

**Rapport au ministre délégué à la Poste,
aux Télécommunications et à l'Espace
et au ministre de la Culture**

Internet

Enjeux juridiques

*Mission Interministérielle
sur l'Internet
présidée par
Isabelle Falque-Pierrotin,
assistée de
Nathalie Gautraud,
Gerulf Kinkelin,
Jacques Louvier,
Sophie Poitou*

16 mars 1996 - 16 juin 1996

Rapport officiel

Isabelle Falque-Pierrotin

© La **documentation** Française

*« En application de la loi
du 11 mars 1957
(art.41) et du code de la propriété
intellectuelle du 1^{er} juillet 1992,
toute reproduction partielle ou totale
à usage collectif de la présente
publication est strictement interdite
sans autorisation expresse de l'éditeur.
Il est rappelé à cet égard que l'usage
abusif et collectif de la photocopie
met en danger l'équilibre économique
des circuits du livre. »*

ISBN 2-11-003756-3
ISSN 0981-3764
DF 5-4104-4
Paris, 1997

Remerciements à tous les ministères, au Service juridique et technique de l'information et de la communication, et à la direction générale des Postes et des Télécommunications pour leur participation à l'élaboration de ce rapport.

**Le ministre délégué à la Poste,
aux Télécommunications
et à l'Espace**

n° 022798

Le ministre de la Culture

*Madame Isabelle Falque-Pierrotin
Maître des requêtes
Conseil d'État - Palais Royal
75100 Paris RP*

Paris le 29 février 1996

Madame,

Le développement international des réseaux et services d'information illustré par le développement d'Internet, pose un certain nombre d'interrogations dans l'opinion publique et de la part des opérateurs au regard de l'application de diverses réglementations nationales en matière de communication et de contenu des informations diffusées dans les services en ligne. Il est probable qu'une coordination internationale doive être mise en place pour répondre au défi posé par l'extra-territorialité de ces réseaux ou services.

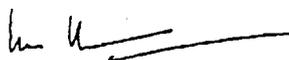
Afin de préparer les diverses initiatives que pourrait prendre le Gouvernement tant au plan national qu'international, nous souhaitons disposer d'une analyse sur les problèmes juridiques posés, sur les réponses actuellement en vigueur au niveau national et international et sur les adaptations nécessaires ou souhaitables.

Nous souhaitons vous confier la mission de présider un groupe de travail interministériel sur ce sujet, dont le secrétariat sera assuré par le SJTIC, et qui associera l'ensemble des services de l'État concernés, en particulier les ministères de la Culture, de l'Industrie (SERICS), des Télécommunications (DGPT°, de la Recherche, de la Justice, de l'Intérieur, de l'Économie (direction générale des Douanes, DGCDRF). Vous associerez également les présidents du CST et du CSA.

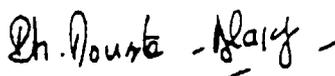
Vous prendrez l'attache de l'ensemble des acteurs économiques du secteur concerné, notamment des offreurs de service en ligne et des fournisseurs d'accès à Internet.

Votre mission aura pour objectif de proposer sous trois mois aux pouvoirs publics des mesures concrètes et des évolutions de la réglementation permettant, dans le strict respect de la liberté de communication, un niveau satisfaisant de garantie de l'ordre public, notamment vis-à-vis de la jeunesse et du consommateur.

Nous vous prions de croire, Madame, à l'assurance de nos respectueux hommages



François Fillon,
ministre délégué à la Poste,
aux Télécommunications
et à l'Espace



Philippe Douste-Blazy,
ministre de la Culture

Sommaire

Sommaire	5
Synthèse	7
Chapitre 1 Présentation du réseau Internet	15
Chapitre 2 Le droit positif	29
Chapitre 3 L'enseignement des exemples étrangers	55
Chapitre 4 Les propositions et les pistes de réflexion	73
Annexes	95
Annexe 1 Personnalités françaises auditionnées	97
Annexe 2 Situation de l'Internet en France et dans le monde	99
Annexe 3 Mission aux USA (6 au 9 mai 1996)	103
Annexe 4 Mission à Bruxelles (13 et 14 mai 1996)	129
Annexe 5 Recommandation du Conseil de l'Europe 95 R 13 (extraits)	135

Annexe 6	
Quelques exemples de « smileys »	141
Annexe 7	
Glossaire	143
Table des matières	147

Synthèse

Le développement des réseaux ouverts au public de type Internet est un phénomène majeur de cette fin de siècle : environ 40 millions de personnes raccordées, peut-être 200 millions en l'an 2000. Ces réseaux offrent des possibilités exceptionnelles d'échanges et de connaissance ; ils ouvrent de nouvelles routes de croissance et de création d'emplois ; ils peuvent être des outils de développement.

Dans le même temps, ils recèlent des risques de dérapage préjudiciables au respect des droits de la personne ; ils bouleversent les modes de fonctionnement traditionnels publics et privés et, en définitive, posent des questions nouvelles aux démocraties occidentales ; ces questions sont d'ordre déontologique, culturel, économique ou judiciaire ; elles sont, dans tous les cas, politiques car de leurs réponses dépendent beaucoup de nos choix dans les années à venir. Certains gouvernements redoutent ce monde nouveau qui se crée et la tentation se fait jour ici ou là de vouloir réguler l'Internet.

Dans ce contexte, le Gouvernement français, à l'initiative de Messieurs les ministres François Fillon et Philippe Douste-Blazy, a souhaité avoir une idée plus claire des outils juridiques actuels dont disposait la France par rapport à ce nouvel espace de communication et de service avec deux soucis majeurs, la protection de l'individu et de l'ordre public d'une part, la protection du consommateur, d'autre part. Une mission interministérielle, présidée par Madame Isabelle Falque-Pierrotin, maître des requêtes au Conseil d'État, a donc été mise en place le 16 mars 1996 avec pour objectif d'étudier le cadre législatif et réglementaire applicable à l'Internet et faire tout type de propositions d'adaptation ou de création de nouveaux textes.

Outre les contributions des différents ministères, plus de 40 professionnels ont été auditionnés ; une mission d'étude aux USA, marché plus avancé que le marché français et ayant déjà expérimenté quelques tentatives de régulation de l'Internet, est intervenue du 6 mai au 9 mai 1996 ; deux jours d'échanges avec les directions intéressées de la Commission européenne ont permis d'appréhender les positions communautaires ; enfin, le travail de la mission s'est enrichi des contributions

recueillies lors de la consultation électronique organisée par le chapitre français de l'Internet Society du 3 au 7 juin 1996.

Ce travail n'est évidemment qu'une première phase : l'on ne peut espérer, en à peine trois mois, faire un bilan exhaustif des questions posées par l'Internet ; il n'aborde pas certains sujets, pourtant essentiels, comme la protection du droit d'auteur ; en définitive, il vise plus à proposer une méthodologie de compréhension de l'Internet, une philosophie générale permettant ensuite, au cas par cas, de répondre aux problèmes posés.

Dès lors, quelles sont les principales conclusions ou propositions de la mission ?

Deux constats tout d'abord.

Il faut, en premier lieu, reconnaître le **caractère spécifique et profondément novateur** de l'Internet qui interdit toute transposition automatique de schémas préétablis ; l'Internet n'appartient ni au monde de la diffusion, ni à celui de la télématique ; il bouscule les définitions classiques du droit de la communication fondées sur la distinction entre correspondance privée et communication audiovisuelle ; c'est en réalité un monde d'utilisateurs, la plupart identifiés, qui passent par différents réseaux interconnectés, grâce à un protocole de communication non propriétaire, pour aller chercher l'information et le service dont ils ont besoin et les rapporter sur leurs ordinateurs. C'est cette logique de la demande qui fonde la sociologie du réseau et son évolution d'un monde clos de spécialistes et d'experts vers l'univers grand public et marchand qui se dessine aujourd'hui.

Il faut admettre, en deuxième lieu, que le **droit actuel assorti de quelques adaptations permet de répondre de façon relativement satisfaisante, sur le territoire national**, au souci de garanties juridiques évoqué plus haut ; il n'y a donc pas vide juridique mais plutôt pléthore de textes de droit commun applicables à l'Internet ; la *priorité* est donc de modifier certaines dispositions du droit positif pour les adapter aux services en ligne et de faire appliquer celui-ci ; en effet, le caractère transnational du réseau, la fugacité des contenus et l'évolution très rapide des techniques et des stratégies suscitent des difficultés spécifiques d'application du droit pénal ou commercial qu'il convient de résoudre, les principales questions étant celles de la détermination de la loi applicable, du régime de responsabilité et de la preuve.

Les constats étant posés : que peut faire la France ?

Quatre convictions méthodologiques tout d'abord :

* Une démarche purement nationale est illusoire.

* Une démarche graduelle et concertée semble nécessaire : l'instabilité des usages et des technologies rendant difficile l'appréhension de la matière juridique et la définition de catégories, l'arsenal juridique actuel permettant de garantir le respect, sur le territoire national, des

principales libertés individuelles et de l'ordre public, il convient, à court terme, d'analyser et de comprendre l'évolution de ce nouveau marché.

* Aucune démarche univoque ne sera efficace : il n'existe pas un remède, une solution unique pour répondre à la question du contrôle des contenus d'Internet ; à l'encadrement législatif et réglementaire doivent s'adjoindre des approches contractuelles, consensuelles, pédagogiques ou informationnelles ; ces approches correspondent à la sociologie du réseau et répondent, dans certains cas de façon plus efficace, à l'exigence de déontologie.

* Enfin, toute politique devra être orientée de façon positive, de façon offensive, pour le développement des services français sur Internet, plutôt que de se limiter à un arsenal défensif.

Ces principes méthodologiques posés, il importe de définir les objectifs de la France concernant l'Internet, ceux-ci conditionnant la mise en place de tout cadre de réglementation.

La **France** est à la **queue du peloton européen** et loin derrière les USA pour le développement du réseau ; compte tenu des potentialités exceptionnelles de celui-ci il faut combler ce retard et favoriser un développement rapide des services en ligne ; cependant ceux-ci ne constituent pas seulement le développement d'une nouvelle technologie ; leur succès, leur universalité en font un nouvel espace social justifiant l'élaboration de nouvelles règles de comportement, celles d'une « nouvelle civilité ». La tradition française est celle des valeurs humanistes, respectueuses des droits et 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.

Par rapport à ces objectifs, les propositions pourraient être les suivantes.

Préférer l'autocontrôle au contrôle *a priori*

Par sa structure d'interconnexion de plus de 70 000 réseaux et son mode de fonctionnement actuel, l'Internet semble difficilement s'inscrire dans un schéma de contrôle administré de type contrôle *a priori* : aucune autorité unique ne gère les flux de données, chacun peut à tout moment et de sa propre initiative être émetteur et récepteur d'informations ; celles-ci enfin ne connaissent pas les frontières. 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.

Dès lors l'objectif sera, d'une part, de mettre en place un contrôle *a posteriori* efficace en favorisant une **justice plus rapide et plus avertie** des enjeux de l'Internet ; une circulaire d'information pourrait être envoyée aux parquets et **une procédure nouvelle d'injonction** à l'encontre d'un serveur litigieux mise en place ; il paraît en outre souhaitable de constituer des forces d'enquêtes dédiées pour ce type

d'infraction. D'autre part, il faut favoriser l'autocontrôle des acteurs, soit par des **dispositifs de filtrage parental** ou de classification des services, soit par **l'élaboration de codes de déontologie** par les professionnels eux-mêmes fixant les règles de transparence, de responsabilité, de respect du cadre légal... De tels codes ont été adoptés par les fournisseurs d'accès en Grande-Bretagne ; ils doivent être repris par leurs homologues français et étendus aux éditeurs et commerçants électroniques et à tout offreur de service en ligne ; il faut enfin à travers les contrats passés entre le fournisseur d'accès et l'abonné et entre l'éditeur et le serveur d'hébergement favoriser l'adoption de **clauses types** garantissant le respect de l'individu et du consommateur.

Clarifier les responsabilités des acteurs

Cette question n'intéresse que les services en ligne de type audiovisuel et ne peut être résolue qu'en adoptant les deux postulats suivants : en premier lieu, **l'éditeur**, créateur de l'information mise en ligne est, en premier chef, **responsable** de celle-ci ; il faut donc toujours pouvoir l'identifier, l'anonymat de la consultation restant possible ; en deuxième lieu, l'on ne peut être responsable que de ce que l'on est capable de contrôler ce qui justifie l'exonération de la responsabilité pénale du fournisseur d'accès lorsque son intervention est purement technique. Dès lors, la seule alternative qui demeure est celle du choix entre le système de la responsabilité en cascade, adopté dans la presse ou l'audiovisuel, et un système de responsabilité de droit commun. A l'étude, il apparaît que cette alternative est, plus d'ordre politique que technique.

Compte tenu notamment des risques de délocalisation de l'activité en ligne en cas de présomption de responsabilité, même par défaut, du serveur hébergement, la mission recommande **l'adoption du système de droit commun**, plus simple et mieux adapté à la démarche empirique et graduelle que nécessite l'Internet.

Développer la coopération internationale

Celle-ci est décisive pour l'avenir de l'Internet dès lors que ce nouvel espace de communication dépasse les frontières nationales et remet en cause les bases territoriales d'application du droit.

Le cyber espace ne pourra réellement s'organiser et définir des règles communes de fonctionnement et de valeurs qu'à travers une négociation internationale sur l'édition électronique souhaitée au demeurant par la plupart des acteurs privés. Une telle négociation doit se traduire à la fois par une **entraide judiciaire accrue** et par l'adoption de principes communs non pas tant sur les contenus que sur la méthodologie de traitement des questions, notamment les questions de responsabilité et de loi applicable.

La coopération judiciaire pourrait conduire à la mise en application de certaines des propositions de la recommandation 95 R 13 du Conseil de l'Europe sur les procédures pénales liées à la technologie de l'information, l'élaboration d'un accord *ad hoc* d'extradition ou

d'entraide avec les USA où sont établis la plupart des serveurs, la création d'un mécanisme d'échange d'informations de type Interpol.

Si l'on souhaite approfondir la coopération, l'Union européenne est évidemment l'instance internationale privilégiée pour mettre en place une telle harmonisation ; une **directive sur les services en ligne** fixant les règles déontologiques minimales à respecter et adoptant le principe du droit du pays d'émission pour les États-membres, de réception pour les autres pourrait être élaboré ; les travaux d'autres instances internationales comme l'UIT, le Conseil de l'Europe, l'OCDE, doivent être poursuivis ; **les membres du G7**, enfin, **pourraient affirmer leur implication** dans l'enjeu que constitue aujourd'hui l'Internet et décider de se doter d'une cellule informelle de conseil et de recommandations afin d'éclairer leurs choix nationaux.

Il faut enfin développer la coopération internationale à travers les instances même de l'Internet et notamment l'Internet Law & Policy Task Force afin de susciter la création d'un lexique descriptif commun des services Web, lexique facilitant la transparence bénéfique à l'utilisateur ; afin également de travailler sur le nommage pour que celui-ci respecte le droit des marques et la possibilité pour chacun d'avoir une adresse mondiale pérenne.

Favoriser le développement du commerce électronique

Les textes actuels sur le commerce électronique semblent difficilement s'accorder, par le formalisme de la protection qu'ils prévoient, avec l'instantanéité du commerce électronique portant sur des biens immatériels ; la protection du consommateur s'organisera donc moins de façon centralisée et uniforme que par le **contrat** et des **dispositifs techniques adaptés** ; il faut donc favoriser l'élaboration de contrats-types par les organismes professionnels ou l'AFCEE, travailler pour la reconnaissance de la validité de la signature électronique, réfléchir à la mise en place d'une « **salestax** » levée sur le pays de destination afin de limiter l'évasion constatée aujourd'hui sur le commerce des biens immatériels ; il faut enfin admettre l'intervention d'un **tiers de confiance** dans la transaction, ce « cybernotaire » garantissant la solvabilité de l'acheteur et l'honorabilité du vendeur, assurant la prestation de confidentialité prévue par la nouvelle loi de réglementation des télécommunications, sécurisant la transaction et en gardant la trace...

Créer un organisme de veille, le Comité des services en ligne

Si la régulation administrative du réseau semble exclue, en revanche la création d'un organisme de **veille**, d'**analyse** et de **médiation** semble utile. Cet organisme conseillera le gouvernement sur les services en ligne et fera toute recommandation d'ordre déontologique ; il recevra les plaintes des utilisateurs et pourra, sur demande de ceux-ci ou du

gouvernement, donner des avis sur des sites litigieux, ces avis pouvant être versés dans une procédure pénale ; il jouera également un rôle de médiateur afin de limiter le recours aux procédures pénales ; le comité développera ses liens avec les instances internationales, publiques et privées, compétentes sur Internet. Sa structure sera légère, reposant sur les associations, les groupes de réflexion et les experts ; il 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 communication.

Favoriser l'information, la formation et la mobilisation des acteurs

Nouvelle forme de relation mondiale, d'intimité mondiale, l'Internet nécessite l'apprentissage d'une nouvelle civilité, correspondant au fonctionnement du réseau ; des campagnes d'information et de sensibilisation doivent donc être lancées, par les associations familiales notamment et un *Mémento des droits et obligations sur l'Internet* doit être édité par le Gouvernement ; le ministère de l'Éducation nationale, quant à lui, doit au plus vite inclure dans ses programmes un enseignement sur ces réseaux (l'Edunet), enseignement visant, outre à informer, à développer la pensée critique des enfants ; les municipalités devraient ouvrir des espaces gratuits de libre accès à l'Internet (Resothèques) pour familiariser les utilisateurs et donner accès à des informations institutionnelles ou de service public. Pourquoi ne pas imaginer enfin un numéro vert sur l'Internet ?

Outre cette pédagogie grand public, il faut former et mobiliser les administrations : un **outil interministériel de coordination et d'impulsion** semble nécessaire à la fois pour permettre à chaque département ministériel de répondre aux questions nouvelles posées par les réseaux en ligne mais aussi pour exploiter, à son profit, le bénéfice de ceux-ci. Cette délégation animera la politique gouvernementale concernant l'Internet et devra coordonner son action avec le comité des services en ligne centré sur une action plus déontologique et se faisant l'écho de la profession.

Enfin, le secteur privé doit se mobiliser à travers les ordres professionnels, chambres de commerce,... chaque secteur risquant de voir son fonctionnement profondément remis en cause par l'émergence de ces nouveaux réseaux.

Favoriser la présence française et francophone sur le réseau

Internet est aujourd'hui un réseau anglo-saxon : 80 % des serveurs sont nord-américains et 90 % des échanges se font en anglais. Outre sa traduction en termes économiques, un tel constat implique des choix de normalisation et de régulation ne correspondant pas nécessairement à l'approche française ou européenne et à ses valeurs. Il est donc vital d'être présent sur le réseau, dans les instances non gouvernementales

qui existent déjà et dans les discussions qui s'engagent. La meilleure manière de se défendre contre l'Internet, si danger il y a, est d'y être ! Pour cela, la France a un potentiel exceptionnel d'expérience et de compétence du fait du Minitel ; toute cette industrie doit au plus vite valoriser ses atouts sur l'Internet et développer de nouveaux services. Pour les utilisateurs français, un serveur français de qualité sera toujours plus attractif qu'un serveur étranger ; il faut donc que **notre industrie se mobilise sur les contenus et également sur les logiciels de réseaux**. En outre, il faut que la représentation française soit plus élevée qu'elle ne l'est actuellement dans les lieux où se discute l'évolution du réseaux : il n'y a aujourd'hui que cent français sur les cinq mille membres de l'Internet International Foundation et très peu dans des instances techniques (Internet Architecture Board et Internet Engineering Task Force) ou à l'Internet Society.

Enfin, il faut poursuivre la mise en place « **d'espaces francophones** » car ceux-ci sont le moyen de favoriser le respect des droits et libertés de la personne auxquelles nous sommes attachés ; renforcer également le rôle du français comme langue véhiculaire, de communication entre les internautes afin de dépasser le taux de 2 % des échanges en français actuellement enregistré.

Conclusion

Une partie de ces propositions a déjà été mise en application à travers les amendements gouvernementaux introduits dans la nouvelle loi sur la réglementation des télécommunications : il s'agit du principe du contrôle parental et de l'exonération de responsabilité pénale des fournisseurs d'accès sauf s'ils n'ont pas proposé à leurs abonnés de dispositifs de contrôle parental, s'ils ont donné accès à un service ayant reçu un avis négatif du Comité supérieur de la télématique (CST), ou s'ils donnent accès en toute connaissance de cause à un serveur litigieux.

Il faut poursuivre le travail. En matière juridique tout d'abord en étudiant les adaptations nécessaires à chacune des branches du droit ; peut-être serait-il opportun de lancer une réflexion sur le droit de la communication, jusqu'ici fondé sur les technologies et l'articuler autour de quelques grands concepts, communs à l'ensemble des supports. Il faut également poursuivre le travail d'ordre non juridique afin de tirer toutes les conséquences de cet espace nouveau de communication et de service mondial.

Ce monde fourmille de multiples initiatives et **échappe parfois à la logique cartésienne française**. Il est difficile à saisir et pour cela inquiète ; pourtant, en définitive, l'Internet c'est nous avec nos usages et nos besoins ; il n'y a donc pas de déterminisme de l'évolution du réseau dans un sens positif, porteur de tous les bienfaits, ou négatif, symbole de déviance. **Une complémentarité** doit donc être trouvée entre l'action légitime des gouvernements pour assurer à leurs nationaux une protection conforme à leurs valeurs et la mise en place, par le réseau lui-même, d'un mode de fonctionnement favorisant son développement.

Chapitre 1

Présentation du réseau Internet

Historique du réseau : de la recherche militaire au réseau international

L'origine de l'Internet se trouve dans une initiative de la défense américaine, prise au temps de la guerre froide, visant à réaliser un réseau de transmission de données grande distance entre différents centres, capable de résister à une destruction partielle.

Un tel réseau d'ordinateurs, Arpanet, fondé sur un maillage et la commutation de paquets de données, a été mis en oeuvre par des centres de recherche universitaire (UCLA, Stanford,...) grâce à des financements du ministère de la défense, puis étendu jusqu'à une quarantaine de sites au début des années 70. Pendant cette période, le réseau est présenté à d'autres pays occidentaux, et des travaux de normalisation (apparition puis diffusion des protocoles de communication TCP/IP, FTP...) et de déploiement sont entrepris, toujours sous l'égide de la défense américaine ; en 1979 l'Internet Configuration Control Board est ainsi créé.

En 1983, la Défense américaine isole la partie militaire du réseau (Milnet), ce qui permet à l'Arpanet de devenir l'épine dorsale du réseau Internet aux États-Unis. En 1990, l'Arpanet, désormais « civil », est intégré au réseau de la National Science Foundation, qui en financera le développement jusqu'en 1995.

En 1995, le réseau est remplacé par quelques grands réseaux interconnectés exploités par de grands opérateurs de télécommunication (MCI, Sprint,...), ce qui ouvre la voie à une dynamique de développement résolument commerciale.

Structure physique et logique du réseau

Ressources physiques de transport de l'information

L'Internet aujourd'hui repose sur une juxtaposition de réseaux de niveau différent :

* des réseaux continentaux servant de support à tous les autres réseaux (Ebone et Europanet pour l'Europe, MCInet, SPRINTlink, ANS-net-AOL et CERFnet aux États-Unis). L'interconnexion des différents réseaux supranationaux se fait, soit grâce à des organismes chargés de mettre en oeuvre l'échange de trafic entre grands réseaux (Global Internet Exchange - GIX), soit directement, par des accords d'échange direct entre opérateurs. Une telle démarche permet une croissance de « proche en proche », souple et décentralisée ;

* des réseaux de desserte ayant leur propre dynamique de développement, pouvant eux-mêmes être organisés en plusieurs strates : par exemple Renater en France et sa vingtaine de réseaux régionaux, ou les réseaux de fournisseurs d'accès internationaux, tel Oléane, qui opère sa propre liaison transatlantique et raccorde lui-même ses différentes plates-formes d'accès européennes par liaisons spécialisées ;

* des fournisseurs d'accès régionaux qui desservent leurs abonnés au moyen de plates-formes d'accès reliées aux réseaux téléphoniques locaux, interconnectées à l'Internet à travers des réseaux régionaux, voire leur propre réseau ;

* des réseaux fermés, internes ou propriétaires, donnant l'accès à l'Internet à leurs abonnés (services en ligne du type America on Line ou CompuServe), ou fonctionnant sur la base des outils de compatibilité de l'Internet (« Intranet » d'une entreprise, accompagné éventuellement d'une passerelle sécurisée (firewall) vers l'Internet) ; ces réseaux ne font pas partie intégrante du réseau, dans la mesure où leur interconnexion ne conduit pas nécessairement à acheminer le trafic général du réseau.

En définitive, la structure du réseau Internet est décentralisée, très répartie, et l'on a pu ainsi le dénommer « le Réseau des réseaux » ; les différents acteurs interagissent en permanence pour gérer la croissance du trafic de façon optimum et utiliser au mieux les ressources du réseau.

