le propriétaire de la marque concernée. Cela entraîne pour conséquence qu'elle ne peut outrepasser les droits qui lui ont été conférés par convention.

Pour ce qui concerne l'Internet, la problématique vient du fait que bon nombre de licences de marques n'ont pas envisagées l'exploitation sur le web.

La décision rendue par le TGI de Paris le 20 décembre 2002, publiée récemment, n'est pas novatrice dans ses motifs, mais elle permet de faire un point sur l'étendue des droits dont dispose le concessionnaire du droit d'utilisation d'une marque dans le cadre de l'utilisation de la marque sur Internet.

Dans cette affaire, un célèbre fabricant de voitures de luxe avait assigné pour contrefaçon de marque une société reconnue comme spécialiste de ce type de voitures, titulaire d'une autorisation d'utiliser la marque. Elle avait constaté que cette dernière utilisait le blason de sa marque en fond d'écran sur son site web. La demanderesse soutenait que si la société en question avait l'autorisation d'utiliser la marque pour illustrer son activité et informer les utilisateurs de son site, en aucun cas elle ne disposait de l'autorisation de reproduire le blason de la marque, en conséquence, la reproduction du blason était contrefaisante.

Le Tribunal a jugé dans cette affaire que si les deux sociétés avaient organisées l'utilisation de la célèbre marque, cette utilisation était limitée contractuellement et la reproduction du blason outrepassait les droits de la société utilisatrice et constituait donc une contrefaçon de marque.

Ce jugement nous rappelle donc qu'en matière d'utilisation de marques, les parties ne peuvent aller au-delà de ce qu'elles ont convenu contractuellement.

Pour en savoir plus: contact@webconseil.fr

07/04/2003

Internet sans fil : les nouveaux enjeux juridiques du Wi-Fi

- Auteur : **Me. Murielle-Isabelle Cahen ,** *Avocate*
- Domaine : COMMERCE_ELECTRONIQUE
- Sous thème : Droit_de_la_communication
- Ordre juridique :

Les réseaux locaux sans fil (WLAN ou RLR pour réseaux Radio Local Radioélectrique) utilisent les ondes radio-électriques permettant la transmission de données entre ordinateurs.

La plupart des technologies actuelles utilisent des fréquences de 2,4 Ghz, jusque-là réservées aux applications militaires, médicales et scientifiques, pour permettre à des appareils de communiquer sans fil par les ondes hertziennes.

Le standard dominant aujourd'hui est la norme 802.11b de l'IEEE (Institute of Electrical and Electronics Engineers), plus communément appelée "Wi-Fi" (Wireless Fidelity).

Wi-fi permet de créer de véritables réseaux locaux capables d'accueillir de très nombreux utilisateurs avec un débit de 11 Mbits/s pour une cellule Wi-fi.

L'intérêt de ce système c'est, entre autres, qu'il évite le câblage des bâtiments qui est coûteux, l'accès au réseau se faisant grâce à des antennes.

I. Le cadre réglementaire actuel d'exploitation des réseaux Wi-Fi

L'Autorité de Régulation des Télécommunications (ART) a rappelé, dans le cadre de sa décision du 23 mai 2001, les usages possibles des technologies de type Wi-Fi. Elle distingue selon que le réseau est destiné à une utilisation à l'intérieur ou à l'extérieur de bâtiments.

A. Utilisation à l'intérieur des bâtiments

Les entreprises, les collectivités territoriales ou les particuliers peuvent utiliser la technologie wi-fi pour installer un réseau à l'intérieur de leurs immeubles sous réserve des conditions de respecter les valeurs maximales de puissance rayonnée

La puissance maximale autorisée à l'intérieur des bâtiments est de 10mW pour l'ensemble de la bande 2,4 GHz (2400 MHz et 2483,5 MHz) et de 100mW pour les fréquences comprises entre 2446,5 MHz et 2483,5 MHz.