Outils logiques de transport de l'information : protocoles, adresses et noms

Le fondement de l'Internet est un langage de communication numérique (TCP/IP : Transmission Control Protocol over Internet Protocol) capable de faire passer sur tout type de réseau des données numériques, d'un expéditeur identifié vers un destinataire identifié.

L'Internet est constitué d'un ensemble de liaisons (réseau téléphonique, réseaux et liaisons spécialisés filaires, fibre optique ou satellite), de noeuds et de réseaux, qui constituent un maillage mondial par lequel transitent les communications entre les points terminaux.

Lorsqu'une communication est établie entre deux points, le message numérique à transférer est découpé en paquets avant d'être envoyé sur le réseau ; chaque paquet y transite de façon autonome, mais porte l'adresse au format IP du destinataire, et à chaque noeud, un routeur lit la destination et le retransmet sur les liaisons qui le rapprochent de la destination finale.

Ces routeurs se réfèrent aux tables de routage qu'ils mettent régulièrement à jour entre eux sur le réseau et à la connaissance instantanée qu'ils peuvent avoir de l'état du réseau et des liaisons qui le composent.

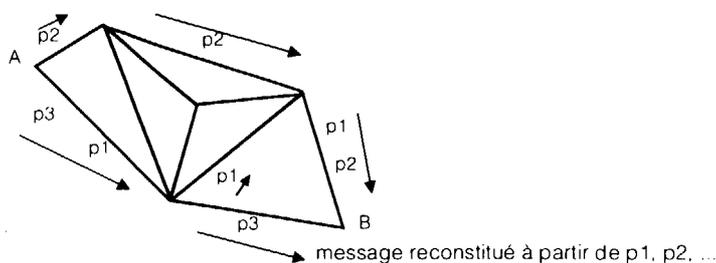
Ainsi, deux paquets successifs peuvent emprunter deux chemins différents selon les variations de l'état du trafic et des liaisons (rupture ou saturation d'une liaison, etc.) ; le message est reconstitué chez le destinataire à partir du réassemblage des paquets reçus.

C'est là la principale différence entre les communications sur l'Internet et les communications téléphoniques classiques : pour ces dernières, le réseau téléphonique établit, après que l'utilisateur ait tapé le numéro du destinataire, une liaison permanente qui restera active jusqu'au raccroché de l'une des deux extrémités ; ceci garantit une communication en temps réel, si l'on oublie les retards apportés par les éventuels tronçons satellitaires, mais la ressource n'est pas utilisée de manière optimale, puisque la consommation est la même quelle que soit la densité d'information véhiculée.

Sur l'Internet en revanche, la communication va emprunter une succession de liaisons dont aucune n'est réservée au début de la communication (à l'exception éventuellement de l'appel téléphonique entre l'abonné et le fournisseur d'accès). Chaque paquet est envoyé au noeud suivant en prenant place dans une file d'attente qui reçoit tous les paquets devant suivre la même direction. Ce mécanisme de fonctionnement assez simple est en revanche inadapté aux communications qui requièrent du temps réel (téléphone, vidéo en ligne) ; cependant, les évolutions futures des protocoles TCP/IP pourraient intégrer des mécanismes de réservation de capacité et de priorité pour ces nouveaux services (protocole IPV6).

Graphique 1

Message découpé chez A en paquets p1, p2... munis de l'adresse de B



De plus, si l'expéditeur et le destinataire connaissent *a priori* le point de départ et le point d'arrivée du message, et éventuellement le premier point d'accès au réseau, ils ne connaissent pas le chemin emprunté, car les paquets de données n'en gardent pas la mémoire. Certes, il existe des logiciels permettant de connaître la route suivie par des paquets, mais ils nécessitent une mise en oeuvre spécifique.

Inversement, les seuls points par lesquels transite nécessairement l'intégralité du contenu d'un message, en dehors des points terminaux, sont les points d'accès des usagers au réseau, la plate-forme d'interconnexion de l'offreur d'accès.

Les machines qui se connectent au réseau Internet ont une adresse IP qui peut être permanente, ou bien une adresse IP attribuée « à la volée » par le fournisseur d'accès pour la durée de la session de raccordement. Dans ce dernier cas, la traçabilité de la connexion s'arrête chez le fournisseur d'accès, mais ce dernier sait qui il raccorde.

La distribution des adresses (adresse informatique des machines raccordées selon le protocole IP) se fait par blocs de numéros négociés par les opérateurs techniques auprès d'organismes ayant reçu délégation de l'Internet Assigned Numbers Authority, le RIPE-NCC en Europe. C'est la saturation prévisible de ces adresses, au maximum de 32 bits aujourd'hui, qui va imposer une évolution du protocole IP.

L'adressage IP des machines est nécessaire mais non suffisant pour permettre de communiquer sur Internet. Le système d'accès aux ressources de l'Internet fonctionne selon une organisation syntaxique URL (Universal Resource Identifier) basée sur le nommage des machines (adresse IP et noms logiques, localisation physique des ressources,...) et sur les protocoles Internet (FTP, HTTP,...).

Les noms de « domaines » - du type « telecom. gov. fr » - sont attribués par zones géographiques et nécessitent une gestion fine, condition d'une croissance harmonieuse du réseau.

Chaque utilisateur a donc une adresse électronique de type Dupont compuserve. fr ; le signe signifiant « chez » et compuserve étant un exemple de fournisseur d'accès.

Le nommage des domaines est assuré par l'INTERNIC au niveau international qui peut déléguer sa compétence au réseau des NIC nationaux. Le NIC-France est géré par l'INRIA et attribue les noms de domaine indexés par « . fr » aux fournisseurs d'accès qui les sollicitent pour eux-mêmes ou pour le compte de leurs clients.

Services offerts par le réseau

Le réseau Internet offre aujourd'hui un grand nombre de services, qui ont en général été développés par des groupes d'utilisateurs (universités, etc.), lorsqu'ils en avaient besoin, puis repris et diffusés dans l'ensemble du réseau. Certains services sont déjà tombés en désuétude, d'autres apparaissent et connaissent une progression fulgurante.

Les services les plus répandus

Les principaux services qui touchent le grand public aujourd'hui sont :

- la messagerie électronique qui permet d'envoyer un message dans la boîte aux lettres (BAL) électronique d'un destinataire connecté à Internet ; il existe toute une gamme de possibilités : correspondance de personnes à personnes, correspondance de personnes à plusieurs personnes choisies par l'émetteur, correspondance vers une liste de personnes (list serv, majordomo) ;
- les forums de discussions ou news groups avec une BAL par groupe : il s'agit de groupes de discussions informels interconnectés sous formes de contributions personnelles accessibles en lecture pour tous. Trois modalités existent :
 - . *modéré* : sorte de courrier des lecteurs placé sur la surveillance d'une personne, le modérateur qui organise la discussion ;
 - . *semi-modéré* : sorte de tableau d'affichage ;
 - . *libre* : aucun contrôle, proche du dazibbao chinois.
- le transfert de fichier : il s'agit d'échange de données à distance ;
- le World Wide Web (W3) « la Toile », service permettant d'accéder à des serveurs multimédia interactifs, généralement limités pour l'instant à du texte, des images fixes, des liens directement accessibles avec d'autres pages et d'autres serveurs - liens dits hypertextes -, et des formulaires permettant de répondre au serveur. Ces attributs sont décrits grâce à la norme HTML, hypertext markup language.

Le World Wide Web a été inventé au CERN en Suisse en 1989, puis intégré dans une université américaine dans le logiciel Mosaic et racheté par la société Netscape, qui en diffuse depuis 1993 une version commerciale qui, de par sa convivialité sans précédent, est à l'origine de la croissance exponentielle du nombre de connections sur le réseau.

L'accès aux différents sites de l'Internet est possible soit en indiquant leur adresse, soit en envoyant des mots-clés à un « moteur de recherche » (lui-même sous forme d'un serveur W3 : Altavista, Lycos, Netscape...) qui renverra la liste des serveurs qu'il a pu identifier comme correspondant à la requête. Ce processus connaîtra sans doute d'importantes évolutions, d'une part en affinant la recherche pour limiter le nombre de réponses, d'autre part en donnant au moteur une valeur ajoutée éditoriale.

Les nouveaux services

Accessibles directement à partir des serveurs W3, de nouveaux services se développent rapidement :

- du son : les flashes de France Info sur le serveur de Radio France par exemple, mais ce service est déjà utilisé pour faire de la promotion d'oeuvres musicales, en général par extraits ;
- des images animées virtuelles (norme VRML : Virtual Reality Modeling Language permettant des images animées en 3 dimensions), qui sont à la base des « rencontres virtuelles », notamment chez Alphaworld : les parties participant à la rencontre commandent chacune un personnage qui les représente dans un décor virtuel où évoluent également les autres parties ;
- des images animées réelles (en temps différé sur le serveur de Sony, en temps réel sur le serveur de Vtcom), qui diffuse les nouvelles régionales de France 3 par une communication temps réel ;
- de la téléphonie vocale aujourd'hui en duplex (Netscape V3.0, Vocaltec...), service qui peut induire des changements fondamentaux dans l'économie des réseaux et la stratégie des opérateurs et ceci, indépendamment de l'ouverture des monopoles ;
- du téléchargement en ligne d'applications intégrées aux pages W3, grâce aux langages Java et Javascript, proches du langage C, mis gratuitement à disposition par Sun ; le champ des possibilités ouvertes est ici probablement extraordinaire, puisque l'on déporte une partie de l'application chez l'utilisateur, ce qui permet de conjuguer interactivité locale et distante ; les premières applications sont des jeux.

Enfin des services de commerce électronique sont disponibles sur le réseau, sous forme de supermarchés virtuels, de plates-formes de téléchargement de logiciels et d'images ; l'Internet peut donc générer du commerce à l'extérieur et à l'intérieur du réseau.

En ce qui concerne les nouvelles applications, l'Intranet mérite une mention particulière : il s'agit de réutiliser la technologie et les produits du monde Internet pour restructurer les réseaux internes des entreprises à moindre frais. En effet, les grandes sociétés ont développé au cours des années sur leurs différents sites des réseaux internes, qu'il s'agit aujourd'hui d'interconnecter ; ces réseaux étant souvent incompatibles, la solution la moins onéreuse est d'y implémenter les normes de l'Internet, ce qui les rend compatibles sans avoir à développer des passerelles spécifiques et coûteuses. Ceci permet également à l'entreprise de bénéficier en interne de tous les services standardisés sur l'Internet. On peut imaginer que cette évolution conduira à l'apparition de services très évolués dans l'entreprise (vidéoconférence, travail en groupe à distance), mettant à profit des liaisons internes dont la qualité sera facile à maîtriser et à faire évoluer.

Le mode d'évolution des normes de l'Internet

Fait de l'interconnexion de multiples réseaux, dépassant le territoire d'un État ou d'une entreprise, l'Internet s'est doté d'un organisme *sui generi*, capable de gérer son développement, accompagner son évolution et définir les grandes options techniques : l'Internet Society (ISOC) ; celui-ci se définit lui-même comme « une organisation globale et internationale destinée à promouvoir l'interconnexion ouverte des systèmes et l'Internet » ; tout utilisateur peut adhérer à l'ISOC, qui délègue à l'Internet Architecture Board (IAB) l'élaboration des normes techniques nécessaires à l'évolution du réseau.

Par ailleurs, l'ISOC fédère plusieurs comités spécialisés, dont les plus importants sont l'Internet Assigned Number Authority pour la gestion des numéros et des codes, responsables de l'attribution des adresses IP, l'Internet Engineering Task Force qui élabore des spécifications pour la mise en oeuvre des protocoles de la famille TCP/IP, et l'Internet Law and Policy Task Force, créée en 1996 pour examiner les questions juridiques et politiques posées par le réseau.

Le mode de normalisation et d'apparition des protocoles et des services sur l'Internet répond à une logique de simplicité et d'efficacité : les projets de nouveaux services sont soumis aux utilisateurs de manière totalement ouverte par leurs promoteurs, avec de préférence une première implémentation logicielle en libre-service ; l'évaluation se fait ainsi « sur pièces », et les concepteurs bénéficient d'un retour d'expérience large et rapide permettant d'améliorer le service ; si ce dernier répond à un besoin, une normalisation « de fait » s'effectue par prolifération naturelle et utilisation du logiciel, qui, s'il a suffisamment de succès, se retrouve intégré aux logiciels de navigation.

Pour des évolutions affectant l'ensemble des maillons du réseau (par exemple la migration prochaine vers une nouvelle version IPV6 capable de soutenir la croissance du réseau à long terme ; le changement de format des adresses nécessite une mise à jour profonde des routeurs et de leurs protocoles), la diffusion « naturelle » ne suffit pas ; dans ce cas, l'approche suivie est d'arriver au consensus sans recourir au vote, de manière à ne pas laisser se développer de rapports de force, dont le jeu affecterait la qualité du résultat obtenu en forçant des compromis politiques et non des optima techniques. La centralisation que requiert cette méthode relève plus de l'intermédiation de la part de l'Internet Architecture Board que de la conduite autoritaire.

Les acteurs en présence

Le monde de l'Internet est celui d'un fourmillement d'acteurs divers orchestré autour d'un acteur principal : l'utilisateur. Il n'existe toutefois pas de barrières entre ces différents acteurs.

Les opérateurs Internet

Il convient en premier lieu d'identifier les opérateurs directement reliés à Internet aux États-Unis et qui offrent une connexion à des clients ou à des fournisseurs de services. Ces opérateurs sont au nombre de quatre en France. Il s'agit :

- du groupement d'intérêt public RENATER (réseau national de télécommunications pour la technologie, l'enseignement et la recherche), créé en 1992 à l'initiative du ministère de l'enseignement supérieur, du Commissariat à l'énergie atomique (CEA), du Centre national d'études spatiales (CNES), du Centre national de la recherche scientifique (CNRS), d'Électricité de France et de l'Institut national de recherche en informatique et en automatique (INRIA). Le rôle de RENATER est d'interconnecter les établissements d'enseignement supérieur et les centres publics ou privés de recherche français ; le réseau s'est donc constitué en fédérant les réseaux universitaires au niveau local, puis les réseaux locaux à des réseaux régionaux connectés eux-mêmes au réseau national d'interconnexion qui permet, *via* Ebone, de se connecter avec les réseaux Internet européens et avec les États-Unis ;
- de Transpac, filiale de France Télécom ;
- d'Oléane et Eunet : il s'agit de sociétés privées qui se sont créées parallèlement et qui offrent des solutions de connexions permanentes à Internet soit directement au client, soit à des fournisseurs de services. Ces solutions sont relativement coûteuses et répondent à un usage intensif d'Internet. Ces opérateurs jouent le rôle de grossiste pour les fournisseurs de services qui y sont connectés.

Il convient en second lieu de mentionner les fournisseurs de services qui sont connectés à Transpac, Oléane ou RENATER. Leur activité consiste à louer de la bande passante à ces opérateurs reliés à Internet et à la sous-louer ensuite à leurs clients afin de les faire accéder de manière ponctuelle à Internet ; ces fournisseurs de services proposent à l'utilisateur final des solutions de connexion modestes convenant à un usage modéré du réseau sur des postes isolés. Au nombre de ces fournisseurs de services, on peut citer FranceNet, Calvacom, Worldnet... Ces fournisseurs de services peuvent également être des **serveurs d'hébergement**, voire même des éditeurs.

Si l'on considère la connexion d'un usager à un éditeur de contenu distant, celle-ci suppose la mise en place d'une chaîne d'opérateurs dont seuls ceux qui sont aux extrémités sont identifiés et ont une véritable relation contractuelle : l'utilisateur avec le fournisseur de service, l'éditeur de contenu avec le serveur distant ; seuls ces deux

opérateurs peuvent donc jouer un rôle dans le contrôle du contenu ; les opérateurs intermédiaires, quant à eux, n'entretiennent pas de relation avec les parties qu'ils contribuent à relier et n'ont, ni la vocation ni les moyens, de maîtriser les informations qui circulent entre eux.

Les éditeurs de contenu

L'Internet ne peut se développer et devenir un véritable marché que si le réseau est capable de fournir du contenu, des services à valeur ajoutée ou services d'information, et s'il existe des instruments ou des navigateurs capable de « piloter » l'utilisateur dans le dédale des informations qu'Internet met à sa disposition.

Le réseau n'est pas seulement un espace de communication mondiale, c'est également un lieu où des services sont offerts. Les éditeurs de contenus constituent donc une des richesses du réseau dans la mesure où ce sont eux qui créent, apportent l'information.

Le serveur d'hébergement

La machine où est stockée l'information qu'elle soit ou non éditée par le serveur lui-même (host).

L'utilisateur

C'est l'intervenant le plus important. L'Internet est un réseau d'utilisateurs, ceux-ci apportant le contenu, développant de nouveaux services et déterminant l'évolution du réseau par leurs nouvelles demandes ; les utilisateurs constituent l'essentiel de l'intelligence et de la dynamique du réseau, contrairement aux réseaux classiques de télécommunications et de diffusion dans lesquels les services sont centralisés et délivrés par le réseau lui-même ; ils ont même développé un langage propre de communication électronique utilisant les signes alphanumériques pour préciser la tonalité d'un message (smileys) ; les utilisateurs peuvent être éditeurs, ouvrir leur propre service Web grâce à la page d'accueil (home page) fournie par la plupart des fournisseurs de services.

Internet et la télématique anonyme

Si l'on veut comparer le fonctionnement d'Internet avec celui de la télématique du type Minitel, certaines différences apparaissent comme fondamentales :

- la télématique est anonyme, le réseau Internet ne l'est pas par construction. En effet, un serveur Minitel ignore, dans la majorité des cas, l'identité des utilisateurs qui le consultent, France Télécom servant de

filtre. À l'inverse, un serveur Internet connaît par définition l'adresse IP de l'utilisateur et son nom de domaine, sauf à procéder par artifices (serveur anonyme) ;

- la télématique est centralisée, nationale et fondée sur une norme et un réseau propriétaire ; le réseau Internet est décentralisé, international, repose sur un protocole non propriétaire et des technologies extrêmement évolutives ; d'où les discussions et les alliances autour du « network computer », un hypothétique micro-ordinateur (PC) à bas coût dédié à l'Internet ;
- alors que le terminal télématique est passif, l'Internet permet d'exploiter au mieux l'intelligence et la polyvalence multimédia croissante des terminaux PC, en particulier avec l'arrivée de Java qui permettra d'activer l'intelligence locale du terminal.

En revanche, l'Internet n'offre ni la simplicité d'utilisation ni un outil commercial équivalent au kiosque du Minitel ; en effet, s'il est possible de passer une commande sur Internet et de déclencher un paiement en ligne par carte bancaire, un tel mode de paiement n'est pas adapté à des petites sommes. Néanmoins, si une solution simple était trouvée, le commerce électronique sur Internet devrait corriger l'un des défauts majeurs du Minitel, à savoir une rémunération à la durée et non au contenu, logique qui a pu engendrer des effets pervers, notamment dans l'Audiotel.

Le kiosque micro proposé par France Télécom peut constituer une solution pour les services français, à condition toutefois que son fonctionnement se fasse dans la continuité de la connexion Internet pour l'utilisateur et qu'il ne limite pas l'intervention d'autres opérateurs (Oléane, opérateurs étrangers...).

L'état de l'Internet en France et les recommandations pour son développement

La pénétration de l'Internet en France présente de l'avis général un retard certain.

Si le monde universitaire est desservi de manière satisfaisante par Renater, le raccordement des entreprises, des administrations et des particuliers est encore peu développé.

Les chiffres⁽¹⁾ actuels, difficiles à établir, permettent d'estimer le nombre d'accédants à Internet à environ 400 000 à 500 000 pour le courrier électronique et à 100 000 à 150 000 pour le World Wide Web parmi lesquels 95 000 abonnés à titre individuel (foyers). Ce constat est

(1) Chiffres Médiangles, mai 1996.

cohérent avec la part de la France dans le parc total des serveurs : 1,4 % soit 150 000 « hosts » sur 7,5 millions dans le monde.

Ce constat n'est ni précis, ni définitif mais il constitue un ordre de grandeur permettant de situer la France dans le monde et en Europe ; en nombre de connexions elle se situe ainsi à la queue du peloton européen, derrière le Royaume-Uni, l'Allemagne, la Finlande, les Pays-Bas et la Suède et même encore derrière la Norvège, la Suisse, le Danemark, l'Autriche et la Belgique en connexion par habitant. Plus inquiétant encore : alors que l'Internet a un taux de croissance de 95 % en 1995 et l'Europe de plus de 101 %, la France n'a connu qu'une hausse de 47 % du réseau.

Plusieurs types d'explications sont avancées pour expliquer ces chiffres :

* La place occupée par le Minitel qui offre de nombreux services d'information et de commande. Les opérateurs de serveurs Minitel montrent un intérêt assez faible pour la migration vers un système qui n'a pas encore organisé de véritable remontée de ressources vers les éditeurs de services.

* Le faible équipement en micro-ordinateurs et en modems, équipements aujourd'hui indispensables pour accéder à l'Internet ; moins d'un foyer sur dix serait équipé, contre un foyer sur trois en Allemagne. Cependant, le rythme d'équipement semble en nette progression. Cette dynamique pourrait se révéler positive à terme, une grande part du parc étant alors composée d'équipements récents. De plus, on commence à voir apparaître sur le marché des terminaux dédiés à l'Internet à quelques milliers de francs (Oracle, Bandai...), qui pourraient stimuler le marché français au bon moment.

* L'offre de France Télécom est très récente (mai 1996 avec le lancement de Wanadoo et la possibilité d'accès au coût d'une communication locale sur toute la France) et de surcroît restreinte ; France Télécom n'a pas organisé de vrai lancement commercial grand public de ce produit, comparable par exemple au lancement du service « T on Line » par Deutsche Telekom il y a un an déjà. Certaines agences France Télécom ne semblent pas toutes connaître l'existence du produit. Les autres offreurs d'accès sont de taille plus modeste et ne disposent pas d'une infrastructure de distribution et d'une capacité d'investissement comparables.

* La trop faible présence de services à contenus français et francophones qui inciteraient le public français à se raccorder à l'Internet pour y accéder. Les administrations commencent à développer leur présence sur Internet - le Ministère de la Culture a été un précurseur, et l'ensemble des ministères doivent être connectés fin 1997. En revanche, de nombreuses sociétés françaises, dont certaines opèrent pourtant dans le domaine des télécommunications et de l'électronique, n'offrent pas de serveur sur le Web ou ouvrent des serveurs de bas niveau et peu réactualisés.

* Le coût des transmissions relativement plus élevé en France qu'à l'étranger : une liaison spécialisée Internet de 64 Kbits en France coûte ainsi le prix de 1,5 Mbits au USA et 128 Kbits en Angleterre.

Conclusion

Internet n'est donc pas un réel réseau physique mais plutôt une communauté d'ordinateurs qui communiquent entre eux, à travers les réseaux existants, grâce à un langage commun ; hérité à la fois de la guerre froide et du libéralisme post soixante huitard il se distingue du monde de la télématique mais aussi de celui de la diffusion audiovisuelle dès lors qu'il est fondé sur une logique de la demande de l'utilisateur final, sans préoccupation de rareté justifiant une réglementation des contenus ; il est en évolution constante et il passe ainsi aujourd'hui d'un monde non marchand et clos de spécialistes et d'initiés à un espace grand public de nature commerciale.

Ce changement de nature d'Internet, sa « socialisation » croissante ne manqueront pas de faire évoluer les règles de fonctionnement du réseau, à l'initiative des utilisateurs eux-mêmes ou des gouvernements.

La plupart d'entre eux, en effet, craignent le développement de ce nouvel espace de communication qui semble défier leur souveraineté nationale en véhiculant sans exclusive, toute information. La France a ainsi vu un premier recours se constituer par l'UEJF (Union des étudiants juifs de France) contre un groupe de fournisseurs d'accès au motif que ceux-ci avaient rendu accessibles des forums révisionnistes, condamnables en droit français ; de tels contenus litigieux sont cependant très minoritaires dans le réseau, peut être 3 % des services ; il est probable cependant que le développement du réseau rendra leur occurrence plus fréquente et que d'autres recours vont apparaître. Il importe donc, à ce stade, d'apprécier la validité et l'efficacité des outils juridiques français par rapport l'Internet avec deux préoccupations principales, le respect des droits de la personne, le respect des droits du consommateur.

Chapitre 2

Le droit positif

Le droit positif assure une protection suffisante qui doit être adaptée aux spécificités de l'Internet

L'analyse du droit positif français nous enseigne que la protection de la personne et du consommateur est assurée de façon satisfaisante par les règles du droit commun qui, pour la plupart s'appliquent à Internet ; le droit spécial, en revanche, de la diffusion ou de la télématique semble peu transposable à Internet qui procède d'une logique différente.

La spécificité de l'Internet

La spécificité de l'Internet repose sur l'imbrication des services et des acteurs qui rend difficile l'application *a priori* d'un régime juridique déterminé et global

Le droit de la communication est aujourd'hui principalement régi par la distinction entre les services de correspondance privée et les services audiovisuels.

Les premiers sont soumis au Code des postes et télécommunications et ne font l'objet d'aucun contrôle du contenu ; les seconds sont définis, par voie résiduelle, par la loi du 30 septembre 1986 et sont soumis à des obligations de contenu.

Les services sur Internet apparaissent comme hybrides.

Distinction communication audiovisuelle/correspondance privée

La communication audiovisuelle est définie à l'article 2 de la loi du 30 septembre 1986 comme « *la mise à disposition du public par tout 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* »

La loi du 10 juillet 1991 consacre le principe du secret des correspondances transmises par la voie des télécommunications, ce qui, au-delà des correspondances téléphoniques, englobe tous les réseaux et télécommunications, c'est-à-dire au sens de l'article L 32 du Code des postes et télécommunications « *toute transmission, émission ou réception de signaux, d'écrits, d'images, de sons ou de renseignements de toute nature par fil optique, radioélectricité ou autres systèmes électromagnétiques* ».

Il n'existe pas de définition légale de la correspondance privée, elle doit cependant être distinguée de la notion de lettre postale (document actuel et personnel). La circulaire du 17 février 1988 relative aux services télématiques est venue préciser « il y a correspondance privée lorsque le message est exclusivement destiné à une (ou plusieurs) personne physique ou morale, déterminée ou individualisée.

À l'inverse, il y a communication audiovisuelle lorsque :

- le message est destiné indifféremment au public ou à des catégories de public, c'est à dire un ensemble d'individus indifférenciés, sans que son contenu soit fonction de considérations fondées sur la personne ;
- le message transmis est à l'origine mis à la disposition de tous les usagers du service, à titre onéreux ou gratuit «.

Cette circulaire énumère une série de services de communication audiovisuelle : services télématiques interactifs, services télématiques de presse, services de messageries par petites annonces, services téléphoniques mettant à disposition du public des messages préenregistrés, services d'informations téléphonées.

Elle prévoit également que le caractère mixte des informations circulant sur les réseaux n'empêche pas la détermination de leur régime juridique. Il suffit dans ce cas que le contenu du service relève en partie de la communication audiovisuelle pour que le service soit soumis au régime de celle-ci en matière de déclaration.

Il reste que la frontière entre communication publique et correspondance privée est parfois difficile à établir. Il s'avère parfois délicat de circonscrire la notion de public ou de catégorie de public. Au delà du caractère nominatif ou non du message, le critère semble être celui de l'aptitude du message à être adressé à tout intéressé ou capté par celui-ci et en particulier à des personnes qui n'avaient aucun lien préalable entre elles.

Le Conseil d'État (29 mai 1991, *Fédération nationale des radio répondeurs*) a jugé que « les services de téléconvivialité permettant l'échange d'informations ou de messages entre utilisateurs sur le réseau téléphonique ne constituent pas des services de communication audiovisuelle, au sens de la loi du 30 septembre 1986 ».

Selon la cour d'appel de Metz (arrêt du 18 juillet 1980) « pour que la communication soit considérée comme privée, il faut non seulement que l'appel soit personnel, libre et privé, mais encore que l'ensemble de

l'échange téléphonique le soit, c'est-à-dire ne présente aucune volonté positive et formelle de porter un acte de communication au public ».

Cette définition inclut donc les opérations de téléconsultation bancaire ou les services de télachat et de télétraitement (réservation de places, billets de transport...) qui impliquent des relations personnalisées entre les correspondants avec envoi d'informations nominatives et confidentielles (numéro de carte bancaire).

Il convient également de se référer aux dispositions prévues par l'article 23 de la loi du 29 juillet 1881 sur la publicité des délits.

La poursuite des délits prévus par la loi de 1881 requiert l'existence d'une certaine publicité. Il doit cependant au préalable être précisé que certaines publications, purement intérieures à un groupe, peuvent contenir des imputations qui ne sont pas réputées publiques mais elles peuvent néanmoins faire l'objet de poursuites prévues par les articles R 621-1 et 621-2 du Code pénal (diffamations non publiques).

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 proférés 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 autre moyen de communication audiovisuelle, auront directement provoqué l'auteur à commettre ladite action* ».

L'ensemble des moyens envisagés visent un grand nombre de formes d'expression. De ce fait, avant que la loi du 13 décembre 1985 n'ajoute le terme de « tout moyen de communication audiovisuelle », les juges avaient appliqué la loi au cinéma, au téléphone ou à la radio.

Au-delà de la nature même des messages, l'article 23 exige que les paroles, cris ou menaces aient été proférés dans des lieux ou réunions publics. Il convient de distinguer les lieux publics par nature des lieux publics par destination : les uns sont ouverts à tous d'une manière permanente sans aucune condition particulière d'accès mais avec l'intention de se faire entendre par le public ; les seconds sont accessibles à tous ceux qui veulent y pénétrer sous certaines conditions (billet d'entrée...).

On remarquera ici l'intérêt de cette distinction pour les services d'Internet accessibles par le biais d'un mot de passe ou bien encore d'un abonnement, la condition d'entrée n'excluant pas la qualification publique du service.

Dans le cadre de la loi de 1881, la réunion publique relève d'une acception large dont la jurisprudence détermine les critères de façon assez aléatoire. La notion est tributaire du nombre de personnes qui y participent, des conditions d'admission et de tenue de la réunion ainsi que de la nature des relations existant entre les participants. Le critère du nombre de participants ne suffit pas à apprécier la nature publique ou non d'une réunion. Les conditions d'admission doivent permettre d'identifier

les groupements privés dès lors qu'une personne étrangère n'a pu s'y infiltrer. Ainsi, un conseil d'administration ou un comité d'entreprise sont considérés comme des réunions privées en raison du nombre limité de ceux qui y sont invités et des conditions propres pour y assister.

Selon un raisonnement analogue, les *forums de discussion* qui invitent un groupe de personnes à échanger leurs opinions sur des sujets donnés conserverait un caractère public dans la mesure où les conditions d'admission sont assez libres et regroupent des personnes qui n'avaient pas de lien préalable entre elles. Ils ne pourraient être assimilés à des « réunions privées » sauf si un modérateur fait le tri préalable des messages et fixe la ligne éditoriale des discussions.

Il convient également de tenir compte du critère de la **communauté d'intérêts** sur lequel se fonde la jurisprudence pour affirmer qu'un groupe de personnes ne constitue pas un public au sens de l'article 23. La jurisprudence semble dominée par les critères de communion de pensée ou de convergence d'intérêts matériels. Ainsi, le personnel d'une entreprise ne constitue pas un public au sens de l'article 23 (Cass. Crim., 4 décembre 1973), alors que les membres de la police nationale ou les membres d'une association (Cass. crim. 15 juillet 1981) représentent une communauté d'intérêts.

Toutefois, une réunion demeure privée dans la mesure où les propos tenus ne tombent pas dans l'oreille d'un public inconnu et imprévisible. Cependant, certaines réunions privées regroupent des personnes qui ne se connaissent guère (grandes associations par exemple) et les personnes n'ont entre elles pas davantage de relations que les membres d'une réunion publique.

En conséquence, le simple regroupement de plusieurs personnes sur un même serveur autour d'un thème donné ne devrait pas suffire à caractériser une « communauté d'intérêts ».

Par ailleurs, l'élément de publicité résulte des personnes atteintes et non nécessairement du lieu où elles se trouvent. La publicité résulte de la mise en contact avec le public par vente, mise en vente ou distribution. Alors que la vente résulte d'un seul acte, la distribution exige que l'on ait touché un certain nombre d'individus autrement qu'à titre confidentiel en portant, envoyant ou donnant l'écrit ou l'image. La jurisprudence n'écarte la publicité résultant d'une distribution par envoi que si les destinataires sont déterminés et limités.

Ainsi, les messageries électroniques reliant des personnes d'une même entreprise ne constituerait pas un mode de publicité. On peut en revanche s'interroger sur la qualification d'acte de distribution dans le cas des listes de diffusion spécialisées sur Internet pour des messages concernant un sujet particulier.

En ce qui concerne le terme de « communication audiovisuelle » de l'article 23 de la loi de 1881, il convient de rappeler que la loi ne s'enferme pas dans une description des modalités techniques de la transmission des paroles ou des images. Destinées à être entendues de

tous, les émissions de radio ou de télévision ont un caractère public, il en va *a priori* de même pour un ordinateur individuel. Même si la diffusion a lieu dans des endroits où le public n'a pas librement accès, l'infraction repose davantage sur la publicité des propos que sur celle des lieux. Le fait que la diffusion se fasse en domicile privé importe peu, le délit étant accompli dans tous les lieux où les émissions ou messages ont pu être reçus.

Il importe que les paroles aient été entendues par n'importe qui et qu'en les proférant, l'auteur sache qu'il pouvait être compris de tous.

Enfin, la jurisprudence analyse la condition de publicité sous l'angle de l'intention. L'auteur peut en effet transformer la nature privée d'un écrit en caractère public et inversement.

Les écrits et dessins privés, comme les autres formes d'expression de même nature, sont destinés à rester ignorés du plus grand nombre et possèdent de ce fait un caractère confidentiel qui les écartent *a priori* des effets de la loi de 1881. Il convient de distinguer les véritables modes d'expression confidentiels des moyens de diffusion semi-publics qui peuvent donner à l'expression un caractère répréhensible. Ainsi, dans le cas de lettres circulaires adressées à un nombre indéterminé de personnes bien que portant la mention « personnel », la CA de Paris a jugé que « pour déterminer le caractère public d'un écrit, il doit être tenu compte de la présentation et du contenu de cet écrit ».

Conclusion

Il ressort de cette analyse que les critères légaux, réglementaires et jurisprudentiels rendront difficiles une segmentation *a priori* des services offerts sur Internet en deux blocs : communication audiovisuelle et correspondance privée ; la plupart des services sont hybrides et l'on passe indifféremment de l'une à l'autre ; en outre un même service (e-mail par exemple) peut-être public ou privé selon les circonstances. Il appartiendra donc au juge, en tant que de besoin, de qualifier les services compte tenu des principes évoqués plus haut.

La délicate application à l'Internet

La qualification des services est important puisqu'elle va déterminer le régime juridique applicable des services et partant des acteurs de l'Internet.

En tant que service audiovisuel utilisant un réseau de télécommunication

Le régime juridique applicable aux services mis à la disposition du public varie en fonction des services et des supports. La loi du 30 septembre 1986 relative à la liberté de communication audiovisuelle a mis en place deux régimes, un d'autorisation et un autre de déclaration.

Les articles 28, 29, 30 et 31 de la loi de 1986 prévoient que les services de radio et de télévision utilisant des fréquences hertziennes sont soumis à autorisation et conventionnement du Conseil supérieur de l'audiovisuel.

Si ces mêmes services sont distribués sur le câble, ils sont soumis à conventionnement (article 34-1), le cablo-opérateur étant autorisé (article 34).

Si de tels services étaient distribués sur des réseaux autres que des réseaux câblés ou hertziens (réseaux de télécommunication), ils seraient soumis à l'article 43 de la loi du 30 septembre 1986.

L'article 43 de la loi du 30 septembre 1986 prévoit que les services de communication audiovisuelle autre que les services prévus aux chapitres I (télévision et radio utilisant la voie hertzienne) et II (télévision et radio distribuées par câble) sont soumis à déclaration préalable. Une circulaire du 17 février 1988 est venue préciser quels étaient les services visés par l'article 43.

Les dispositions de cet article ont vocation à s'appliquer aux services en ligne de communication au public de type Internet.

Ainsi, tout service visé par cet article et utilisant les réseaux de télécommunication doit déposer une déclaration auprès du procureur de la République. Il doit être porté à la connaissance des utilisateurs les éléments d'identification de l'exploitant du service (nom, prénoms ou siège social de l'exploitant, nom du directeur de publication, liste des publications).

La plupart des fournisseurs de services ou des éditeurs de contenu français ne connaissent pas cette obligation de formalités légales qui s'appliquent même aux pages d'accueil des utilisateurs (home page).

Outre cette obligation de déclaration préalable, les acteurs de l'Internet sont amenés à contracter avec les opérateurs de télécommunication pour utiliser les réseaux de télécommunications.

En effet, la réglementation prévoit des régimes distincts pour trois grandes catégories de service fournis au public :

- la fourniture du service téléphonique, entre points fixes, est réservée à l'exploitant public ;
- la fourniture de services-supports⁽¹⁾, et notamment l'utilisation de liaisons louées, est autorisée de plein droit pour l'exploitant public dans des conditions fixées par son cahier des charges et autorisée pour les autres personnes ;
- la fourniture de services à valeur ajoutée sur le réseau commuté est libre ; s'ils sont fournis à partir de liaisons louées, ils sont soumis soit à

(1) Il s'agit de services dont l'objet est d'acheminer des signaux entre les points de terminaison d'un réseau sans faire subir à ces signaux des traitements autres que ceux nécessaires à leur transmission, leur acheminement et au contrôle de ces fonctions.

déclaration préalable, soit à autorisation, selon la capacité d'accès aux liaisons louées.

Les fournisseurs d'accès à Internet peuvent s'adresser à l'une des dix sociétés autorisées à fournir des liaisons louées : Transpac, Sprint International, Compagnie Générale de Vidéo-communication, British Telecom France, SIRIS, SITA, Air France, Axone, Fax Link et La Poste.

Les services disponibles sur Internet correspondent à la fois à des services-supports (simple transfert de fichiers) et à des services à valeur ajoutée (messageries, news, etc.); étant fournis au public et utilisant des liaisons louées, ces services doivent être autorisés et/ou déclarés, conformément aux articles L 34-2 et L 34-5 du Code des postes et télécommunications.

La future loi de réglementation des télécommunications va modifier ce schéma :

- la fourniture du service téléphonique va être autorisée à compter du 1^{er} janvier 1998 ; sous réserve de répondre à la définition du service téléphonique au public, tout fournisseur de service téléphonique via Internet devra être également autorisé ;
- les services-supports et les services à valeur ajoutée seront libres, sous réserve du respect des exigences essentielles (sécurité des usagers et du personnel des exploitants de réseaux de télécommunications, protection des réseaux, interopérabilité des services et des équipements) et des prescriptions exigées par la défense et la sécurité publique. Ces services restent toutefois soumis à autorisation s'ils utilisent des fréquences hertziennes et à déclaration pour les réseaux câblés.

En tant que service dont la nature est de la correspondance privée

Les correspondances privées sont secrètes et ce caractère protégé. Mais il est possible de renforcer la confidentialité en utilisant la cryptologie.

Le respect du secret est principalement garanti par des dispositions pénales.

La loi du 10 juillet 1991 relative au secret des correspondances émises par voie de télécommunications, qui s'inspire des prescriptions de la convention européenne des droits de l'homme, a pour but de protéger les libertés individuelles par la garantie du secret des correspondances émises par la voie des télécommunication et d'éviter que l'autorité publique porte atteinte à ce secret en dehors des seuls cas de nécessité prévus par la loi.

L'article 226-15 du Code pénal réprime d'une peine délictuelle d'un an d'emprisonnement et de 300 000 francs d'amende « 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 ».

La même peine est encourue pour 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 ».

La notion de « correspondances émises par la voie des télécommunications » définit le champ d'application de la loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances. L'article 1 de ladite loi dispose en effet que le « secret des correspondances émises par la voie des télécommunications est garanti par la loi ».

Or, il ressort clairement, aussi bien du rapport de la commission des lois de l'Assemblée nationale (rapport Massot pages 34 à 36), que des débats au Sénat (débat JO du 26 juin 1991, pages 2070 et 2071), que ce terme vise non seulement les seules communications téléphoniques mais aussi tous les modes de transmission de données (textes, d'images et de sons) dès lors que ceux-ci recourent aux procédés de télécommunications.

Le ministre de la justice a précisé lors de ces débats que le terme de « correspondance » devait être entendu au sens de l'article 8 de la convention européenne des droits de l'homme, à savoir comme une communication d'une personne à une autre.

Il convient de considérer que l'article 226-15 du Code pénal s'applique aux utilisations à des fins de correspondance privée des réseaux et services de l'Internet.

Deux types d'interceptions sont légalement possibles :

- les interceptions judiciaires,
- les interceptions administratives.

Les dispositions relatives aux interceptions judiciaires incluses dans le titre premier de la loi du 10 juillet 1991, sont destinées à s'insérer dans le Code de procédure pénale aux articles 100 à 100-7.

L'article 100 définit le cadre juridique dans lequel peuvent être ordonnées des interceptions de correspondances émises par la voie des télécommunications. Il prévoit notamment que les écoutes judiciaires ne peuvent intervenir que dans le cadre d'une information judiciaire et ne doivent être autorisées qu'en cas d'infraction présentant « un certain degré de gravité », c'est-à-dire lorsque la peine encourue est égale ou supérieure à deux ans d'emprisonnement. La décision d'interception doit être écrite. Elle n'a pas de caractère juridictionnel et n'est susceptible d'aucun recours.

Les dispositions du titre II de la loi visent à définir le cadre juridique dans lequel les pouvoirs publics peuvent, à titre exceptionnel, procéder à des écoutes administratives appelées « interceptions de sécurité ». Cette catégorie d'écoutes doit se fonder sur des motifs légaux d'interception définis de façon limitative. Aux termes de l'article 3 de la loi, les écoutes administratives doivent en effet, avoir pour seul objet de :

« ... rechercher les renseignements intéressant 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. »

La cryptologie vise à transformer, à l'aide de convention secrète, des informations ou des signaux clairs en informations ou signaux inintelligibles pour des tiers ou à réaliser l'opération inverse à l'aide de moyens logiciels ou matériels conçus à cet effet.

Le régime de cryptologie est défini par l'article 28 de la loi du 29 décembre 1990 sur la réglementation des télécommunications, modifiée prochainement par l'article 12 de la nouvelle loi de réglementation des télécommunications.

Cet article établit la liberté complète d'utilisation de moyens de prestations de cryptologie pour les fonctions d'authentification et d'intégrité, et la liberté pour les fonctions de confidentialité, à condition que ces dernières utilisent des conventions secrètes gérées par les organismes agréés par les pouvoirs publics (tiers de confiance).

Seule l'utilisation de moyens ou de prestations de cryptologie pour assurer des fonctions de confidentialité utilisant des conventions secrètes non gérées par ces tiers de confiance reste soumise à autorisation du Premier ministre.

On est donc passé du principe de déclaration prévu par la loi de 1990 au principe de liberté d'utilisation, le régime d'autorisation restant l'exception.

L'exportation reste, quant à elle, soumise à autorisation dès lors qu'il s'agit de moyens ou de prestations de cryptologie utilisés pour assurer des fonctions de confidentialité. Les tiers de confiance nationaux qui se mettront en place se rapprocheront sans doute pour proposer des prestations de confidentialité sur des communications transfrontalières.

Le dispositif législatif actuel

Le dispositif législatif actuel est suffisant pour sanctionner sur le territoire la plupart des infractions concernant la protection des personnes, des consommateurs et des données.

Les dispositions sanctionnant les atteintes à la vie privée

La protection civile repose sur la combinaison des articles 9 et 1382 et 1383 du Code civil.

Ces dispositions permettent à la fois au juge civil de prononcer toutes mesures propres à faire cesser l'atteinte à l'intimité de la vie privée (article 9 alinéa 2) et de décider, le cas échéant, d'une réparation du préjudice occasionné par l'auteur de l'atteinte (articles 1382 et 1383).

Il convient d'insister sur le caractère très souple et très complet de ce dispositif eu égard aux applications qu'en fait la jurisprudence :

- en l'absence d'une définition légale de la vie privée, délimitation de celle-ci à partir des éléments retenus par les tribunaux comme en faisant partie ;
- possibilité de sanctionner, quel que soit le support technique ayant servi à l'atteinte, des formes très diverses d'immixtion dans la vie privée ou de divulgation des éléments de celle-ci ;
- rapidité et diversité des mesures pouvant être prises pour prévenir ou faire cesser l'atteinte, celles-ci devant toutefois être proportionnées à la gravité du trouble ;
- flexibilité de la notion de faute (faute intentionnelle ou imprudente, fait positif ou abstention) ;
- pouvoir souverain des juges du fond quant à la nature et au montant de la réparation.

Il ne fait aucun doute que la jurisprudence développée sur le fondement de l'article 9 du Code civil puisse permettre, sur la base du maintien des textes actuels, d'appréhender les atteintes à la vie privée résultant de l'emploi des techniques de transmission et de stockage de l'information propres aux réseaux multimédias.

L'article 226-1 du Code pénal réprime « le fait, au moyen d'un procédé quelconque, de porter atteinte volontairement à l'intimité de la vie privée d'autrui » en captant, fixant, enregistrant ou transmettant, sans le consentement de la personne ses paroles ou son image.

Par ailleurs, l'article 226-2 réprime la conservation ou la diffusion de ces documents ou enregistrements.

Il apparaît que ces dispositions réprimant la captation et la divulgation illicite de l'image ou des paroles d'une personne sont, sous réserve de l'interprétation souveraine des tribunaux, susceptibles de s'appliquer à ceux des réseaux et services d'information et à celles des applications d'Internet qui gèrent des documents multimédias.

Il en va de même de l'article 226-8 du Code pénal, lequel réprime la publication non autorisée, par quelle que voie que ce soit, de montages réalisés avec les paroles ou l'image d'une personne.

Il convient cependant d'observer que ces dispositions ont été jusqu'à présent peu appliquées, les victimes préférant agir sur le fondement de l'article 9 du Code civil.

L'article 226-13 du Code pénal, réprimant les atteintes au secret professionnel, permet d'incriminer la « révélation d'une information à caractère secret », quels que soient le support et les moyens utilisés pour celle-ci.

Ne peuvent cependant commettre une telle infraction en qualité d'auteurs principaux que des personnes qui sont dépositaires d'une information à caractère secret soit par état ou par profession soit en raison d'une fonction ou d'une mission temporaire.

Il y a lieu, en revanche, de noter que la protection assurée par l'article 226-13 du Code pénal est susceptible, sous certaines conditions, d'être étendue au delà des personnes concernées par l'obligation de secret professionnel.

Il peut en aller ainsi dans l'hypothèse du recel (art. 321-1 du Code pénal), celui-ci pouvant porter sur des documents ou des données frauduleusement communiqués à un tiers par l'auteur de l'infraction.

Il en irait de même dans une hypothèse de complicité (art. 121-7 du Code pénal) qui serait ainsi réalisée en cas de fourniture des moyens servant à la divulgation d'une information couverte par le secret professionnel, si toutefois cette assistance résulte d'actes antérieurs ou concomitants au fait principal.

Compte tenu de ces rappels, il apparaît que le tenancier du cybercafé de Besançon, dans l'affaire *Miterrand CI Plon et Gubler*, aurait pu être poursuivi pour complicité et recel de violation de secret professionnel et atteinte à la vie privée.

Les dispositions protégeant les mineurs

Il existe des dispositions non pénales protégeant les mineurs

La responsabilité de l'éducation des enfants appartient en premier lieu aux parents. Cette mission emporte celle de contrôler les sites qu'ils visitent sur l'Internet.

En effet, l'article 371-2 du Code civil dispose que l'autorité parentale appartient aux pères et mères pour protéger l'enfant dans sa sécurité, sa santé et sa moralité. Cet article ajoute qu'ils ont à son égard droit et devoir de garde, de surveillance et d'éducation.

L'autorité parentale permet aux parents de prendre toutes mesures pour assurer la protection de leurs enfants.

En cas de défaillance des parents, le juge des enfants peut prendre les mesures d'assistance éducative prévues aux articles 375 et suivants du Code civil.

Par ailleurs, il existe des réglementations spécifiques à chaque média pour protéger les mineurs :

Réglementations spécifiques à chaque média

* **Pour la presse écrite** la source de la protection se trouve dans la loi.

La loi du 16 juillet 1949 dans son article 14 prévoit un contrôle particulier des publications principalement destinées aux enfants et adolescents et un contrôle des publications en général susceptibles de présenter un danger pour la jeunesse.

L'article 2 prévoit que les publications destinées à la jeunesse ne doivent comporter « aucune illustration, aucun récit, aucune chronique, aucune rubrique, aucune insertion présentant sous un jour favorable le banditisme, le mensonge, le vol, la paresse, la lâcheté, la haine, la débauche ou tous actes qualifiés crimes et délits ou de nature à démoraliser l'enfance ou la jeunesse ou à inspirer ou entretenir des préjugés ethniques ».

La loi du 4 janvier 1967 a modifié l'article 14 de la loi du 16 juillet 1949 et habilité le ministre de l'intérieur à prendre des mesures d'interdiction des publications de toute nature qui recèlent un danger pour la jeunesse, en raison du caractère licencieux ou pornographique, de la place faite au crime et à la violence et, depuis la loi du 31 décembre 1987, à la discrimination et à la haine raciale, à l'incitation à l'usage, à la détention ou au trafic de stupéfiants.

Les décisions du ministre de l'intérieur consistent en :

- une interdiction de vente aux mineurs,
- une interdiction d'exposition,
- une interdiction de publicité.