L'utilisation des fréquences 5150 MHz - 5350 MHz est autorisée à l'intérieur des bâtiments avec une puissance maximale de 200mW.

B. Utilisation à l'extérieur des bâtiments

La puissance maximale autorisée à l'extérieur des bâtiments est de 100mW, sur les propriétés privées ou sur le domaine privé des personnes publiques, pour les seules fréquences comprises entre 2446,5 Mhz - 2483,5 MHz. Cette utilisation reste soumise à une procédure d'autorisation préalable avec avis du Ministère de la défense.

L'utilisation à l'extérieur des bâtiments sur le domaine public n'est pas autorisée.

Pour résumer, les RLAN à l'extérieur des bâtiments et sur le domaine public sont interdits ; ils sont en revanche autorisés à l'intérieur des bâtiments et à l'extérieur tant qu'il s'agit d'un domaine privé et tant que les émetteurs respectent des limites de puissance.

II. Les nouvelles règles adoptées pour l'expérimentation des réseaux locaux radio-électriques (RLAN) ouverts au public

L'Autorité de Régulation des Télécommunications a adopté le 7 novembre 2002 les décisions permettant, à compter de janvier 2003 et dans 38 départements pilotes, l'utilisation de réseaux Wi-Fi pour la fourniture au public de services Internet haut débit, en particulier dans les lieux de fort passage du public (dits "hot spots") comme les gares, les aéroports, les centres d'affaires ou encore les hôtels. Au jour d'aujourd'hui le nombre de départements où l'exploitation de réseaux Wi-Fi est autorisée est 58.

Le même jour, l'ART a arrêté les lignes directrices fixant les conditions d'expérimentation de réseaux RLAN ouverts au public, sur la bande de fréquence des 2,4 GHz.

Ces expérimentations ne pourront être conduites qu'après la délivrance d'une autorisation, qui sera délivrée gratuitement, sur la base de l'article L.33-1 du code des postes et télécommunications pour une durée maximale de dix-huit mois.

III. Les enjeux juridiques du Wi-Fi

Le non-respect de l'ensemble de ces dispositions fait l'objet de sanctions prévues par le Code des Postes et des Télécommunications.

Ainsi, le fait d'établir ou de faire établir un réseau indépendant (de type Wi-Fi) sans autorisation ou le fait de le maintenir en violation d'une décision de suspension ou de retrait de cette autorisation est puni d'un emprisonnement de six mois et d'une amende de 30.000 euros (article L.39-1 alinéa 1 CPT)

Sont donc visés, aussi bien les installateurs que les entreprises qui ont souhaité l'installation de tels réseaux.

Il est également interdit de perturber, en utilisant une fréquence, un équipement ou une installation radioélectrique, dans des conditions non conformes aux dispositions de l'article L. 34-9 ou sans posséder l'autorisation prévue à l'article L. 89 ou en dehors des conditions réglementaires générales prévues à l'article L. 33-3, les émissions hertziennes d'un service autorisé (article L.39-1 alinéa 2 CPT)
L'utilisation du réseau Wi-Fi peut, par ailleurs, poser des problèmes tant techniques que juridiques, quant, notamment, à son niveau de sécurisation. En effet, un des inconvénients de la technologie Wi-Fi est la possibilité "d'écouter" les transmissions de données, notamment du fait d'une faille de sécurité dans la phase d'autorisation d'accès au réseau sans fil.

Bien que des nouveaux outils de sécurisation sont déjà en voie d'élaboration (par exemple remplacement du protocole à clé fixe appelé WEP par un nouveau système de chiffrement), des nouveaux types de piratage informatique sont susceptibles d'apparaître (1) .

1) En droit français, l'intrusion dans un système de traitement informatisé de données est réprimée par l'article L.323-1 du Nouveau code pénal qui prévoit, en effet, que « *le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni d'un an d'emprisonnement et de 15 000 euros d'amende* »