Ces dispositions sont cependant inapplicables à Internet en l'état, la loi de 1949 ayant limité son champ d'application à l'écrit ; est également inapplicable à Internet le contrôle administratif préalable pouvant déboucher sur une interdiction de circulation, de distribution et de mise en vente d'une publication étrangère prévu par l'article 14 de la loi du 29 juillet 1881 ; seule pourrait trouver application en théorie la « reproduction » sur Internet d'un journal ou écrit déjà interdit par arrêts du ministre de l'Intérieur ; en pratique, il y a lieu de penser qu'une telle infraction serait commise hors des frontières, ce qui rendrait les poursuites difficiles.

* **Pour ce qui concerne** le domaine spécifique de l'**audiovisuel**, le mécanisme de protection repose sur la directive Télévision sans frontières (TSF), la loi et les recommandations du CSA.

L'article 22 de la directive TSF oblige les États membres à s'assurer que les émissions de télévision ne comportent pas de « programme susceptibles de nuire gravement à l'épanouissement physique, mental, ou moral des mineurs, notamment des programmes comprenant des scènes de pornographiques ». La Commission européenne s'est contentée de renvoyer aux autorités nationales le soin de définir les programmes pornographiques ou de violence gratuite et les autres c'est-à-dire les programmes susceptibles de nuire gravement aux mineurs

et ceux simplement susceptibles de leur nuire. Elle laisse aux autorités nationales le soin de définir, pour le second type de programmes, l'horaire adéquat de diffusion et les moyens techniques nécessaires.

L'autorisation délivrée aux chaînes de télévision par le CSA, s'accompagne d'un engagement à respecter diverses règles définies par la loi, concernant notamment la protection de la jeunesse dans la programmation des émissions.

Le CSA se voit confier par la loi du 30 septembre 1986 la mission de veiller au « respect de la personne humaine et de sa dignité, à la protection de l'enfance et de l'adolescence », règles édictées dans le décret du 27 mars 1992 relatif à la publicité ainsi que dans les cahiers des charges des différentes sociétés de programmes, publiques ou privées.

Sur la base de cet article, le CSA a adopté une directive en date du 5 mai 1989 par laquelle il recommande aux chaînes de veiller à ce que les programmes diffusés avant 22H30 ne comportent pas de scènes susceptibles de heurter la sensibilité du jeune public et de s'abstenir de diffuser des émissions, notamment des oeuvres cinématographiques et audiovisuelles, à caractère érotique ou d'incitation à la violence, entre 6 heures et 22H30.

En outre, l'article 26 du décret du 1^{er} septembre 1992 en matière de câble prévoit en ce qui concerne les services émis depuis un pays membre de la CEE « *la possibilité pour le CSA, de suspendre pour une durée n'excédant pas un mois, la retransmission de chacun des services lorsqu'une émission comporte des séquences susceptibles de nuire de façon manifeste, sérieuse et grave à l'épanouissement physique, mental ou moral des mineurs, comprenant notamment des scènes de pornographie ou de violence gratuite, alors qu'il n'est pas assuré par le choix de l'heure de l'émission ou par toute mesure technique que les mineurs se trouvant dans le champ de diffusion ne voient pas ou n'écoutent pas normalement cette émission, ou lorsqu'une émission comporte une incitation à la haine pour des raisons de race, de sexe, de religion ou de nationalité.* »

Le CSA est doté d'un pouvoir de décision et de recommandation mais également d'un pouvoir de sanction et de saisine d'autres instances. Il a la possibilité, sauf pour les émissions en direct, de visionner les émissions préalablement à leur diffusion.

Le respect de la déontologie fait ainsi l'objet d'avis épisodiques de l'autorité de régulation qui a déjà eu l'occasion d'infliger des sanctions pécuniaires à certaines chaînes pour diffusion de téléfilms trop violents et de scènes à caractère sadique et violent dans des dessins animés.

Le CSA tolère la diffusion de films érotiques après 22H sur les chaînes hertziennes ainsi que pour les chaînes cryptées comme Canal plus.

* La protection est assurée en matière de **télématique anonyme** grâce aux recommandations du CST (Conseil supérieur de la télématique).

Le fournisseur de service télématique se doit de respecter les recommandations déontologiques figurant dans le contrat qui le lie à France Télécom.

Le conseil supérieur de la télématique (CST) et le comité de la télématique anonyme (CTA), créés par le décret du 25 février 1993, sont chargés de veiller au respect par les parties des engagements souscrits par le fournisseurs de service. Le CTA peut être saisi par l'une ou l'autre des parties au contrat en cas de différend relatif au respect des recommandations de nature déontologique applicable aux services télématiques anonymes, écrits ou vocaux (Télétel ou Audiotel) et à leurs conditions d'accès. Il est en particulier consulté par France Télécom avant toute décision de résiliation ou de suspension d'une convention.

Selon la convention « Télétel », le fournisseur de services s'engage tout particulièrement à respecter les engagements déontologiques parmi lesquels figurent le rappel des dispositions de l'article 283 et 284 du Code pénal ; dans le cadre de ces stipulations, doit être écarté, notamment, du système du kiosque télématique, tout service mettant à la disposition du public des écrits ou images susceptibles, par leur nature, de porter atteinte au respect de la personne humaine et de sa dignité, et de la protection des enfants et des adolescents et, de ce fait, de porter atteinte à l'image du service public, signataire de telles conventions kiosques ».

En outre, le fournisseur de service s'engage auprès de France Télécom, en vertu de l'article 3 de la convention Télétel sur la promotion des services, « à être tout particulièrement attentif à la protection des mineurs et à ne pas employer dans sa communication publicitaire d'images dégradantes du corps de l'homme et de la femme ».

Si le service ne respecte pas les obligations précitées à la suite d'une mise en demeure de France Télécom, l'exploitant public demande la résiliation ou la suspension du service et saisit pour avis le CTA. Ce motif est à l'origine de la majorité des avis prononcés par le comité.

Enfin, il convient de signaler que la **loi n° 96-299 du 10 avril 1996 relative aux expérimentations** dans le domaine des technologies et des services de l'information prévoit à son article 2 in fine que le titulaire d'autorisation est tenu de subordonner l'accès au réseau des fournisseurs de services déclarés, au titre de l'article 43 de la loi n° 86-1067 du 30 septembre 1986, à l'observation par ces derniers de « règles assurant le respect de la personne et la protection de la jeunesse et du consommateur ».

Le Code pénal comporte plusieurs infractions relatives à la mise en péril des mineurs

Une section du Livre II du Code pénal est consacrée aux infractions de mise en péril des mineurs ; péril physique ou moral.

Parmi ces infractions celle prévue à l'article 227-24 du Code pénal est la plus générale. L'article 227-24 reprend pour partie l'incrimination de l'outrage aux bonnes mœurs actuellement prévue par les articles 283 et suivants. Son champ d'application est limité au cas où le message présentant un caractère immoral serait « susceptible d'être vu ou perçu par un mineur ».

Mais, à d'autres égards, l'incrimination est plus étendue que celle de l'actuel article 283 réprimant, plus largement, les messages présentant un « caractère violent ou pornographique ou de nature à porter gravement atteinte à la dignité humaine ». La formulation retenue évoque en réalité les faits visés par l'article 2 de la loi n° 49-956 du 16 juillet 1949 sur les publications destinées à la jeunesse.

L'extension donnée à la notion d'atteinte à la moralité publique par l'article 227-24 semble d'ores et déjà poser certaines difficultés dans la pratique judiciaire.

Les parquets se montrant réservés pour poursuivre aussi largement que le texte le permettrait.

Les critères de l'article 227-24 sont considérés par la majorité des praticiens comme beaucoup trop vagues.

Les principales dispositions encadrant le droit de la consommation s'appliquent quel que soit le support

Ces dispositions visent à assurer l'information des consommateurs, à encadrer certaines pratiques commerciales, notamment la publicité et la vente à distance, interdire un certain nombre de pratiques tendant à tromper le consommateur (abus de faiblesse, vente sans commande préalable, ventes liées) et à réglementer les conditions générales des contrats par l'interdiction des clauses abusives et le respect d'un certain formalisme sont applicables aux biens et services accessibles par des services en ligne de type Internet.

Il importe de préciser que les dispositions spécifiques à la vente à distance prévues à l'article 121-16 et suivants trouvent application. Elles garantissent aux consommateurs un droit de rétractation dans un délai de 7 jours à compter de la livraison du produit.

La loi du 21 mai 1836 et la loi du 12 juillet 1983 modifiée, réglementant les loteries, répriment la vente de marchandises effectuées par la voie du sort et, plus généralement, toute opération offerte au public pour faire naître l'espérance d'un gain qui serait acquis par la voie du sort. Il ne semble pas, au regard des textes existants, que les sanctions

pénales prévues par ces textes seraient applicables à Internet sauf à considérer que le lieu où est consulté Internet est la dépendance privée d'un lieu public. La législation fiscale sur le produit des jeux se trouve enfin, elle aussi totalement contournée par l'existence des casinos virtuels.

Deux lois garantissent la protection des données

La protection des données à caractère personnel : loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

Les informations à caractère personnel ne sont librement disponibles ni dans leur accès ni dans leur traitement ; elles ne peuvent être librement publiées ou stockées dans une base de données ou un autre corpus qu'après autorisation et selon certaines modalités.

La loi de 1978 apparaît comme le texte fondateur de la charte des libertés et droits de la personne informatisée. L'article 1^{er} de la loi constitue une déclaration d'intention qui dicte à cette loi son esprit : l'informatique doit être au service de chaque citoyen et doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles et publiques.

Les fichiers comportant des mentions nominatives doivent faire l'objet soit d'une autorisation, soit d'une déclaration préalable auprès de la CNIL. Cette loi impose aux détenteurs de fichiers des obligations relatives à la collecte des données et à leur conservation.

Le respect de ce texte s'impose aux acteurs de l'Internet et assure ainsi une garantie à ses utilisateurs.

En application de ce texte, les fichiers implicites (« cookies ») retraçant les consultations de l'abonné devraient faire l'objet d'une déclaration à la CNIL ainsi que toutes autres collectes d'informations à caractère personnel.

Protection contre la fraude informatique

La loi du 5 janvier 1988 dite « loi Godfrain » a introduit un certain nombre de dispositions pénales dans le but de protéger les informations véhiculées par l'informatique.

Les articles L 323-1 et suivants du Code pénal portant sur les atteintes aux systèmes de traitement automatisé de données sanctionnent :

- le fait d'accéder ou de se maintenir, frauduleusement dans tout ou partie d'un système de traitement automatisé de données ;
- le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données ;
- le fait d'introduire frauduleusement des données dans un système de traitement automatisé ou de supprimer ou de modifier frauduleusement les données qu'il contient.

Manifestement, cette loi est un élément de sécurisation de l'Internet, puisqu'elle sanctionne toutes les atteintes susceptibles que pourraient subir les systèmes informatiques des utilisateurs.

Adaptation du dispositif législatif aux spécificités de l'Internet

Les dispositifs législatifs de protection doivent cependant être dans certains cas adaptés à certaines caractéristiques de l'Internet.

L'inadaptation de certains dispositifs législatifs de protection est due à trois caractéristiques de l'Internet : la transnationalité du réseau, la fugacité et la volatilité des contenus, l'évolution très rapide des techniques et des stratégies des acteurs.

La transnationalité de l'Internet

80 % des serveurs étant aujourd'hui d'origine nord-américaine, la plupart des échanges sur l'Internet, marchands ou non marchands, dépassent les frontières françaises. Cette transnationalité est une source de difficulté d'application du droit pénal et du droit commercial.

Le droit pénal

Les règles générales de compétence du droit français permettent en théorie d'appréhender la plupart des comportements délictueux.

La loi pénale française est applicable aux infractions commises sur le territoire de la République (art. 113-1 du Code pénal). L'infraction est réputée commise sur le territoire de la République dès lors qu'un de ces faits constitutifs a eu lieu sur le territoire (art. 113-2 du Code pénal). Pour un acte de complicité commis en France, bien que le crime ou le délit ait été commis à l'étranger, le complice pourra être poursuivi en France si l'infraction de base est poursuivable dans les deux États concernés (art. 113-5 du Code pénal).

La loi pénale française est applicable aux infractions commises hors du territoire de la République dans les situations suivantes :

- pour les crimes et délits punis d'une peine d'emprisonnement commis par un Français ou un étranger ;
- pour les crimes et délits commis par un Français.

En outre la jurisprudence considère que la juridiction française est compétente pour connaître des faits commis à l'étranger par un étranger dès lors que ces faits apparaissent comme formant un tout indivisible avec les infractions imputées en France à cet étranger et dont elle est également saisie.

Toutefois, dans le cas d'Internet ces règles de compétence peuvent se heurter à des difficultés pratiques de localisation et de poursuite des contrevenants et de mise en oeuvre de la coopération pénale internationale.

En effet, le maillage du réseau, la multiplicité des opérateurs facilitent l'évasion d'autant que certaines pratiques, comme les sites miroirs, simples relais d'information, compliquent la recherche de la source du délit.

En outre, certains fournisseurs d'accès étrangers, notamment finlandais, permettent à des utilisateurs de rester anonymes lors de leur présence dans le réseau ; une des méthodes consiste dans l'attribution d'adresses à la volée qui autorise l'utilisateur à se faire adresser des messages à une adresse attribuée pour l'occasion tout en prescrivant son anonymat.

En fait, dans l'hypothèse où les contrevenants sont à l'étranger, l'efficacité de la procédure, de l'enquête à l'exécution de la décision judiciaire, dépend de la bonne volonté de l'Etat ou les États de résidence.

Le principe de territorialité de la compétence des agents de la force publique a conduit les États à développer une entraide répressive internationale qui peut être définie comme l'ensemble des moyens par lesquels un État prête le concours de sa force publique ou de ses institutions judiciaires à l'instruction, au jugement ou à la répression d'une infraction par un autre État.

L'extradition est le moyen juridique d'obtenir d'un État (dit requis) la livraison d'une personne mise en examen ou condamnée qui se trouve sur son territoire à un autre État (dit requérant) compétent pour punir et qui le réclame aux fins de mise en jugement ou d'exécution de sa peine.

Le droit extraditionnel est formé des lois nationales et des conventions internationales à défaut des pratiques internes ou des usages internationaux.

La France est liée par plus de cinquante conventions bilatérales dont chacune à son économie propre.

La France a ratifié la convention européenne d'extradition du 13 décembre 1957.

En l'absence de texte international le droit extraditionnel français est réglementé par la loi du 10 mars 1927.

Cependant, l'extradition ainsi que la plupart des autres formes d'entraide répressive ne sont possibles que pour les infractions répondant à une qualification **pénale** dans les deux États ainsi qu'à un **minimum de gravité** et n'ayant pas un caractère **politique**. Ces conditions limitent le recours à l'extradition dans le cas d'Internet.

Certes, des extraditions et des enquêtes ont déjà été opérées sur ces bases pour des faits commis à l'étranger.

À titre d'exemple les États Unis ont obtenu l'extradition d'Américains exploitant un serveur sadomasochiste au Mexique.

Cependant, la règle de la double incrimination sera souvent un obstacle aux actes d'enquête et de poursuite ; les États-Unis n'incriminent pas ainsi les propos racistes ou révisionnistes. Dès lors, aucune coopération n'est envisageable avec ce pays pour faire condamner des serveurs racistes qui y seraient installés ; de plus, dans la plupart des pays, les délits de presse et notamment l'incitation à la haine raciale, sont considérées comme des infractions politiques.

Au delà, il existe des États avec lesquels l'entraide judiciaire est quasiment inexistante. Ces États risquent de devenir vite des « paradis Internet ».

Enfin, les mécanismes de l'entraide judiciaire induisent une lenteur, due notamment à la transmission diplomatique des actes, qui sera une source d'impunité, les preuves de l'infraction risquent de disparaître rapidement compte tenu de la fugacité des contenus.

Droit commercial

Le commerce de biens immatériels est redevable des droits fiscaux. En revanche, l'absence de flux matériels se prête à l'évasion fiscale.

Il convient de constater que ce type de transaction est difficile à appréhender, non seulement par les services fiscaux mais aussi par les services douaniers. En l'absence de franchissement physiques d'une frontière on peut s'interroger sur le bien fondé juridique de la perception de droits de douanes.

En outre, le principe de l'autonomie de volonté des parties qui prévaut en matière contractuelle peut paraître un facteur supplémentaire d'insécurité juridique. En effet, ce principe signifie que les parties choisissent la loi applicable à leur contrat. Ce choix peut être implicite ou explicite.

En cas d'absence de choix de la loi du contrat, le juge est censé retrouver la volonté des parties telle qu'elle se manifeste dans la localisation de leur opération. Les indices retenus habituellement sont :

- les lieux de conclusion ;
- le lieu d'exécution ;
- la forme ;
- la langue ;
- la teneur des lois en présence.

L'ensemble de ces règles s'applique sous réserve de textes spécifiques notamment les conventions internationales par exemple la convention de Vienne pour la vente, et le droit dérivé communautaire comme le projet de directive concernant la protection des consommateurs en matière de contrat à distance.

Pour ce qui concerne les relations contractuelles internationales, en l'absence de stipulations définissant la loi applicable, les tribunaux auront de grandes difficultés à déterminer la volonté des parties dans la mesure où il s'agit de contrat à distance, sans écrit, et dont la langue utilisée est l'anglais non par volonté explicite mais par simple commodité.

Protection des données de caractère personnel

L'article 24 de la loi du 6 janvier 1978 avait prévu un contrôle des flux transfrontaliers des données à caractère personnel. Cet article prévoyait que son application serait déterminée par un décret. Or, les pouvoirs publics n'ont jamais pris ce texte. Face à cette carence, la CNIL a dû inventer un cadre juridique pour ces flux par deux avis s'inspirant des techniques du droit civil : le transfert des données dans le respect des principes fondamentaux de la loi de 1978 peut être ainsi mis en oeuvre soit par stipulations contractuelles, soit par engagement unilatéral du pays de destination. Ce mécanisme ponctuel devra être élargi aux flux de données sur l'Internet.

Fugacité et volatilité des contenus

La fugacité et la volatilité des contenus est une cause de difficulté pour l'enquête pénale et pour l'application de certains textes.

Difficulté de l'enquête

L'enquête pénale a pour but d'identifier l'auteur de l'infraction et d'établir l'existence des éléments constitutifs de celle-ci.

La preuve en matière pénale est libre.

Les infractions commises sur l'Internet seront souvent difficiles à établir.

Le message litigieux risque fort de disparaître. En plus, son auteur pourra se défendre en expliquant qu'il a été modifié par un tiers.

Le simple témoignage d'une personne ayant vu le message ou son enregistrement par un utilisateur de l'Internet n'aura pas la même force probante qu'un procès verbal constatant l'infraction.

Or, les personnes chargées de constater les infractions interviendront souvent tardivement.

Difficulté d'application de certains textes

Quelques exemples :

* L'article 6 de la loi n° 82-652 du 29 juillet 1982 prévoit que toute personne 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.

Ce texte s'applique évidemment aux réseaux en ligne.

Cependant, il est prévu que la réponse acceptée ou imposée doit être diffusée de manière que lui soit assurée une audience équivalente à celle du message (L. 1982, précité, art. 6 alinéa 4). Cette règle de diffusion équivalente, qui n'est que la reprise en matière audiovisuelle des principes régissant le droit de réponse que connaît la presse écrite, est quasiment inapplicable à Internet, dès lors que l'appel du document se faisant sur demande, il paraît difficile d'être assuré que la réponse ait une audience équivalente.

En outre, l'article 6 alinéa II de la loi de 1982 prévoit, afin de garantir la réalité du droit de réponse, la conservation des « documents audiovisuels nécessaires à l'administration de la preuve ». Il s'agit, à l'évidence, de lutter contre ce qu'on peut appeler la fugacité de l'audiovisuel. Le délai de droit commun est de quinze jours, mais s'agissant de la télématique, il est ramené à huit jours :

« Les messages et tous autres documents nécessaires à l'administration de la preuve des imputations de nature à porter atteinte à l'honneur ou à la réputation du demandeur doivent être conservés sous la responsabilité du directeur ou du codirecteur de la publication pendant huit jours à compter de la date à laquelle ils ont cessé ». (D. 6 avril 1987, art. 8, al. 2).

Ce n'est pas toutefois le délai qui constitue le point qui mérite le plus d'attention. C'est davantage le fait que si les messages et documents nécessaires à l'administration de la preuve doivent être conservés, cela signifie, ou peut signifier *a priori*, que tout ce qui transite par le service doit être conservé en mémoire. On peut se demander si c'est là une chose parfaitement réaliste. Faut-il dans cette logique aller jusqu'à penser que les forums soient concernés par la mise en mémoire ?

* La protection des consommateurs est assurée par l'édiction de règles tendant à garantir le caractère éclairé de leur consentement. Pour ce faire la loi a prévu un délai de réflexion pour certains contrats et organisé un formalisme de protection. Ce formalisme étant d'ordre public, les parties ne peuvent y renoncer.

Ces dispositions semblent difficilement transposables lorsque la transaction porte sur un bien immatériel, tel le téléchargement d'un logiciel ; dans ce cas il y a instantanéité totale entre acte d'achat et de consommation.

Comment dès lors faire la preuve du point de départ du délai de rétroaction ?

En matière civile, la loi fixe les moyens de preuve qui peuvent être produits en cas de litige et en détermine le cas échéant, les conditions d'admissibilité et la force probante. La preuve est dite « légale ».

Les règles de preuve de certains actes juridiques sont expressément imposées par le droit. Il en est ainsi par exemple, dès que l'acte exige, outre le consentement des parties, l'exécution d'une formalité spéciale.

Ainsi, pour les contrats « solennels », la formalité exigée est tantôt la rédaction d'un acte notarié (exemples : la donation, le contrat de mariage, le contrat d'hypothèque, la vente d'immeuble à construire), tantôt la rédaction d'un écrit quelconque (exemples : le gage, le bail rural, le contrat d'édition, la cession de brevet d'invention...).

L'article 1341 du Code civil institue non seulement l'obligation de pré constituer un écrit dès lors que l'objet du contrat a une valeur supérieure à 5 000 francs, mais impose sa prééminence sur d'autres modes de preuve comme le témoignage.

Ainsi, même dans le cas où un écrit a été passé pour une somme égale ou inférieure à 5 000 francs, l'article 1341 exclut toute preuve par témoignage contre cet acte.

Il paraît difficilement envisageable de passer un contrat solennel sur Internet, l'officier ministériel devant être physiquement présent pour s'assurer du consentement des parties. Pour la preuve des autres actes, les parties peuvent toujours renoncer aux règles de preuve prévues dans le Code civil, puisqu'elles ne sont pas considérées comme d'ordre public. La Cour de cassation a admis dans le cadre de contrat de carte bancaire la validité de la signature informatique.

Si, comme on vient de le rappeler, l'exigence d'une preuve écrite en matière civile sera difficilement adaptée au réseau Internet par nature instantané, le principe de la liberté de la preuve en matière commerciale à l'instar du droit pénal, aboutit à la même difficulté que celle décrite pour une enquête judiciaire sur ce réseau. Il sera malaisé pour l'utilisateur d'apporter une preuve matérielle.

En conséquence, l'absence de formalité du droit commercial et le trop grand formalisme du droit civil semblent inadaptés au réseau d'Internet et risquent de favoriser pour le consommateur l'impression de vide juridique dans la mesure où il ne pourra pas faire la preuve de son bon droit.

Évolution très rapide des techniques et des stratégies

Internet est un monde en rapide mutation où le statut et le rôle des acteurs sont éminemment variables : ceci rend difficile l'appréhension de la matière mais aussi la définition de catégories sur lesquelles est fondée toute approche juridique. Deux exemples :

* Les « cookies », tout d'abord, fichiers implicites tenu par le fournisseur d'accès retraçant les consultations d'un abonné ; ces fichiers peuvent se révéler utiles puisqu'ils permettent au fournisseur de connaître

les sites préférés de son client et de les rapatrier sur ses machines diminuant ainsi le temps d'accès ; cependant, de tels « cookies » ne sont pas toujours connus des utilisateurs alors qu'ils constituent un risque pour la vie privée de ceux-ci ; d'autres techniques peuvent apparaître et le droit doit apprendre à les connaître ;

* Autre exemple, l'utilisateur : celui-ci peut à la fois être éditeur, serveur, consommateur... et cette confusion des rôles rend parfois difficile de trouver la règle de droit applicable.

Conclusion

Même si l'Internet bouleverse les définitions classiques du droit de la communication fondées sur la distinction entre correspondance privée et communication audiovisuelle et contrairement à ce qui a pu être dit ici où là, il n'y a pas de vide juridique sur Internet mais au contraire pléthore de textes applicables ; certaines adaptations doivent cependant être mises en oeuvre par chaque branche du droit afin de faciliter le respect, par les services en ligne d'un genre nouveau, des règles protectrices de la personne et du consommateur. A plus long terme, une réflexion sur le droit de la communication à partir de quelques concepts communs à tous les supports pourrait s'engager.

Chapitre 3

L'enseignement des exemples étrangers

Les USA

L'exemple américain est intéressant dans la mesure où diverses tentatives de régulation de l'Internet ont été entreprises sur un marché plus mûr que le marché français.

L'Internet est beaucoup plus développé aux USA qu'en France : on estime ainsi à environ 9,6 millions les foyers en ligne en 1995 en raison notamment de la croissance exceptionnelle d'America on line, principal service destiné aux particuliers ; le nombre des foyers américains connectés atteindra 35,2 millions en l'an 2000, soit un tiers de tous les foyers du pays, selon une étude publiée par le Cabinet Jupiter Communication.

Diverses tentatives de régulation ont été entreprises aux États-Unis : les dispositions législatives du Communications Decency Act, adoptées en février 1996 à l'occasion du vote de la loi sur les télécommunications ; il se dégage toutefois une réaction de rejet très forte à l'encontre de ce texte qui semble prématuré ; les essais d'autorégulation des acteurs eux-mêmes qui apparaissent plus prometteurs.

Les principales dispositions du Decency Act

Protection des mineurs

Au-delà de la mise à jour des dispositions législatives rendues nécessaires par l'apparition de nouvelles technologies, le Communications Decency Act of 1996 tend à renforcer la protection des mineurs d'une part, par la mise en place de dispositifs techniques dans les programmes audiovisuels et d'autre part, par l'extension du champ de protection aux messages à caractère « indécent ».

Les services audiovisuels

Un système de contrôle et de classification des programmes a été mis en place.

En liaison avec les organisations concernées, les industriels de la télévision disposent d'une année à compter de la promulgation de la loi pour développer un système de classification des programmes prenant

en compte leur caractère plus ou moins violent et sexuel. Ils devront également édicter des règles imposant aux diffuseurs d'intégrer à leurs programmes un signal tenant compte de cette classification (article 551 du Communications Decency Act).

En outre, les fabricants devront, dans un délai maximal de deux ans à compter de la promulgation de la loi équiper tout appareil dont la taille d'écran est supérieure à 13 pouces, d'une puce électronique (V-chip) destinée à reconnaître le signal de classification diffusé et à offrir aux utilisateurs la possibilité de bloquer la réception de certains programmes.

Les réseaux câblés

Le Communications Decency Act of 1996 prévoit également des mesures de nature à renforcer la protection des mineurs. Les câblo-opérateurs doivent désormais, à la demande d'un abonné, brouiller individuellement l'une quelconque des chaînes faisant partie de leur bouquet sans frais additionnels (article 640 du Communications Act). Les diffuseurs de bouquet comprenant des programmes à caractère pornographique doivent brouiller ces programmes afin de s'assurer que des personnes n'ayant pas souscrit d'abonnement ne sont pas en mesure de les recevoir. Tant que cette obligation n'est pas remplie, les diffuseurs devront s'abstenir de diffuser ces programmes durant la journée dans une plage horaire que la FCC doit définir (article 641 du Communication Act).

Tout en réaffirmant que les câblo-opérateurs n'ont pas à exercer de contrôle éditorial sur les chaînes qu'ils proposent, la loi leur permet de refuser de distribuer un programme ou une partie de programme comportant des obscénités, des propos indécents ou de la nudité.

Les services de télécommunications et les services en ligne

Le Communications Decency Act étend les sanctions pénales préexistantes en matière d'obscénité et d'indécence à l'ensemble des communications initiées à partir d'un appareil de télécommunications et non plus uniquement à partir d'un téléphone (article 223 a1 du Communications Act). Le fait d'utiliser des services interactifs en vue de diffuser des obscénités ou des propos indécents de nature manifestement offensante à l'intention des mineurs est sanctionné d'une amende et d'une peine de prison (article 223 d du Communications Act).

Cependant, afin de ne pas voir opposer la liberté d'expression aux personnes qui limiteraient l'accès à des programmes qu'elles jugent à caractère pornographique ou indécent, la loi prévoit que les utilisateurs et les fournisseurs de services informatiques interactifs ne pourront être tenus responsables de violation du premier amendement de la Constitution au titre d'actions prises de bonne foi pour limiter la disponibilité de contenus jugés offensants ou obscènes (Good samaritan blocking, article 230 c du Communications Act).

Le régime de responsabilité

Si les définitions de l'indécence ou de la nudité sont unanimement contestées car elles apparaissent trop vagues et trop larges, le régime de responsabilité mis en place par la loi semble relativement équilibré.

Le Communications Decency Act prévoit que les fournisseurs et utilisateurs de services interactifs ne pourront être considérés comme étant les éditeurs d'informations obtenues auprès d'un fournisseur de contenus (article 230c du Communications Act).

Il précise le régime de responsabilité applicable aux opérateurs de réseaux de télécommunications en limitant cette responsabilité aux seuls cas où l'opérateur autorise l'utilisation de ses infrastructures en sachant qu'elles sont utilisées pour des activités prohibées par la loi (article 223a - 2 - et 223d - 2 - du Communications Act). La seule fourniture d'accès à un système ou un serveur à l'origine de telles activités ne peut être sanctionnée pénalement à condition que cette fourniture d'accès ne soit pas liée à la création de contenus et qu'elle ne fasse pas l'objet de publicité (article 223e).

La loi prévoit également qu'un employeur ne sera pas tenu responsable des actes commis par des employés hors du champ de leurs activités professionnelles (article 223e - 4 - du Communications Decency Act). De même, elle stipule également que lors d'une action pénale, des « mesures raisonnables et efficaces » visant à restreindre l'accès de mineurs à des serveurs (numéro d'identification, carte de crédit,...) suffiront à établir la bonne foi du défendeur (article 223e - 6 - du Communications Decency Act).

Conclusion

Il convient de signaler que certaines des dispositions du Communications Decency Act font l'objet d'un recours en constitutionnalité pour violation du premier amendement de la Constitution des États-Unis qui garantit les libertés de parole, de culte, d'expression, de rassemblement et de manifestation contre l'autorité publique ; la Cour de Philadelphie a, dès à présent, conclu à l'inconstitutionnalité du Decency Act ; la question est désormais en appel devant la Cour Suprême. Par ailleurs, une Cour de première instance (District Court) de l'État du Delaware a enjoint provisoirement le Gouvernement des États-Unis, y compris la FCC, à ne pas appliquer les dispositions portant sur le brouillage de programmes à caractère sexuel. L'entrée en vigueur des dispositions les plus controversées du Communications Decency Act semble donc pour l'instant remise en question.

Les principaux enseignements de l'expérience américaine relative à l'Internet

Une initiative prématurée

Le Decency Act apparaît comme une initiative prématurée, conçue en appliquant un modèle audiovisuel clairement inadapté aux yeux des spécialistes de l'Internet.

Pour la plupart des interlocuteurs, le Decency Act a été adopté de manière prématurée car il ne repose pas sur une analyse de fond d'un concept nouveau et en pleine évolution.

Un concept en pleine évolution

Il s'agit pour beaucoup d'une industrie de transition qui est actuellement en perpétuelle évolution : certains estiment que les navigateurs vont croître car c'est le premier outil nécessaire sur Internet ; d'autres que les capacités du réseau vont exploser et qu'il est très probable que les compagnies de téléphone vont reprendre le leadership. Tous s'accordent pour dire que le marché va se restructurer. Beaucoup se demandent ce que signifie contrôle dans cette dynamique.

La plupart des industriels rencontrés estiment qu'il s'agit du premier acte politique vis-à-vis de l'Internet. Le Congrès aurait d'abord dû, selon eux, essayer de savoir ce qu'était l'Internet et quel était son fonctionnement avant de légiférer. Ils ont toutefois souligné qu'il existe maintenant un groupe de travail sur l'Internet en son sein. Certains vont plus loin et pensent que toute loi nationale visant l'Internet est insuffisante pour ce média à vocation internationale. Des lois de type législation maritime ou espace seraient selon eux plus appropriées.

Un concept nouveau

Les institutionnels (FCC, ministères) ont reconnu que la tentative dans le Decency Act de transposer d'anciens modèles à Internet n'était pas facile. Ils s'accordent à dire qu'il n'est pas nécessaire de prendre d'autres textes tant que la ou les techniques ne seraient pas stabilisées, sauf peut être en ce qui concerne les droits d'auteurs ; ils ne seraient pas mécontents que les tribunaux, à la suite du recours en constitutionnalité introduit, « gèlent » une partie des dispositions de la loi.

L'Internet se différencie en effet aux yeux d'un grand nombre de professionnels de la télévision pour deux raisons :

- le rôle actif de l'utilisateur qui n'est plus simplement spectateur ;
- le champ d'application international de l'Internet ;
- l'absence (relative) de pénurie des ressources.

Beaucoup préconisent donc d'adopter le modèle du kiosque à journaux ou de la librairie plutôt que celui de l'audiovisuel.

Un grand nombre de personnes pense que les notions d'éditeurs et de distributeurs prennent un tout autre sens compte tenu du

fonctionnement de l'Internet qui repose sur des terminaux interactifs comme les ordinateurs.

Les organismes de l'Internet ont une approche similaire. Ils pensent que l'Internet est un vecteur de diffusion de l'information et donc de démocratie et que la caractéristique majeure de l'Internet repose dans un degré d'intervention très fort des utilisateurs : n'importe qui peut devenir un éditeur.

Auto-régulation

L'autorégulation par les acteurs eux-mêmes est la voie préférée; nombreux sont les professionnels qui prennent conscience de la nécessité de réguler le réseau par la mise en place de solutions technologiques, de codes de bonne conduite, la sensibilisation du grand public au fonctionnement et aux risques de l'Internet.

Cette volonté d'autorégulation est illustrée par l'attitude de la Federal Communication Commission (FCC) : celle-ci, face à la plainte de l'America's Carriers Telecommunications Association (ACTA) pour la fourniture de service téléphonique via Internet, a volontairement choisi de ne pas intervenir sur les services à valeur ajoutée comme ceux qui existent où sont fournis par Internet, notamment parce qu'elle pense que la croissance sera d'autant plus forte que la régulation ne sera pas pesante ; La Federal Communication Commission estime que le Decency Act relève d'ailleurs plutôt du Department of Justice et que la mission première de la FCC porte plus sur la régulation des infrastructures.

Pour la majorité des industriels, l'Internet est un magnifique instrument de croissance. Dans de nombreux cas, la technique aura la ou les réponses aux problèmes juridiques posés.

Reprenant cette philosophie, l'Internet legal forum a établi un premier jeu de propositions et compte démontrer qu'un Code de bonne conduite « volontaire » allié à des solutions technologiques habiles est plus efficace qu'une législation mal conçue.

De nombreuses tentatives d'autocontrôle semblent voir le jour avec la diffusion de logiciels de contrôle imaginés par l'association PICS qui regroupe un grand nombre de professionnels de l'industrie de l'informatique ou des télécommunications.

Une grande action de sensibilisation des utilisateurs a été entreprise par exemple par l'Interactive services association et la National Consumers League. Ces associations ont édité des dépliants et des brochures intitulés Project OPEN - the Online Public Education Network, afin de sensibiliser les utilisateurs aux dangers que peut receler l'Internet, faire connaître les réflexes ou attitudes à avoir sur le réseau, etc.

Il est intéressant de souligner l'ouverture d'esprit des professionnels et même la volonté de voir s'auto-réguler le réseau au fur et à mesure qu'il évolue ; un certain nombre de propositions ont ainsi été tout à fait bien accueillies comme par exemple la mise en place d'une

classification des centres serveurs accompagnée d'une offre de logiciels de contrôle parental « multi-critère », les parents pouvant choisir ensuite leur référentiel permettant le blocage et/ou la sélection de sites selon leurs choix.

Enfin, depuis le 14 mars dernier, le Congrès étudie une nouvelle loi qui assouplirait le Decency Act : le Online Parental Control Act ; cette initiative de la député démocrate Anna Estroo démontre qu'un contrôle parental, à partir des outils de la plateforme PICS, est possible sur Internet et préférable à un contrôle gouvernemental. Un label L18 (moins de 18 ans) devrait bientôt apparaître.

Conclusion

Il semble que les acteurs de l'Internet (organismes de l'Internet et une grande partie des industriels) soient conscients de la nécessité de « réguler » le réseau et favorables à ce que des discussions supranationales soient ouvertes, non sur des questions de contenus mais sur des questions de méthodologie : partage des responsabilités, loi applicable,... Les institutionnels américains semblent plus hésitants par rapport à une initiative internationale portant sur le droit de l'Internet sauf en ce qui concerne la protection des droits d'auteurs et une éventuelle coopération judiciaire car ils estiment qu'il s'agit d'un marché nord-américain et non mondial. Néanmoins, une cellule de réflexion a récemment été constituée auprès du Président Clinton sur les questions de déontologie afin de définir pour la fin du mois de juin un message présidentiel.

Le Canada

Le Conseil de la radiodiffusion et des télécommunications canadien (CRTC) a entamé une réflexion sur l'Internet : il ne s'agit pas d'une réflexion strictement juridique car les canadiens privilégient l'autorégulation, sans exclure pour autant une certaine surveillance. Cette approche originale a déjà trouvé à s'appliquer en matière de violence à la télévision.

L'approche canadienne de l'Internet : liberté et présence sur le réseau

Pour les canadiens, Internet est une technologie et un marché encore jeune qu'il n'est pas question de censurer. L'attitude adoptée est donc celle d'une extrême prudence pour ne pas nuire à la liberté d'expression. Le régulateur n'a rien fait et ne compte rien faire dans l'immédiat.

De plus, il leur semble que la censure de l'Internet n'a pas beaucoup de sens : l'exemple de la Chine qui a essayé de restreindre l'accès au réseau en exigeant que l'accès à l'Internet se fasse uniquement grâce à quatre organisations étatiques n'est pas transposable à la France qui dispose de réseaux de télécommunications très performants ; l'exemple de Bavière est également un cas marginal, procédant plus d'un effet de surprise pour Compuserve qui ne se reproduira pas.

L'essentiel pour le Canada est aujourd'hui d'être présent sur l'Internet ; des mesures d'accompagnement peuvent le favoriser comme la baisse du coût d'accès (tarifs forfaitaires), l'instauration de dégrèvements fiscaux pour l'achat d'ordinateurs de particuliers ou d'entreprises ; il faut aussi offrir des services en anglais, au moins dans un premier temps, pour provoquer l'attrait et la curiosité envers la culture francophone (?).

La méthodologie canadienne : une démarche non juridique, modeste et ciblée

La démarche retenue pour Internet veut s'inspirer de celle de l'audiovisuel à l'encontre de la violence. Quelle est celle-ci ?

La méthode est non juridique, modeste, ciblée et basée sur la preuve médicale :

- la preuve médicale : il y a une corrélation entre la violence à la télévision et la délinquance des jeunes ;
- la cible : les mineurs de moins de douze ans ;
- la question a été limitée à la violence et non à d'autres sujets comme le sexe, qui procède d'un tout autre registre : idéologies religieuses, valeurs chrétiennes...

Les chaînes de télévision ont créé un Code de déontologie adapté leur thématique propre et agréé par l'industrie ; un Code non agréé confère une publicité très négative à la chaîne. L'industrie, les parents et les professeurs ont reconnu l'existence de ce lien et reprise à leur compte la démarche.

Les producteurs ont classifié leur programme et une importante campagne de sensibilisation a été menée auprès des parents, écoles... Enfin, le dispositif du « V-chip » sur les postes de télévision a été rendu obligatoire. Cependant, cette technologie n'est qu'une petite partie de la solution visant à combattre la violence à la télévision, 80 % de la solution résidant dans la sensibilisation, l'éducation populaire ou ce que l'on pourrait appeler « l'instruction médiatique ».

Conclusion

Le CRTC semble avoir retenu une approche modérée et réaliste de l'Internet. Cette approche ne signifie pas inaction puisque le CRTC

estime que l'Internet appelle des solutions harmonisées au niveau international et que pourrait, par exemple, être imaginé la mise en place d'une structure commune de réflexion, et non de surveillance ; un groupe composé d'experts techniques de l'Internet au niveau du G7, qui aurait pour mission de conseiller les États ou les ministres, pourrait dans cette optique être utile.

La Communauté européenne

La Communauté européenne qui a initié depuis plusieurs années une réflexion sur la société de l'information ne pouvait pas se désintéresser du développement de l'Internet. Son interrogation sur ce réseau s'articule autour du bien-fondé de son intervention et de ses modalités. D'ores et déjà, force est de constater que certaines réglementations communautaires spécifiques assurent une protection d'objectifs d'intérêt général.

Compétence de la Communauté

La Communauté ne jouit que d'une compétence d'attribution, c'est-à-dire que ses activités peuvent et doivent se déployer dans un certain nombre de domaines limitativement déterminés par le traité ; le principe demeure la compétence nationale, la compétence communautaire étant l'exception.

Il est prévu, en outre, à l'article 235 du traité de la communauté européenne que si une action de la Communauté apparaît nécessaire pour réaliser, dans le fonctionnement du marché commun l'un des objectifs du traité, le conseil statuant à l'unanimité sur proposition de la commission et après consultation du Parlement, prend les dispositions appropriées.

L'article 235 précité a pour limite la règle de la subsidiarité, selon laquelle la communauté ne doit agir que lorsqu'un objectif peut être mieux réalisé au niveau communautaire qu'au niveau national.

La libre circulation des marchandises étant l'un des objectifs de la Communauté (article 59 de la CEE), une éventuelle intervention de la Communauté sur Internet peut se justifier au nom de la libre circulation de l'information. En effet, en l'absence d'un niveau de protection juridique équivalent entre États-membres, chaque pays tente d'élaborer sa propre législation, ce qui risque d'entraîner une fragmentation du marché intérieur ; rappelons que les mesures discriminatoires ne sont compatibles avec le traité que si elles peuvent être justifiées par des raisons impérieuses d'intérêt général.

Dès lors, l'objectif est d'élaborer une réglementation communautaire assurant un niveau équivalent de protection des objectifs d'intérêt général concernés afin de supprimer les barrières juridiques éventuelles créées par la disparité des réglementations nationales.

Approche générale d'Internet

La première étape de la réflexion de la Communauté sur la société de l'information se trouve dans la recommandation au Conseil européen intitulée « L'Europe et la société de l'information planétaire », plus connue sous le nom de rapport Bangemann. L'approche de ce rapport repose sur la distinction des infrastructures et des contenus. L'action réglementaire envisagée consiste à accélérer le processus de libéralisation sans appréhender les contenus ; elle vise à établir un cadre commun pour la protection des droits de propriété intellectuelle, de la vie privée et de la sécurité de l'information.

S'il existe toujours un consensus pour distinguer la prestation de service du contenu, la Commission a pris conscience de la complémentarité des secteurs « culture » et « télécommunications » qui doit permettre d'intégrer les valeurs culturelles dans le développement des nouvelles technologies.

La Commission essaie actuellement de déterminer les enjeux et les questions posés par l'Internet avant de s'engager dans une éventuelle intervention.

L'idée d'étendre le champ de la directive « Télévision sans frontière » aux nouveaux services, comme le souhaitaient certains États et le Parlement européen, a été abandonné ; le conseil des ministres du 11 juin 1996 a en effet estimé que le cadre actuel de ce texte relatif à la diffusion ne s'y prêtait pas. ; en effet, la diffusion est la transmission d'un point vers des points multiples alors que les nouveaux services fonctionnent par transmission d'un point à un autre.

Dans le contexte de la préparation d'un Livre Vert sur le développement des nouveaux services audiovisuels, la commission a lancé une consultation des États membres visant à approfondir la question de la protection des intérêts généraux : liberté d'expression, protection des mineurs, ordre public, respect de la vie privée.

Toutefois, les réponses des États se fondent sur le droit positif, alors que l'analyse juridique de l'Internet ne fait que commencer chez la plupart d'entre eux.

Pour prendre en considération les législations futures, la direction générale DG XV avait envisagé un mécanisme de transparence obligeant les États membres à lui adresser tout projet de texte ou de réglementation concernant les services en ligne ; devant l'hostilité des États et l'absence de base juridique de ce système, le projet a été abandonné.

Enfin, dans son Livre Vert relatif aux communications commerciales dans le marché intérieur, achevé en mai 1996, la commission souligne les conséquences du développement de l'Internet notamment au regard de la communication commerciale transfrontière ; selon la Commission, la nature même des nouveaux réseaux rend encore plus indispensable la mise en place d'un cadre réglementaire basé sur les principes fondamentaux du marché intérieur et, plus précisément, sur le principe du contrôle par le pays d'origine chaque fois que cela sera possible et approprié ; en effet, une fois qu'un message a été envoyé sur l'Internet, il peut être reçu instantanément en n'importe quel point du globe ; avec une réglementation confiant le contrôle du service au pays d'origine, il sera plus facile de retrouver les contrevenants.

Des textes spécifiques protégeant les objectifs d'intérêt général

Plusieurs directives horizontales ont été adoptées ou sont en voie d'adoption afin d'accompagner le développement de la société de l'information et de protéger le consommateur.

La protection du consommateur

Il ressort clairement de l'article 129 A du Traité que la Communauté doit agir dans tous les domaines relevant de la protection des consommateurs et pas seulement dans les domaines ayant trait au marché intérieur.

La protection du consommateur est assurée notamment par la directive 84/450/CEE du Conseil du 10 septembre 1984 relative au rapprochement des dispositions législatives, réglementaires et administratives des États membres en matière de publicité trompeuse et le projet de directive concernant la protection des consommateurs en matière de contrats à distance.

Ce dernier texte organise l'information précontractuelle, fixe le principe d'un délai de rétractation et celui d'une confirmation écrite des informations ; pour prendre en considération les nouveaux services, il est prévu dans la dernière version de la directive que l'écrit s'entendra de tout « support durable » à la disposition du consommateur ; dès lors la confirmation écrite des informations pourra prendre la forme d'un courrier électronique ; en revanche les dispositions relatives au délai de rétractation semblent difficilement adaptées à l'achat de biens immatériels.

Par ailleurs, il importe de rappeler que l'article 13 de la convention de Bruxelles du 27 septembre 1968 donne la possibilité aux consommateurs de saisir le tribunal de leur domicile pour tout litige en matière de droit de consommation.

Protection de la propriété intellectuelle

Cette protection est assurée par cinq directives :

- la directive 91/250/CEE sur la protection juridique des programmes d'ordinateurs ;
- la directive 92/100/CEE relative au droit de location et de prêt et à certains droits voisins du droit d'auteur dans le domaine de la propriété intellectuelle ;
- la directive 93/83/CEE 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 ;
- la directive 93/98/CEE relative à l'harmonisation de la durée de protection du droit d'auteur et de certains droits voisins ;
- la directive relative à la protection juridique des bases de données du 11 mars 1996.

Protection de la vie privée

La directive 95/46/CEE du 24 juillet 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la circulation de ces données institue un niveau de protection comparable à celui de la loi « informatique et liberté ». Le champ d'application de la directive est plus large que la loi française, puisqu'elle appréhende le traitement du son et de l'image.

Le texte communautaire constitue un instrument pour les États membres leur permettant de contrôler les fichiers implicites existant sur l'Internet.

Conclusion

À la lumière des travaux de la Commission, il apparaît que celle-ci, hormis des textes ponctuels, n'a pas encore défini sa position sur les services en ligne de type Internet ; elle attend les contributions des États membres aux différents Livres Verts tout en redoutant la multiplication de réponses nationales divergeantes.

Deux exemples européens : l'Allemagne et la Grande-Bretagne

En Allemagne

L'Internet est un enjeu politique important entre les Länder et le Bund, ce dernier favorisant une approche libérale, fondée sur l'auto-limitation.

Le débat constitutionnel

Bund et Länder s'estiment tout deux compétents concernant l'Internet à l'instar du débat qui les a opposé depuis 1989, en matière de radiodiffusion, à la suite du recours du gouvernement bavarois.

L'objet du recours visait la décision du gouvernement fédéral du 8 mars 1989 d'approuver le projet de directive Télévision sans frontières et la manière dont le gouvernement fédéral avait oeuvré à son élaboration jusqu'à son approbation par le conseil des ministres de la Communauté européenne le 3 octobre 1989 ; par une décision de 1995, la Cour constitutionnelle de Karlsruhe a confirmé la constitutionnalité de la décision du 8 mars 1989 ; en revanche elle a considéré que la manière dont le Bund, à la suite de cette décision, avait représenté les intérêts de la République fédérale lors de l'élaboration de la réglementation sur les quotas constituait une violation des droits de l'État libre de Bavière, et des Länder associés à sa démarche, au regard de l'article 70 de la loi fondamentale qui donne une compétence législative du droit commun comme aux Länder, le Bund n'ayant qu'une compétence d'attribution et au regard de l'article 24 qui autorise le Bund à consentir des transferts de souveraineté à des autorités interétatiques.

Il convient de préciser que l'arrêt de la Cour est intervenu avant l'insertion dans la loi fondamentale allemande d'un nouvel article ménageant aux Länder, *via* le Bundesrat, un droit de regard étendu sur les affaires audiovisuelles. En principe, ces nouvelles dispositions constitutionnelles devraient éviter ce type de conflit. En outre, la « loi de participation » prise en application de ces dispositions impose au Bund de tenir compte de l'avis du Bundesrat dans les domaines de compétence exclusive des Länder que sont, essentiellement, l'éducation et la culture. Il est clair que la décision de la Cour Constitutionnelle incite le Gouvernement à interpréter ces dispositions dans un sens favorable aux Länder qui ne peuvent toutefois s'exprimer que d'une seule voix, celle du Bundesrat.

L'Internet aujourd'hui fait donc l'objet d'un débat de compétence entre le Bund et les Länder, ceux-ci voulant voir appliquer le même raisonnement que celui ayant motivé la décision constitutionnelle de 1995 ; l'enjeu est de taille car l'approche et la compréhension des réseaux en ligne par chacune des parties sont fort différentes.

L'Internet aujourd'hui fait l'objet d'un débat de compétence entre le Bund et les Länder, ceux-ci voulant appliquer le même raisonnement que celui ayant motivé la décision constitutionnelle de 1995 ; l'enjeu est de taille car l'approche et la compréhension des réseaux en ligne par chacune des parties sont fort différentes.

L'approche de l'Internet

* Lorsqu'il a présenté les grandes lignes directrices de la « loi multimédia », le ministre fédéral Jürgen Rüttgers a « tenu à se faire l'avocat d'une analyse commune » entre l'Etat fédéral et les Länder en ce qui concerne tant les possibilités que le multimédia offre et les dangers qu'il recèle.

Après avoir rappeler la spécificité du multimédia, qui recouvre des formes élaborées de communication individuelle interactive et de communication de masse, le ministre a exposé les principales lignes directrices de la future loi multimédia ; celle-ci devrait :

- assurer le libre exercice de l'activité grâce notamment à la libéralisation du marché des télécommunications ;
- assurer la protection du citoyen car celle-ci est indispensable au développement des nouveaux médias ; la protection du consommateur ce qui implique que l'offre de nouveaux services doit être transparente ; la protection des données ce qui nécessite le respect du principe de la non collecte de données personnelles, préservant dans la mesure du possible l'anonymat ;
- mettre en place un cadre réglementaire favorisant le développement de nouveaux services : il s'agit d'adapter la loi relative au droit d'auteur, réfléchir au cadre juridique permettant de reconnaître la validité d'une signature digitale.

Les allemands ont une conception très proche de la notre en ce qui concerne les actions à mener relatives à Internet ; tout comme l'État français, l'Etat fédéral ne tolérera pas que le multimédia permette la diffusion de programmes illégaux tels que la pornographie enfantine ou l'expression d'opinions extrémistes ; outre une adaptation du Code pénal, le ministre allemand estime nécessaire de se mettre d'accord au niveau international sur ce qui possible et souhaitable dans la lutte contre l'utilisation abusive d'Internet. Par ailleurs, il estime que la loi doit définir clairement qui est responsable des contenus sur Internet. Pour lui, les responsables sont les personnes qui produisent et qui offrent ces contenus. L'autocontrôle des offreurs revêt donc une importance capitale. Ce n'est que lorsque l'autocontrôle, exercé par les utilisateurs, échoue que l'État doit intervenir.

* Les Länder, en revanche, ont une approche beaucoup plus traditionnelle et veulent appliquer à l'Internet un modèle plus contraignant, comparable à celui de la radiodiffusion.

L'initiative assez rapide du ministre fédéral pour dévoiler les grandes lignes d'une loi multimedia vise à fixer un cadre dans lequel devront s'insérer les initiatives des Länder et limiter, par là, les tentations trop restrictives de ceux-ci, avant toute décision relative aux compétences respectives du Bund et des Länder.

En Grande-Bretagne

L'exemple anglais est intéressant car il favorise une autorégulation des contenus dans une approche de droit commun à orientation libérale.

Le ministre des sciences et des technologies, Ian Taylor a eu récemment l'occasion de résumer l'approche britannique de l'Internet : selon lui, le cadre législatif actuel est suffisamment solide pour s'adapter aux nouveaux supports électroniques et les lois actuelles permettent de

sanctionner les contenus illégaux ; cependant il est certain que le développement du réseau risque d'aggraver le risque d'occurrence de tels contenus notamment ceux de pornographie infantine, même si les informations manifestement illégales sont aujourd'hui marginales ; les industriels doivent donc coopérer afin de limiter les poursuites judiciaires. Pour les contenus non pas illégaux mais offensants, le Gouvernement, en dépit de fortes pressions de la part de l'opinion publique, préfère l'autorégulation des acteurs. Face à un marché en pleine expansion, il importe de favoriser l'innovation et les initiatives plutôt que de risquer de brider celles-ci par une réglementation trop « efficace » ; les industriels doivent donc adopter des codes de bonne conduite à l'image de celui élaboré dernièrement par l'Internet Service Providers Association (ISPA).

Ce Code, qui a vocation à s'appliquer aux membres de l'Internet Service Providers Association, se divise en trois parties traitant des exigences générales, des règles de promotion des services et des procédures et sanctions.

Les exigences générales portent sur :

- la légalité : obligation de ne pas offrir des services contraires à la loi,
- la décence : obligation de faire son possible pour s'assurer que les services offerts ne comportent pas de contenu à caractère violent, sadique, ou racial ou que ces services ne permettent pas ou ne facilitent la prostitution ;
- l'honnêteté : obligation de s'assurer que les services ou contenus n'induisent pas en erreur par exagération, omission ou ambiguïté ;
- la protection des données : obligation lorsque les données sont enregistrées de les communiquer en vue de permettre une régulation des contenus ; l'ISPA pouvant être un potentiel utilisateur de ses données, obligation d'informer l'utilisateur sur l'usage qu'il est fait de données à caractère personnel le concernant (comme le nom et l'adresse) ; obligation de donner la possibilité à l'utilisateur d'empêcher cet usage.
- loyauté du service : obligation d'agir décemment, honnêtement et raisonnablement, notamment dans les relations avec les consommateurs.

Les obligations relatives à la promotion des services portent sur :

- le champ d'application : obligation de se conformer aux règles du Code de bonne conduite dans les annonces faites par voie de presse, de radiodiffusion, de téléphone ou de fax ;
- l'information sur les prix : obligation de s'assurer que le prix du service est clairement spécifié dans les annonces promotionnelles, incluant la TVA le cas échéant ; toute charge additionnelle doit être précisée ;
- la présentation du prix : obligation de présenter de manière lisible, horizontale afin de ne pas nécessiter un examen minutieux.

Les procédures et sanctions sont les suivantes :

- l'introduction de la plainte : la procédure exacte d'introduction de la plainte n'est pas encore définie faute de statistiques fiables sur le nombre de plaintes qui seront déposées.

Deux procédures sont possibles :

- la plainte peut être effectuée directement par un particulier auprès d'un membre de l'association ; celui-ci doit prendre les mesures nécessaires pour y répondre ; si le membre de l'association n'apporte pas de réponse satisfaisante au particulier, celui-ci peut saisir le secrétariat de l'ISPA ;
- la plainte peut être déposée directement par un particulier au secrétariat de l'ISPA ; une fois le secrétariat saisi, la procédure suivie dépendra de la nature de la plainte. Le secrétariat a la charge de l'instruction de la plainte, il est autorisé à effectuer des consultations (par exemple auprès de l'Office of Faire Trading).

Le secrétariat s'engage à contacter, dans un premier temps de manière informelle, le membre de l'association mis en cause ; si celui-ci est en mesure de se conformer aux décisions du secrétariat mais refuse de le faire, ou si le membre viole de façon répétée le code de bonne de conduite, le secrétariat sera en droit d'enregistrer la plainte de manière formelle et de la notifier au membre concerné. Les membres s'engagent à respecter les décisions du secrétariat, y compris les décisions de sanctions. Dans le cas où un membre viole de manière répétée le code, le secrétariat peut l'exclure de l'ISPA.

* Une autre illustration de l'approche de régulation des britanniques est celle mise en place pour les services audiotex.

Ceux-ci sont sous le contrôle de l'ICSTIS, Independent Commuter for the Supervision of the Standards of Telephone Information Service, organisme de droit privé, reconnu par le directeur général des Télécommunications.

Les missions de l'ICSTIS sont les suivantes :

- édicter des normes en relation avec le contenu et la promotion des services audiotex à tarifs majorés (kiosque) ;
- surveiller ces services audiotex et s'assurer que les normes susvisées sont appliquées grâce à des contrôles aléatoires ; les services qui ne sont pas préenregistrés, doivent être enregistrés en direct, l'ICSTIS pouvant visiter les locaux sans avertissements afin de les vérifier et d'interroger les animateurs sur leur connaissance des règles déontologiques ;
- instruire les plaintes du public en relation avec le contenu et la promotion de ces services ;
- publier des rapports sur le nombre et la catégorie des plaintes reçues et les actions prises pour y remédier.

Le président et les membres de l'ICSTIS sont nommés par les autres membres, sous réserve de l'approbation de l'OFTEL.

Il existe deux comités consultatifs : le premier gère les relations ICSTIS - opérateurs de télécommunications, le second gère les relations ICSTIS - fournisseurs de services. Ces comités sont présidés par le président de l'ICSTIS.

Le budget de l'ICSTIS de 13,6 MF est prélevé sur les revenus de l'industrie de l'audiotex selon un pourcentage variable et selon des budgets annuels agréés par les opérateurs de réseaux.

Aux termes de contrats les liant aux opérateurs de télécommunications, les fournisseurs de services sont obligés d'appliquer les règles édictées par l'ICSTIS et contenues dans un Code de déontologie. Si un fournisseur de services ne respecte pas les dispositions ci-dessus, l'ICSTIS recommande alors à l'opérateur de télécommunications de couper ledit service.

Le schéma est donc celui d'une régulation stricte par les industriels eux-mêmes avec des moyens conséquents donnés à l'organisme de contrôle.

Chapitre 4

Les propositions et les pistes de réflexion

Pour formuler des recommandations et, compte tenu des difficultés et des spécificités évoquées plus haut, il importe de préciser l'objectif de la France concernant Internet.

Ce réseau offre des possibilités exceptionnelles d'échange et d'information. Il ouvre de nouvelles pistes de croissance et de création d'emplois ; il faut le développer et combler notre retard. Dans le même temps, il ne constitue pas seulement le développement d'une nouvelle technologie ; son succès, son universalité en font un nouvel espace social justifiant l'élaboration de nouvelles règles de comportement, celles d'une « nouvelle civilité ». La tradition française est celle des valeurs humanistes, respectueuses des droits et libertés de chacun ; il importe dès lors de favoriser la reprise de celles-ci par le réseau afin que celui-ci soit un outil de progrès et d'enrichissement plutôt qu'un synonyme de danger.

Quatre convictions méthodologiques tout d'abord :

- une démarche purement nationale est illusoire ;
- une démarche trop hâtive peut être contre productive : l'arsenal juridique actuel permettant de garantir le respect, sur le territoire national, des principales libertés individuelles et de l'ordre public, il convient, à court terme, d'analyser, de comprendre l'évolution de ce nouveau marché et de faciliter l'application et l'adaptation du droit actuel ;
- aucune démarche univoque ne sera efficace : il n'existe pas un remède, une solution unique pour répondre à la question du contrôle des contenus d'Internet ; à l'encadrement législatif et réglementaire doivent s'adjoindre des approches contractuelles, consensuelles, pédagogiques ou informationnelles ; ces approches correspondent à la sociologie du réseau (libertarisme post soixante-huitard) et répondent, dans certains cas, de façon plus efficace, à l'exigence de déontologie ;
- enfin, toute politique devra être orientée de façon positive, de façon offensive pour le développement des services français sur Internet, plutôt que de se limiter à un arsenal défensif.

Compte tenu de ces principes méthodologiques, les propositions pourraient être les suivantes.

Préférer l'autocontrôle au contrôle *a priori*

Par sa structure d'interconnexion de plus de 70 000 réseaux et son mode de fonctionnement actuel, Internet semble difficilement s'inscrire dans un schéma de contrôle administré de type contrôle *a priori* : aucune autorité unique ne gère les flux de données, chacun peut à tout moment et de sa propre initiative être émetteur et récepteur d'informations ; celles-ci enfin ne connaissent pas les frontières. 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.

Dès lors, les formalités actuelles extrêmement simplifiées de prestations d'une offre de service en ligne sont suffisantes et doivent être demandées au fournisseur de service et à l'éditeur (simple déclaration de l'article 43 de la loi de 1986), une telle déclaration pouvant même être supprimée pour les simples pages d'accueil individuelles, offertes par la plupart des fournisseurs de services à leurs abonnés ; ces déclarations doivent permettre d'identifier l'offreur, les services qu'il héberge ou qu'il édite. La seule question éventuelle est celle de savoir auprès de quelle autorité elles doivent se faire : Procureur de la République ou Comité des services en ligne ?

Dès lors, l'objectif sera, outre celui de mettre en place un contrôle *a posteriori* de droit commun efficace, de favoriser l'autocontrôle des acteurs.

Un contrôle *a posteriori* efficace

Le système qui doit être mis en place pour les services en ligne s'inspire de l'approche de la presse : « tout est autorisé sauf ce qui est interdit ». C'est donc l'application du droit commun et la sanction *a posteriori* par le juge.

Une telle approche nécessite une justice plus rapide et plus avertie des questions spécifiques d'Internet qu'elle ne l'est aujourd'hui.

En effet, un moyen efficace de dissuader les contrevenants d'Internet sur le territoire national est de mettre en place une procédure judiciaire rapide et efficace.

Pour cela, il faut tout d'abord informer l'institution judiciaire sur la nature, les services qu'offrent le réseau et les nouveaux délits qu'il peut susciter afin de définir progressivement les orientations d'une politique pénale ; une circulaire d'information pourrait être envoyée aux parquets, rappelant le droit applicable, le souci de favoriser des procédures rapides et de centraliser informations et poursuites à la Chancellerie afin de constituer rapidement un noyau d'expérience et de compétence ; faut-il aller plus loin et créer des « cyberjuges ». Outre les difficultés juridiques

que cela poserait, il semble plus utile de disséminer la formation dans tout l'appareil judiciaire, conformément au caractère décentralisé du réseau, tout en créant un lieu de centralisation de l'expérience acquise.

En revanche, la création de forces d'enquête spécialisées (cybergendarmes) apparaît souhaitable pour garantir une intervention rapide et efficace contre toute forme de délinquance sur le réseau.

Au-delà de la formation des juges, les délits commis sur Internet, éminemment volatiles et fugaces appellent des procédures nouvelles : le droit pénal permet au Procureur de la République de prendre toute mesure nécessaire pour faire cesser ces infractions ; cette disposition a fondé la saisie des matériels informatiques dans l'affaire *Worldnet c/ Francenet*. Dans certains cas, un dispositif plus léger serait utile et plus respectueux de la liberté d'expression : que penser en effet d'un serveur d'hébergement sur lequel un tiers aurait, dans l'intention de lui nuire, téléchargé des contenus délictueux et qui serait immédiatement saisi ; une procédure **d'injonction** pourrait être imaginée et, en cas de refus de l'intéressé, être suivie d'une saisie.

Favoriser l'autocontrôle des acteurs

L'autocontrôle peut être défini comme toute démarche volontaire sur les contenus des différents acteurs dans un souci de protection de la personne.

Il permet :

- un contrôle en amont de la réception du message, au niveau de l'utilisateur ou de l'éditeur de contenu ;
- au niveau de l'utilisateur : le contrôle technique ;
- au niveau de l'éditeur de contenu : les codes de déontologie ;
- entre les différents acteurs : les contrats.

Le contrôle par les utilisateurs

Le contrôle par les utilisateurs existe depuis longtemps sur le réseau à travers la Net étiquette : cette civilité mondiale veut faciliter la bonne utilisation du réseau par des règles de comportements non écrites (pas de publicité, pas de questions redondantes dans les forums,...) mais aussi faire respecter quelques valeurs universelles. Il faut développer cette étiquette, peut être la formaliser.

Outre ces règles générales, des dizaines de dispositifs techniques existent déjà auprès des fournisseurs américains et consistent en des logiciels de filtrage (Cyberpatrol, Netnanny,...) à disposition des parents interdisant l'accès à des sites comportant des mots-clés prédéfinis ; ces systèmes sont utiles dans la mesure où, à l'initiative de l'utilisateur, ils restreignent l'accès à des sites intuitifs ; cependant, leur efficacité est limitée : ils écartent de la même manière tout message inscrit sous le même mot-clé, quelle que soit l'orientation, délictueuse ou non ; ils peuvent conduire, de façon extrême, à bannir du vocabulaire d'appel des

enfants et des parents, tout mot pouvant susciter une interprétation suspecte; enfin ils peuvent, dans certains cas, déresponsabiliser les parents, faisant confiance à la machine pour assurer la surveillance de leurs enfants.

Certains moteurs de recherche (Altavista, Webcrawler) ont d'ores et déjà pris la décision de filtrer leurs logiciels à partir de mots clés «interdits»; Yahoo, quant à lui, intègre tout ou partie de la technologie de Surfwatch au sein d'un site dédié aux enfants.

Toutes ces initiatives sont intéressantes même si la prolifération des sites Internet justifie une mise à jour permanente des listes de diffusion autorisées; elles responsabilisent les utilisateurs et permettent d'établir au sein d'une communauté les mêmes valeurs.

Une démarche plus complète est celle de l'association PICS, association regroupant de grands acteurs américains (Apple, AOL, AT&T, CompuServe, Netscape,...) et France Télécom et offrant un système de classification des sites selon quatre critères (violence, nudité, sexe et textes) et cinq niveaux d'acceptabilité. L'objectif ici n'est plus seulement restrictif mais aussi informationnel. La difficulté dans ce cas est celle de l'organisme de classification et de sa représentativité et également celle du respect, par des initiatives largement anglosaxonnes, de la sensibilité spécifique européenne.

Il conviendrait dès lors, soit d'inciter chacun des éditeurs à s'autoclassifier soit de faire en sorte que plusieurs institutions indépendantes, proposent leurs propres classification selon des critères variés: l'on aurait ainsi par exemple la sélection des sites Web par les associations familiales, ou celle d'un journal, ou celle de l'Education nationale, chacun de ces organismes, en fonction de leur public de chalandise, recommandant ou non certains sites.

Les codes de déontologie

De tels codes existent aujourd'hui dans la télématique; il faut les étendre et les adapter aux services en ligne.

Il est en effet prévu que les recommandations déontologiques du CST figurent en annexe aux contrats liant France Télécom aux fournisseurs de services; ces recommandations fixent des objectifs généraux de respect de la personne, de loyauté du service... Elles font partie des obligations contractuelles sur la base desquelles se déroule la prestation.

Les professionnels de l'Internet, fournisseurs d'accès, éditeurs, commerçants électroniques, doivent progressivement définir les conditions d'un développement harmonieux de leurs activités, dans le respect des droits de la personne et du consommateur. L'exemple britannique pour les fournisseurs d'accès est particulièrement éclairant et aborde la plupart des questions de déontologie évoquées plus haut; de tels codes pourraient ainsi rappeler l'application du cadre légal français, fixer un cadre

déontologique minimum, fixer les règles de responsabilités, fournir des contrats-types à l'instar de ce qui est prévu dans le cadre de déontologie actuel proposé par l'AFTEL, favoriser enfin la reconnaissance de label de qualité des prestataires.....

Les professionnels ont intérêt à la mise en place de tels codes car l'absence de démarche volontaire risque de conduire le gouvernement à une démarche plus administrée ; les pouvoirs publics y ont intérêt car l'adoption de ces codes par les professionnels eux-mêmes garantit de façon assez efficace, et conformément avec l'approche traditionnelle du réseau, le respect des droits de la personne et du consommateur. Les seules questions seront celles de l'agrément ou non de tels codes par les pouvoirs publics ou le comité des services en ligne ainsi que la détermination de l'instance professionnelle représentative.

Les contrats

Les contrats peuvent donner une base légale à un filtrage du contenu sans susciter de réactions négatives de type censure. Deux contrats sont intéressés à ce titre : le contrat abonné/fournisseur, le contrat éditeur/serveur d'hébergement.

Un fournisseur de services peut ainsi s'engager auprès de ses abonnés de type familial à ne pas donner accès à des serveurs délictueux ; il constitue ainsi autour de lui une communauté de sensibilités qui partage les mêmes valeurs et le délègue pour les faire respecter. Une telle solution risque cependant de modifier le métier du fournisseur d'accès qui de distributeur du contenu va devoir surveiller celui-ci ; cela ne semble pas souhaitable, le contrôle parental, à la réception du message semblant préférable et facile à mettre en oeuvre.

L'autre contrat permettant de faire peser, de façon volontaire, des obligations sur le contenu est celui liant l'éditeur au serveur d'hébergement ; ce contrat peut prévoir le respect d'obligations concernant les mineurs, les consommateurs,... Il faut développer de tels contrats et prévoir éventuellement des contrats types recommandés par le comité des services en ligne ou par les différentes associations des professionnels de l'Internet.

Un cas particulier intermédiaire entre ces 2 contrats est celui de la page d'accueil de l'utilisateur : dans celle-ci, l'utilisateur/abonné devient éditeur et peut être soumis aux mêmes types d'obligations contractuelles que les autres éditeurs hébergés par le serveur.

Clarifier les responsabilités des acteurs

La question de la responsabilité est une question juridique majeure concernant Internet ; elle ne concerne évidemment que les services en ligne de type « audiovisuels ». Qui est responsable et donc éventuellement coupable d'un message délictueux au regard de droit français ? Que répondre dans le cas d'un serveur « miroir » installé sur notre territoire qui ne fait que réémettre de l'information venue d'ailleurs ? Dans le cas d'un serveur hébergeant quelques milliers de « home page » modifiables à tout moment par les intéressés ? dans le cas, plus connu maintenant après le référé UEJF, des news groups ? Dans le cas enfin, de « pointeurs » Web, partant d'un serveur « sain » vers un délictueux ? Les questions sont d'autant plus délicates que chacun, à tout moment, peut devenir éditeur. Le schéma de responsabilité doit donc être clarifié, compte tenu des principes généraux de mise en jeu de la responsabilité pénale.

Les principes de mise en jeu de la responsabilité pénale

Dans le droit commun, une personne physique engage sa responsabilité quand il est prouvé qu'elle a matériellement exécuté l'acte prohibé par la loi. Elle est considérée comme l'auteur matériel des actes constitutifs de l'infraction qu'elle a accompli personnellement. Le ministère public doit, dans ce cas, faire la preuve non seulement de la réalité du fait délictueux mais aussi de l'élément intentionnel de son auteur.

À titre exceptionnel, la loi considère comme auteur, quelqu'un qui n'a pas accompli lui-même l'acte matériel constitutif du délit, mais qui a été simplement la cause intellectuelle de la commission de celui-ci. Il est alors prévu une présomption de faute. La faute qui consistera alors en une négligence résultant du seul fait de la violation ou du non-respect des prescriptions légales ou réglementaires n'a pas à être démontrée par le ministère public ; elle est présumée, et ne tombe que devant la preuve de l'absence de faute. Si cette preuve ne peut exonérer l'auteur, il y a présomption de responsabilité.

Le régime de responsabilité de la presse et de l'audiovisuel se distingue du droit commun par un certain nombre de caractères spécifiques

La responsabilité éditoriale a été instaurée pour la presse écrite par la loi du 29 juillet 1881, étendue aux services de communication audiovisuelle par la loi du 29 juillet 1982, et maintenue en vigueur par la loi du 30 septembre 1986 relative à la liberté de communication.

Le législateur a souhaité instaurer un principe de responsabilité particulier, dérogeant au droit commun, afin de simplifier son éventuelle

mise en jeu. Le système réside dans le principe de la responsabilité de plein droit en cascade, c'est-à-dire la détermination *a priori* et automatique d'un responsable : le directeur de la publication, à défaut, l'auteur, et à défaut l'imprimeur, puis les vendeurs, les distributeurs et les afficheurs (article 42 de la loi du 29 juillet 1881).

Toutefois, le régime général de responsabilité subsiste parallèlement à ce régime spécifique et la responsabilité éditoriale ne s'applique qu'aux infractions de presse prédéterminées par la loi (chapitre IV de la loi de 1881).

Ces infractions sont les suivantes :

- provocation aux crimes et délits ;
- provocation à la discrimination, à la haine ou à la violence raciale (loi du 1^{er} juillet 1972 modifiée par la loi du 13 juillet 1990) ;
- délit contre la chose publique ;
- délit contre les personnes (diffamation, injure) ;
- délit contre les chefs d'État ;
- diffusion de publications interdites (actes d'accusation de procédures criminelles avant leur lecture publique, etc.).

Pour assumer cette responsabilité, le directeur de la publication doit être à même de contrôler les messages diffusés, c'est pourquoi l'article 93-3 de la loi du 29 juillet 1982, introduit par la loi du 13 décembre 1985 précise que le régime de la responsabilité en cascade ne s'applique que « lorsque le message incriminé a fait l'objet d'une fixation préalable à sa communication au public », c'est-à-dire lorsqu'il y a eu enregistrement. De ce fait, en cas d'émissions en direct, seule la responsabilité personnelle de celui qui a commis l'infraction peut être engagée.

De plus, les dispositions de la loi de 1881 et de celle de 1982 prévoient que les auteurs peuvent être poursuivis comme complices.

Plusieurs dispositions du Code pénal ont rendu applicables le jeu de la responsabilité éditoriale à des infractions de droit commun commises par voie de presse écrite ou audiovisuelle.

C'est notamment le cas de l'infraction de l'article 227-24 du Code pénal qui punit le fait, soit de fabriquer, de transporter, de diffuser par quels que moyens que ce soient 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.

Aux termes de l'article 227-28 du Code pénal, l'application de la responsabilité éditoriale est étendue aux infractions des articles 227-18 à 227-23 du Code pénal :

- provocation de mineurs à l'usage de stupéfiants ;
- provocation de mineurs à la consommation habituelle et excessive de boissons alcooliques ;
- provocation de mineurs à la mendicité ;

- fixation, enregistrement ou transmission de l'image d'un mineur présentant un caractère pornographique.

La télématique a emprunté le régime de responsabilité du droit de la presse et de l'audiovisuel

À l'exception des services qui relèvent exclusivement de la correspondance privée, tous les autres services télématiques constituent des services audiovisuels au sens de la loi du 30 septembre 1986 modifiée auxquels s'appliquent les dispositions de l'article 93-2 de la loi du 29 juillet 1982 modifiée par la loi du 13 décembre 1985.

En matière de responsabilité pénale, la jurisprudence a estimé que les délits télématiques ne sont pas commis par voie de presse lorsque les services ne constituent pas des publications de presse au sens de la loi du 1^{er} août 1986 (message écrit, périodicité). Seuls les services proposant la consultation d'une base de données dont le contenu est préenregistré sont susceptibles d'engager la responsabilité pénale du directeur de publication pour les délits prévus au chapitre IV de la loi de 1881.

En outre, les fournisseurs de services doivent signer une convention avec France Télécom et s'engagent ainsi à respecter les lois et règlements en vigueur et l'image de marque de l'exploitant. Une annexe des conditions générales prévoit le respect d'un certain nombre de règles d'ordre déontologique (rappel des dispositions pénales applicables à la télématique, engagements de déontologie professionnelle et de surveillance des informations mises à disposition du public et des modalités de promotion publicitaire des services). France Télécom a le pouvoir de suspendre ou de résilier le contrat. Cette sanction doit observer un certain nombre de formalités (mise en demeure, respect des délais, consultation du comité de la télématique anonyme).

Il convient de rappeler que les juridictions ont toujours admis la non-responsabilité du centre serveur, par fourniture de moyens ou complicité. Le serveur est responsable du bon fonctionnement du service informatique mais s'exonère de toute responsabilité lorsque le dommage est dû à une faute de l'utilisateur. Seul le fournisseur de service a la maîtrise de la forme et du contenu du service.

Le juge a consacré le principe de la neutralité du transporteur (France Télécom) de messages. Cette exonération de responsabilité est toutefois subordonnée à l'absence de connaissance du délit ou de la violation de l'engagement contractuel avant ou au moment de la commission des infractions. (arrêt *Midratel* du 17 novembre 1992); dans cet arrêt, la Cour de cassation a consacré l'imputation du délit de l'article 284 alinéa 2 du Code pénal au fournisseur de service, à titre principal pour avoir fait en sorte que « publiquement, l'attention soit attirée sur des occasions de débauche ».

Cette position jurisprudentielle est à rapprocher des dispositions contractuelles aux termes desquelles le fournisseur de service s'engage à « effectuer une surveillance constante des informations mises à la disposition du public de manière à éliminer au maximum avant affichage les messages publics mêmes reçus en direct et susceptibles d'être contraires aux lois et règlements en vigueur (..) La mise en oeuvre de ces obligations fera l'objet de la part du fournisseur de service de contrôles aléatoires effectués manuellement ». Le fournisseur peut ainsi voir sa responsabilité engagée à raison du contenu du service transmis.

La preuve de la faute, ayant pour objet une information transmise électroniquement, soulève de nombreuses difficultés dues au caractère instantané et fugace des messages diffusés. En vertu du décret du 6 avril 1987, le directeur de la messagerie se voit cependant imposer une obligation de conservation des messages. La plupart des messages des services télématiques font l'objet d'une mémorisation avant leur mise à disposition du public mais tel n'est pas toujours le cas, le stockage des informations dépend de la nature du message (boîtes aux lettres, pseudonymes, annonces...).

En outre, les messageries de correspondance privée ne peuvent être concernées.

Les options possibles

Compte tenu de ces rappels, où trouver une logique pour guider le raisonnement alors qu'Internet apparaît comme un nouveau monde de communication ?

Une première règle doit être énoncée : l'éditeur, créateur de l'information mise en ligne, personne ou société, est responsable en premier chef de cette information. Il faut donc pouvoir **l'identifier** ; Internet n'étant pas un monde anonyme cela semble envisageable et les différents acteurs (serveurs d'hébergement, IAP, transporteur) doivent s'engager à fournir le l'identité de l'auteur en cas de procédure judiciaire ; en revanche, toute personne qui consulte des informations doit pouvoir rester anonyme à condition éventuellement qu'elle soit habilitée à les consulter (par login et mot de passe sans relation avec l'identité).

Une deuxième règle doit suivre : on ne peut être responsable que de ce que l'on est capable de contrôler; de ceci découle une exonération de responsabilité pénale de la fonction de fourniture d'accès dès lors que celle-ci est purement technique, sans intervention éditoriale. Ces postulats étant posés, quel schéma de responsabilité envisager ?

Transposition du droit spécifique de la presse et de l'audiovisuel

Dans la logique de l'évolution du droit de la communication, la solution la plus immédiate consiste à transposer en l'adaptant le régime

de la responsabilité éditoriale ; celui-ci s'applique, dès à présent, aux services de l'article 43 de la loi de 1986 sur la liberté de communication.

Sur la base du **régime de la presse**, l'implication des acteurs s'ordonnerait de la façon suivante :

- le directeur de la publication au sein de l'éditeur de contenu ;
- l'auteur du message incriminé ;
- l'imprimeur : entité chargée de la médiation informatique, le serveur d'hébergement ;
- le diffuseur ou l'afficheur : centre d'hébergement, fournisseur d'accès ou transporteur.

Sur la base du **régime de l'audiovisuel** : directeur de la publication ; auteur ; producteur : le serveur d'hébergement.

Compte tenu de ces éléments, le régime de responsabilité en cascade qui s'appliquerait aux services en ligne serait le suivant : le premier maillon juridique de la chaîne serait l'éditeur de contenu ; en second lieu, l'auteur, ces deux entités pouvant être confondues dans le cas d'un éditeur individuel ; en troisième lieu, la plate-forme d'intermédiation technique du serveur d'hébergement.

En revanche ne serait pas compris dans la cascade le fournisseur d'accès qui se borne à mettre en contact l'utilisateur avec le réseau, sans choix des services consultés et sans contrôle éditorial de ceux-ci ; serait exclu également le transporteur du fait du principe de neutralité en matière de télécommunications. Une responsabilité de droit commun, en revanche, serait toujours applicable à ceux-ci.

Avantages du système

* Les victimes de l'infraction sont toujours assurées de trouver un responsable ce qui, dans le cas d'un réseau où les éditeurs de contenus sont à 80 % hors du territoire national, garantit le respect d'un certain état de droit.

* L'automatisme de la cascade en fait un mécanisme simple et connu à mettre en oeuvre par le juge évitant les procédures judiciaires longues.

* Le fait d'être exclus de la cascade, comme pour les fournisseurs d'accès ou les transporteurs, les exonère de toute responsabilité éditoriale sauf pour le juge à démontrer le contraire.

* Un même message se verra identiquement contrôlé quel que soit le support d'accès par le consommateur : presse, audiovisuel et « on line ».

* Une telle présomption n'est pas irréfragable : les mis en cause pouvant toujours démontrer leur innocence.

Inconvénients du système

* Rendre le serveur d'hébergement responsable, même par défaut, d'un message délictueux risque de porter atteinte au développement du réseau Internet en France dans la mesure où beaucoup de ces serveurs n'ont aucune responsabilité éditoriale réelle sur les informations stockées chez eux. Les news groups ou les serveurs miroirs par exemple, ne font que reprendre de l'information produite hors de France les home pages ne sont pas sous le contrôle du serveur ; le risque est dès lors grand de voir une partie non négligeable de l'activité en ligne quitter le territoire national vers un pays à législation moins restrictive.

* Le système de la cascade, par la fixation préalable des responsables potentiels, implique la connaissance exhaustive de ceux-ci et l'invariabilité de leurs fonctions ce qui, dans le cas d'Internet, ne sera pas toujours vérifié.

* La cascade nécessite la fixation préalable du message, formalisme qui devra éventuellement s'adapter aux réseaux ouverts.

Application aux services en ligne des règles de droit commun

L'autre solution est d'appliquer aux réseaux ouverts au public comme l'Internet un système de responsabilité de droit commun : en effet ces réseaux, en raison de leur spécificité (immatérialité du contenu, extraterritorialité et diversité des législations nationales, étendue des secteurs d'activité concernés, opacité juridique des liens entre acteurs, structure non centralisée du réseau et variabilité du rôle des acteurs...) constituent un nouvel espace de communication, sans rapport avec celui de la presse et de l'audiovisuel pour lequel il faut peut être inventer des règles particulières ; ils ne mettent pas en jeu la seule responsabilité de professionnels mais celle de tout utilisateur.

Dans ce cas et compte tenu des deux postulats énoncés plus haut, tous les acteurs (auteur, hébergeur, fournisseur d'accès, transporteur) pourraient être poursuivis comme auteurs principaux, coauteurs ou complices si ils ont sciemment mis à disposition du public des services contraires à l'ordre public dès lors que le ministère public aura prononcé leur participation à l'infraction et à charge pour celui-ci d'analyser les circonstances atténuantes éventuelles de chacun. Une telle solution est souple, permet de faire du cas par cas en fonction des responsabilités réelles de chacun ; elle part du principe de liberté et d'absence de responsabilité sauf à démontrer l'intention coupable ; elle correspond tout à fait aux principes de fonctionnement d'Internet, pragmatique et concret.

Une telle responsabilité ne doit pas conduire les fournisseurs d'accès ou les transporteurs à surveiller *a priori* les messages transitant chez eux ; en revanche, si il apparaît qu'après un avis négatif sur un service donné par le comité des services en ligne ils ont maintenu l'accès au dit service, l'intention coupable pourra être démontrée.

Sa principale faiblesse tient à l'incertitude juridique qu'elle peut créer auprès des acteurs, aucun d'entre eux, même les transporteurs, n'étant *a priori* exonéré de toute responsabilité. Elle peut donc également, quoique de façon moins automatique, favoriser le départ d'opérateurs du territoire national.

Conclusion

Compte tenu des éléments ci-dessus mentionnés, il apparaît que le choix entre chacune des deux solutions est moins d'ordre technique que politique ; la mission pense qu'il est préférable d'adopter la deuxième solution.

Développer la coopération internationale

Dans le cadre de la coopération judiciaire

Comme nous l'avons souligné le droit international privé et le droit pénal international apportent de nombreuses solutions. En effet déjà les mécanismes généraux de l'extradition et de l'entraide répressive internationale peuvent, si les conditions de forme et de fond sont réunies, trouver à s'appliquer en cas d'infraction de droit commun commis sur Internet.

En outre, certaines conventions règlent les problèmes de conflit de loi par exemple la convention de Bruxelles de 1968, telle qu'interprétée par la Cour de Justice des Communautés européennes, en accordant à la victime d'une diffamation un large choix quant à la juridiction civile devant laquelle elle entend faire réparer son dommage.

Enfin, l'International users requirements, adopté par le conseil des ministres de l'Union européenne en janvier 1995, prévoit l'obligation pour les opérateurs de réseaux de télécommunications de permettre l'interception des télécommunications aux autorités légalement autorisées.

De même, l'exequatur des décisions judiciaires est quasiment automatique pour les décisions prononcées par les juridictions des pays partis à la convention de Bruxelles de 1968.

Cependant des difficultés demeurent ; pour pallier celles-ci et favoriser l'entraide des États pour la répression des crimes et délits les plus graves commis sur Internet, il serait opportun de mettre ces questions à l'ordre du jour des réunions des États membres du Conseil de l'Europe signataires de la convention européenne d'extradition du 13 décembre 1957 et de la convention européenne d'entraide judiciaire en matière

pénale du 20 avril 1959 et solliciter des experts leur point de vue sur le sujet ; d'ores et déjà, la recommandation 95 R 13 du Conseil de l'Europe relative aux problèmes de procédures pénales liées à la technologie de l'information pourrait fournir les bases d'une entraide judiciaire; il convient de mettre certaines de ces propositions en application dans chacun des pays ; par ailleurs, d'éventuelles modifications ou assouplissements pourraient être utilement apportés à ces textes internationaux.

Les grands absents de ces conventions sont les États-Unis avec lesquels la France est liée pour l'extradition par un accord du 6 janvier 1929 ; cet accord a la particularité de lister les infractions permettant la mise en oeuvre de la procédure d'extradition. En revanche, il n'y a aucun accord avec les USA en matière d'entraide répressive internationale ; ne serait-il pas opportun de mettre en place un accord ad hoc qui compléterait utilement la nouvelle convention d'extradition récemment signée et non encore ratifiée ? A court terme, il pourrait être envisagée la création de magistrats de liaison entre la France et les USA à l'instar de ce qui existe déjà avec l'Italie et les Pays-Bas.

Enfin, un mécanisme de coopération « informationnelle » du type Interpol pourrait être imaginé pour Internet.

Dans le cadre de la coopération politique Au sein de la communauté européenne

L'Union européenne est, par sa cohérence économique et culturelle l'instance internationale privilégiée pour élaborer, à l'instar de la directive Télévision Sans Frontière, des règles communes tant sur le respect d'une déontologie des contenus que sur des problèmes de méthodologie (responsabilité, loi applicable, coopération judiciaire).

Ces règles communes pourraient s'inscrire dans un projet de directive sur les services en ligne ; elles prévoiraient, ainsi, concernant la loi applicable, d'adopter le principe du droit du pays d'émission, ce qui serait cohérent avec les dispositions de la directive TSF et avec la reconnaissance de la responsabilité première de l'éditeur de contenus ; pour les pays non membres, l'on adopterait en revanche le droit du pays de réception ; des règles de transparence pourraient également être partagées notamment pour les services commerciaux.

Une telle harmonisation permettrait au marché européen de ne pas se fragmenter par des réponses nationales divergeantes et garantirait à l'utilisateur européen, citoyen ou consommateur, une certaine protection. En outre, il constituerait une forte incitation pour les étrangers et notamment pour les USA, de s'accorder avec l'Europe sur les conditions de l'édition sauf à se voir appliquer, en cas de conflit, le droit européen.

Concernant la coopération judiciaire, la recherche de règles communes, l'échange d'informations... seraient dans la logique du troisième pilier de l'Union européenne qui a pour vocation de lutter notamment contre les conséquences internationales indésirées de la libre

circulation des biens et des personnes ; bien que cette coopération intergouvernementale repose sur l'unanimité, elle permet de prendre une position commune cohérente et favorise une action concertée efficace.

Partageant cette volonté de développer la coopération européenne relativement à l'Internet, François Fillon a, lors du Conseil informel des ministres de la culture et des télécommunications d'avril 1996, indiqué que la France « était favorable à une initiative internationale sur la déontologie et la protection du consommateur ».

En dehors de la Communauté européenne

Les déclarations sur la société de l'information se succèdent dans des instances variées, le Conseil de l'Europe, l'OCDE, l'UIT...

Les problématiques évoquées vont de l'impact sur l'emploi et les conséquences sur l'équilibre Nord-Sud à la nécessité de faire tomber plus rapidement les monopoles sur les télécommunications et la réglementation sur la cryptographie.

Les réflexions qui ont démarré au sein du Conseil de l'Europe permettront sans doute de préparer une doctrine juridique commune sur différents aspects de la société de l'information, avec notamment l'extension du concept de service universel au contenu et la protection de l'individu ; cependant, ces efforts de fond visent le long terme et une certaine universalité.

L'OCDE sert aujourd'hui de forum à d'importantes négociations concernant l'avènement de la société de l'information et les éventuelles barrières commerciales entre états qui pourraient le retarder ; sont notamment examinées les modalités d'utilisation des moyens de cryptologie et la place que doivent ou peuvent se réserver les pouvoirs publics dans le domaine.

L'Union internationale des télécommunications (UIT), organisation spécialisée de l'ONU, chargée de favoriser le développement des infrastructures de télécommunication dans tous les pays, s'efforce de trouver un moyen de faire accéder tous les pays à l'Internet dans les meilleures conditions, notamment en sensibilisant les pays qui ont la capacité de déployer des infrastructures.

Ces nombreuses déclarations et recommandations sur la société de l'information illustrent la prise de conscience progressive qui se fait jour concernant Internet et la nécessité d'une harmonisation juridique minimale permettant de résoudre certains problèmes concrets et de réprimer efficacement et rapidement les abus les plus graves ; elles soulignent également la nécessité d'une approche empirique face à un phénomène dont personne ne maîtrise les implications réelles dans la société de demain en termes éthiques, culturels, économiques ou sociaux.

Dans cette perspective, la réunion du G7 de juin 1996 pourrait être l'occasion d'une déclaration solennelle commune des États qui inviterait à une réflexion conduisant à ce que les pays s'accordent sur un

minimum de principes communs, notamment pour la détermination de la loi applicable (pays d'émission ou de réception), la définition de responsabilités communes et le principe d'une coopération judiciaire accrue. Les membres du G7 pourraient également décider la création d'une cellule de conseil et d'expertise auprès d'eux afin d'éclairer leurs choix nationaux.

Dans les instances de l'Internet

D'après les contacts que la mission a pu avoir avec celles-ci, les différentes instances de l'Internet sont conscientes des questions qui agitent aujourd'hui le réseau et qui se font jour dans la plupart des pays.

Ces questions, dans la mesure où elles risquent de susciter l'insécurité des utilisateurs et, par là, freiner le développement du réseau, leur semblent inquiétantes ; nos interlocuteurs ont également reconnu que certains problèmes techniques ne peuvent être traités qu'au plan international (nommage, droit applicable,...). Dans ces conditions, une réflexion commune avec l'Internet Law and Policy Task Force pourrait être envisagée, à l'initiative française ou au niveau européen. Quelques exemples de champs de coopération non gouvernementaux :

- attribution des noms de domaines permettant à chaque utilisateur d'avoir une adresse mondiale pérenne lorsqu'il change de prestataire ou de région ;
- définir un lexique descriptif commun à l'ensemble des pays pour les services Web semble utile ; l'utilisateur serait par là assuré du type de contenu auquel il souhaite avoir accès ;
- chacun des NIC locaux pourrait enfin conditionner l'octroi d'un nom de domaine en respect de principes déontologiques. L'INRIA en France envisage cette possibilité ; de façon générale, la transparence des acteurs (identification, description des contenus, conditions des prestations...) doit être recherchée.

Le commerce électronique

Le caractère transnational, non centralisé et multiforme de l'Internet laisse une place restreinte à l'intervention des pouvoirs publics ; les questions de localisation du contrat, de loi applicable et de droit de la preuve ne feront sans doute pas l'objet à très court terme de réponses cohérentes et universelles. Par ailleurs, le droit positif semble difficilement s'accorder, de part son formalisme avec l'instantanéité des transactions commerciales qui interviennent dans le réseau. Dans ces conditions, la protection du consommateur s'organisera moins de façon centralisée et uniforme qu'à travers le contrat et grâce à des dispositifs techniques adaptés.

Le contrat permet en effet de fixer entre deux parties toutes les conditions nécessaires au bon déroulement de la prestation et notamment son lieu d'exécution et le droit applicable ; sa réalité et notamment l'authentification des parties sera assurée par différents procédés de type « signature électronique » que les experts doivent au plus vite valider aussi sûrement qu'une signature manuelle ; la jurisprudence a reconnu la validité des clauses contractuelles permettant de substituer à la signature manuscrite la signature électronique ; il faut poursuivre cette dématérialisation dès lors que la sûreté technique des procédés sera démontrée.

Néanmoins, l'intervention d'un **tiers** restera nécessaire, autant pour sécuriser la transaction, et éventuellement en garder la trace, que pour garantir la solvabilité de l'acheteur et la respectabilité commerciale du vendeur, assurer la prestation de confidentialité définie dans la nouvelle loi sur la réglementation des télécommunications, déclencher la transaction bancaire, garantir la qualité des prestations... Le commerce électronique sera vraisemblablement, à l'avenir, un « commerce à trois » et une nouvelle profession peut se constituer ; quelle sera la stratégie des différents acteurs du réseau (fournisseurs d'accès, serveurs de logiciels - Netscape) ? Voudront-ils se positionner ou laisseront-ils ces acteurs plus traditionnels comme les banques devenir des « cyber-notaires » ?

Une autre question doit être résolue, celle de la fiscalité des transactions commerciales sur Internet portant sur des biens immatériels ; celles-ci, aujourd'hui, échappent à toute forme d'imposition alors que de la valeur ajoutée transite sur le réseau ; la solution est peut-être celle d'une convention internationale fixant le principe d'une « salestax » levée par le pays de destination ; un tel schéma est cohérent avec le commerce des produits manufacturés ou des prestations de services et légitime, compte tenu des services publics du pays de destination dont bénéficie le consommateur ; la difficulté sera évidemment de déterminer les modalités de recouvrement de cette taxe et notamment les acteurs qui en seront chargés ; les tiers de confiance pourraient, à ce stade, jouer un rôle important, soit en offrant à la demande du client un service de validation fiscale de la transaction, soit en percevant automatiquement, à la demande des États, les taxes intéressant la transaction qu'ils auraient par ailleurs validé.

Ces adaptations et ces initiatives doivent permettre d'élaborer un cadre de confiance pour le consommateur final, condition nécessaire au développement du commerce électronique. Les acteurs eux-mêmes doivent se mobiliser pour définir une charte commerciale claire des droits et obligations des « commerçants » vis-à-vis du consommateur ; l'Association française pour le commerce et les échanges électroniques (AFCEE) pourrait y travailler et envisager même la création d'un label garantissant la qualité de la prestation de service et « l'honorabilité » du commerçant ; il importe de se mobiliser rapidement dès lors que les grands distributeurs américains, soucieux de satisfaire des consommateurs habitués à un haut niveau de service, ne manqueront pas d'adapter leurs pratiques à ce nouvel espace de distribution « virtuel ».

Créer un organisme de veille : le Comité des services en ligne

Face à l'extrême incertitude sur l'évolution d'Internet, ses techniques, ses usages et la stratégie des acteurs, il est utile de mettre en place un organisme de veille et d'analyse qui constituera progressivement un lieu d'expertise et « d'intelligence ». Cet organisme conseillera le Gouvernement et formulera recommandations ou avis en matière déontologique ou pour d'autres objets.

En outre, recevant les plaintes des usagers, le Comité pourra, sur demande de ceux-ci ou du Gouvernement, mener des enquêtes très rapides sur des sites jugés litigieux, ses conclusions étant de nature à être versées dans une procédure pénale ; cependant avant l'enclenchement de celle-ci, le comité pourra avoir un rôle de médiation entre les parties. L'objectif est par la conciliation de résoudre les principales difficultés sans entrer dans une procédure officielle qui par sa publicité risquerait plus de faire connaître les sites litigieux que de les empêcher.

Enfin, le comité développera ses liens avec les instances internationales, publiques et privées, compétentes sur Internet afin de favoriser la mise en place d'une coopération sur ces questions. La composition du comité sera équilibrée entre les différentes catégories d'acteurs de l'Internet ; son fonctionnement devra s'appuyer sur le réseau des associations, des groupes de réflexion ou d'experts déjà existants, afin que, léger et réactif, il puisse répondre en temps réel aux questions posées par le réseau.

L'articulation de ce nouveau comité avec les organismes de régulation existants devra être précisée : il se substitue au Conseil supérieur de la télématique dont il reprend les compétences, tout en procédant d'une logique et d'une approche différente ; Il devra s'articuler avec le CSA en matière déontologique afin qu'une cohérence s'établisse sur les contenus, quel que soit le support de communication.

Favoriser l'information, la formation et la mobilisation des acteurs publics et privés

Internet est une nouvelle forme de relation mondiale, « d'intimité » mondiale. Tout en s'efforçant de promouvoir la mise en place d'une déontologie sur le réseau et le respect d'un certain nombre de principes protecteurs des individus en tant que personnes ou en tant que consommateurs, il est nécessaire d'éduquer et de former les utilisateurs à ce nouveau monde. La « pensée critique » de ceux-ci, leur vigilance, est la meilleure garantie contre les excès du réseau et la meilleure protection

de la jeunesse ; comme l'on apprend à ses enfants à vivre, à se comporter au sein d'une ville, il faut que les parents et l'école apprennent aux enfants les avantages et les dangers d'Internet, ce qu'ils peuvent faire et doivent respecter ; en un mot une sorte de nouvelle « civilité ».

Pour cela, des campagnes d'information et de sensibilisation pourraient être lancées par les associations familiales et les administrations intéressées. Cette campagne comprendrait notamment l'adoption d'un Mémento des droits et obligations sur Internet, rappelant la réglementation applicable ; l'éducation nationale, quant à elle, pourrait inclure dans les programmes scolaires des enseignements sur ces réseaux, l'Edunet, non pas tant dans leur appréhension technique mais plutôt dans les questions intellectuelles, éthiques ou civiques qu'ils peuvent susciter. Enfin, les municipalités devraient ouvrir des espaces gratuits de libre accès au Net, des « Resothèques », pour familiariser les utilisateurs et leur donner accès à des informations institutionnelles ou de service public ; ainsi se limiterait le risque que dénoncent certains d'exclusion de certaines catégories défavorisées du monde de l'Internet du fait du coût élevé de l'équipement ; pourquoi enfin, ne pas imaginer un numéro vert sur Internet ?

Outre cette pédagogie tournée vers le « grand public », il faut mobiliser les administrations, celles-ci vont être amenées à statuer sur de nombreuses questions : propriété intellectuelle et droit des marques, fiscalité, politique pénale, etc. ; dans bien des cas, ses représentants ne peuvent trouver de réponses aux problèmes que posent les réseaux dans la méconnaissance qu'ils ont de leur fonctionnement technique et précis et donc de ce qu'il est possible de faire ; en outre, ils ne savent pas toujours comment exploiter à leur profit, les immenses potentialités qu'offre Internet. Il faut donc les informer et les mobiliser sur les adaptations à mettre en oeuvre dans leurs départements ministériels et les secteurs dont ils ont la charge. Un **outil interministériel de coordination et d'impulsion** semble nécessaire ; une telle délégation devra évidemment coordonner son action avec le comité des services en ligne, l'un animant la politique gouvernementale, l'autre « plus déontologique » se faisant le médiateur de la profession. Outre ce nouvel outil, un séminaire de formation des fonctionnaires ainsi que des séances systématiques de formation permanente doivent dès aujourd'hui être mis en place.

Il est nécessaire enfin, d'informer et de motiver les professionnels par la mobilisation des ordres professionnels, des chambres de commerce,... afin que chacun des secteurs d'activité prennent conscience des enjeux liés au développement des réseaux ouverts au public : deux exemples parmi d'autres ? Quel avenir pour les professions réglementées ? Quelles conséquences sur le secteur de la distribution, le réseau pouvant assurer la fonction d'intermédiation, voire être lui-même la marchandise (téléchargement de logiciels) ? Comment assurer une meilleure promotion des produits français sur le réseau ?

Favoriser la présence française et francophone sur le réseau

Internet aujourd'hui appartient au monde anglo-saxon. Outre sa traduction en termes économiques, un tel constat implique des choix de normalisation et de régulation ne correspondant pas nécessairement à l'approche française ou européenne et à ses valeurs. Nous l'avons vu, par exemple, pour les logiciels de contrôle. Il est donc vital d'être présent sur le réseau, dans les instances non gouvernementales qui existent déjà et dans les discussions qui s'engagent. La meilleure manière de se défendre contre Internet, si danger il y a, est d'y être ! Pour cela, la France a un potentiel exceptionnel d'expérience et de compétence du fait du Minitel ; toute cette industrie doit au plus vite valoriser ses atouts sur le Net et développer de nouveaux services. Pour les utilisateurs français, un serveur français de qualité sera toujours plus attractif qu'un serveur étranger ; il faut donc que notre industrie se mobilise sur les contenus et aussi sur les logiciels de réseaux. Il faut en outre renforcer notre représentation dans les lieux où se dessine l'avenir du réseau : il n'y a que cent français sur les cinq mille membres de l'Internet International Foundation, très peu dans des instances techniques (Internet Architecture Board et Internet Engineering Task Force) ou à l'Internet Society. Comment espérer dans ces conditions faire prévaloir un modèle « humaniste » à la française ?

Enfin, il faut poursuivre la mise en place « d'espaces francophones » car ceux-ci sont le moyen de favoriser le respect des droits et libertés de la personne auxquelles nous sommes attachés ; renforcer également le rôle du français comme langue véhiculaire, de communication entre les internautes afin de dépasser le taux de 2 % des échanges en français actuellement enregistrés.

Annexes

Annexe 1

Personnalités françaises auditionnées

A. Beaussant, GESTE

Me Bensoussan, Cabinet Bensoussan

F. Benveniste, Calvacom

J.-M. Billaut, Atelier Compagnie Bancaire

D. de Boisseson, Alcatel

P. Bouriez, P. Auboin, Lyonnaise Communication

Me N. Brault, Cabinet Weil, Armfeld et associés

J.-J. de Bresson, H. Soymie, M. Favard, Conseil supérieur de la télématique

MM. Burnel - Mayeux, Union nationale des associations familiales

J.-P. Courtois - F. Bogacz, Microsoft France

J.-J. Damlamian, P. Reynaud, E. Guillaume, France Télécom

Me Dupuis-Toubol et Tonnelier, Cabinet Jeantet

G. Eymery, France télécom multimédia ; **R. Courtois**, France Télécom interactive

A. Grange-Cabanne, Union des annonceurs

J. Hayward, Cie générale de vidéocommunication

C. Huard, ADEIC-FEN - bureau du Conseil national de la consommation

Pierre Huet, conseiller d'État

O. Iteanu, avocat

Me Kahn, Cabinet Kahn & associés

Pierre Lafitte, sénateur

M. Lartail, GIP Renater

Bruno Lasserre, direction générale des Postes et Télécommunications

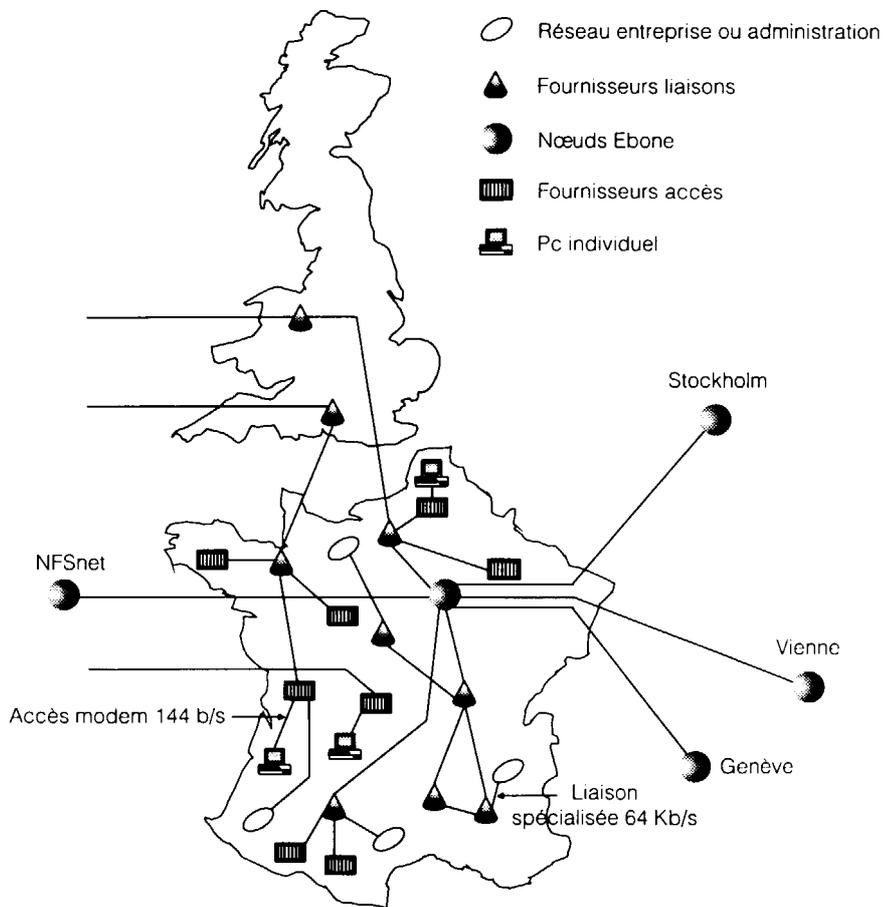
J.-B. Levy, Matra Communication

R. de Lochounoff, Sligos
Me J. Martin, avocat
Henri de Maublanc, Aftel
F. Mauduy, Philips
B. Oudet, chapitre français de l'Internet Society
J.-C. Pelissolo, Galeries Lafayette - Association française pour le commerce et les échanges électroniques
Marcel Pinet, Conseiller d'État - CNIL
M. Planche, Oléane
Bernard Porte, Fédération nationale de la presse française
M^{me} Renard - M. Babonneau, Institut national de recherche en informatique et en automatique
P.O. Rousseau, CSA
Keith Spicer, Conseil de la radiodiffusion et des télécommunications canadiennes
G. Thery, Cité des sciences et de l'industrie
J. Thibon, Thomson Multimédia
B. Touraine, Vidéopole
J.-L. Tournier, SACEM
B. Usunier, Compuserve

Annexe 2

Situation de l'Internet en France et dans le monde

Graphique 1
Les acteurs de l'Internet

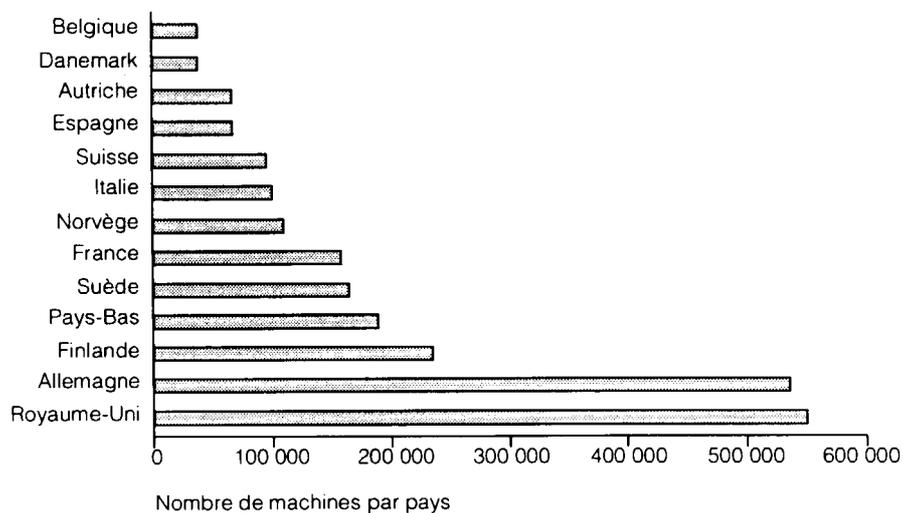


L'Internet n'est pas un réseau organisé, mais l'interconnexion, selon des modalités très diverses, d'une multitude de réseaux.

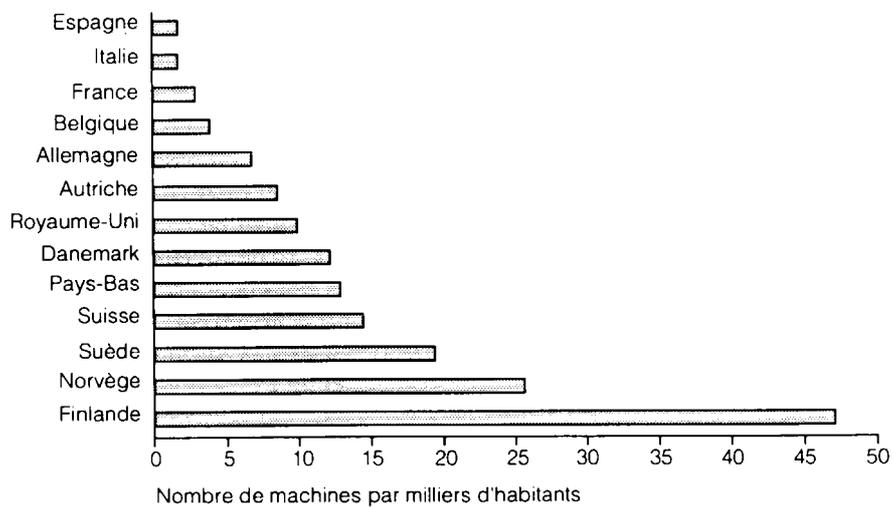
(note : les vitesses indiquées sur le schéma le sont uniquement à titre d'exemple)

Source : rapport de l'AFTEL (octobre 1995)

Graphique 2
Nombre de machines connectées à l'Internet par pays en Europe
 d'après le « RIPE NCC Hostcount » du 31 mars 1996

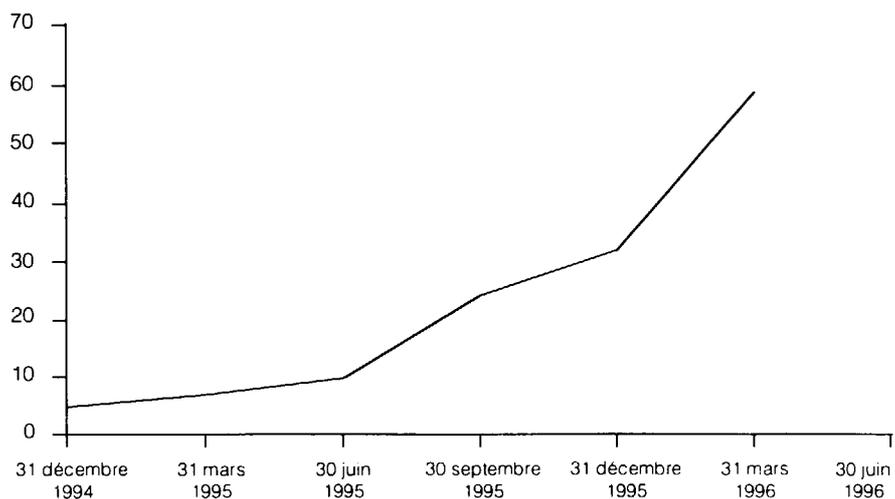


Graphique 3
Nombre de machines connectées à l'Internet par milliers d'habitants
 Estimations d'après les populations de 1982-1988
 et le « RIPE NCC Hostcount » du 31 mars 1996

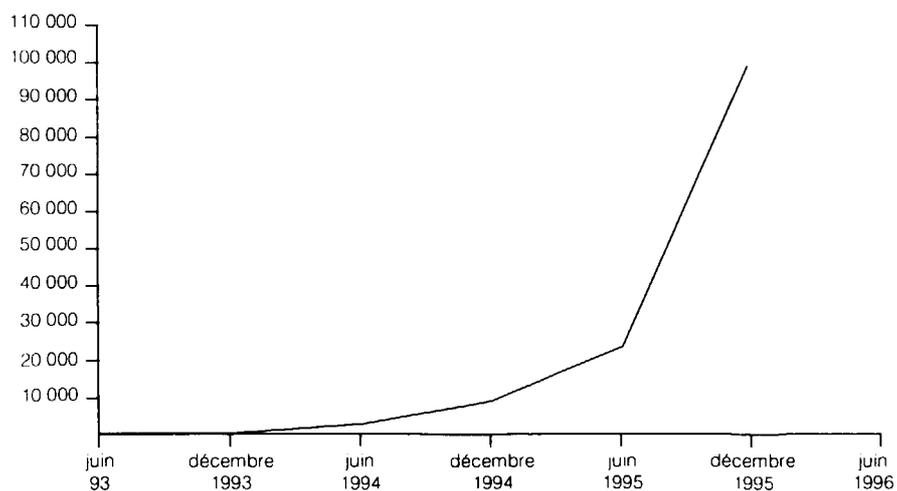


Source : NIC France - Avril 1996

Graphique 4
Évolution du nombre de prestataires Internet ayant adhéré au NIC France

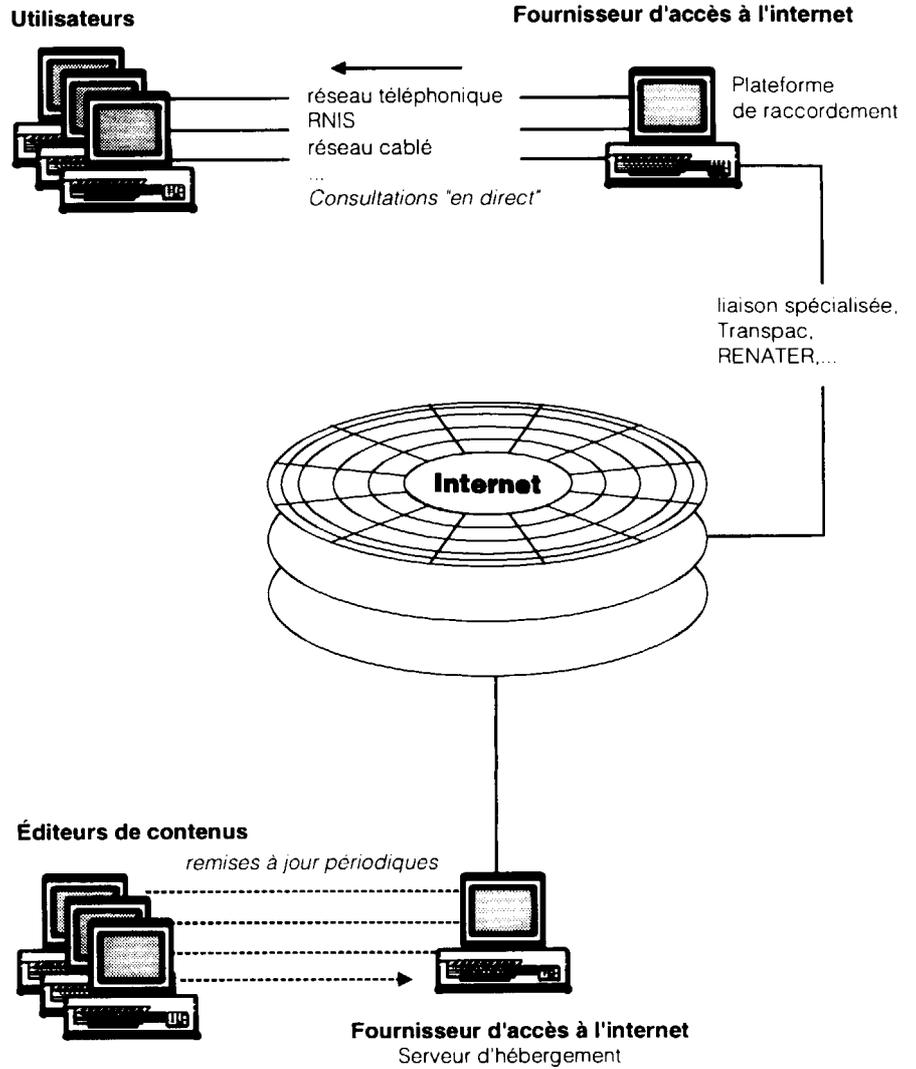


Graphique 5
Évolution du nombre de serveurs WWW dans le monde



Source : NIC France - Avril 1996

Graphique 5
**Schéma simplifié d'introduction, de consultation
 et de cheminement des contenus sur le Web**



Annexe 3

Mission aux USA 6 au 9 mai 1996

Liste des personnes rencontrées

En ce qui concerne les institutionnels, ont été auditionnés :

- **Michael Nelson**, conseiller à la Maison Blanche
- La Federal Communication Commission
- La National Telecommunications and Information Administration

En ce qui concerne les industriels, ont été auditionnés :

- Table ronde autour du Center for Strategie and International Study regroupant Computer and Communications Industry Assoc., Hogan & Hartson, US WEST, General Electric, Compuserve, AT & T, Jenner & Block, Eclips, Cybercash
- America On Line (AOL)
- MCI

En ce qui concerne les groupes de réflexions, consultants ou avocats :

- Washington Research Group
- Center for Democracy and Technology : association s'étant séparée récemment de l'Electronic Frontier Foundation
- **Donald Heath**, président de l'Internet Society
- Family Research Group
- American Civil Liberties Union
- **Gary Epstein**, avocat, cabinet Latham & Watkins
- **Jeffrey Cunnard**, avocat

Decency Act of 1996

[Communications Decency Act of 1996 ("CDA"), Title V, Telecommunications Act of 1996, Act of Feb. 8, 1996, Pub. L. No. 104-104 (S.652), 1996 U.S.C.C.A.N. (110 Stat.) 133-43]

No. 1

March 1996

United States Code Congressional and Administrative News 104th Congress - Second Session

Members and Committees

Public Laws

104-90 to 104-92, 104-94,

104-99 to 104-106

Legislative History

Proclamations

Executive Orders

Presidents Messages

Federal Regulations

Court Rules

Tables

Index

West Publishing Co.

610 Opperman Drive, P.O. Box 64526

St. Paul, MN 55164-0526

PUBLIC LAW 104-104 [S. 652]; February 8, 1996

TELECOMMUNICATIONS ACT OF 1996

For Legislative History of Act, see Report for P.L. 104-104 in U.S.C.C. & A.N. Legislative History Section.

An Act to promote competition and reduce regulation in order to secure lower prices and higher quality services for American telecommunications consumers and encourage the rapid deployment of new telecommunications technologies.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE; REFERENCES.

(a) SHORT TITLE - This Act may be cited as the "Telecommunications Act of 1996".

(b) REFERENCES - Except as otherwise expressly provided, whenever in this Act an amendment or repeal is expressed in terms of an amendment to, or repeal of, a section or other provision, the reference shall be considered to be made to a section or other provision of the Communications Act of 1934 (47 U.S.C. 151 et seq.).

SEC. 2. TABLE OF CONTENTS.

The table of contents for this Act is as follows:

Sec. 1. Short title references.

Sec. 2 Table of contents.

Sec. 3 Definitions.

TITLE I - TELECOMMUNICATION SERVICES

Subtitle A - Telecommunications Services

Sec. 101. Establishment of part II of title II.

"PART II - DEVELOPMENT OF COMPETITIVE MARKETS

"Sec. 251. Interconnection.

"Sec. 252. Procedures for negotiation, arbitration, and approval of agreements.

"Sec. 253. Removal of barriers to entry.

"Sec. 254. Universal service.

"Sec. 255. Access by persons with disabilities.

"Sec. 256. Coordination for interconnectivity.

"Sec. 257. Market entry barriers proceeding.

"Sec. 258. Illegal changes in subscriber carrier selections.

"Sec. 259. Infrastructure sharing.

"Sec. 260. Provision of telemessaging service.

"Sec. 261. Effect on other requirements".

Sec. 102. Eligible telecommunications carriers.

Sec. 103. Exempt telecommunications companies.

Sec. 104. Nondiscrimination principle.

Subtitle B - Special Provisions Concerning Bell Operating Companies

Sec. 151. Bell operating company provisions.

"PART III - SPECIAL PROVISIONS CONCERNING BELL OPERATING COMPANIES

"Sec. 271. Bell operating company entry into interLATA services.

"Sec. 272. Separate affiliate; safeguards.

"Sec. 273. Manufacturing by Bell operating companies.

"Sec. 274. Electronic publishing by Bell operating companies.
"Sec. 275. Alarm monitoring services.
"Sec. 276. Provision of payphone service."

TITLE II - BROADCAST SERVICES

Sec. 201. Broadcast spectrum flexibility.
"Sec. 336. Broadcast spectrum flexibility."
Sec. 202. Broadcast ownership.
Sec. 203. Term of licenses.
Sec. 204. Broadcast license renewal procedures.
Sec. 205. Direct broadcast satellite service.
Sec. 206. Automated ship distress and safety systems.
"Sec. 365. Automated ship distress and safety systems."
Sec. 207. Restrictions on over-the-air reception devices.

TITLE III - CABLE SERVICES

Sec. 301. Cable Act reform.
Sec. 302. Cable service provided by telephone companies.

"PART V - VIDEO PROGRAMMING SERVICES PROVIDED BY TELEPHONE COMPANIES

"Sec. 651. Regulatory treatment of video programming services.
"Sec. 652. Prohibition on buy outs.
"Sec. 653. Establishment of open video systems."
Sec. 303. Preemption of franchising authority regulation of telecommunications services.
Sec. 304. Competitive availability of navigation devices.
"Sec. 629. Competitive availability of navigation devices."
Sec. 305. Video programming accessibility.
"Sec. 713. Video programming accessibility."

TITLE IV - REGULATORY REFORM

Sec. 401. Regulatory forbearance.
"Sec. 10. Competition in provision of telecommunications service."
Sec. 402. Biennial review of regulations; regulatory relief.
"Sec. 11. Regulatory reform."
Sec. 403. Elimination of unnecessary Commission regulations and functions.

TITLE V - OBSCENITY AND VIOLENCE

Subtitle A - Obscene, Harassing, and Wrongful Utilization of Telecommunications Facilities

Sec. 501. Short title.
Sec. 502. Obscene or harassing use of telecommunications facilities under the Communications Act of 1934.
Sec. 503. Obscene programming on cable television.
Sec. 504. Scrambling of cable channels for nonsubscribers.

"Sec. 640. Scrambling of cable channels for nonsubscribers."
Sec. 505. Scrambling of sexually explicit adult video service programming.
"Sec. 641. Scrambling of sexually explicit adult video service programming."
Sec. 506. Cable operator refusal to carry certain programs.
Sec. 507. Clarification of current laws regarding communication of obscene materials through the use of computers.
Sec. 508. Coercion and enticement of minors.
Sec. 509. Online family empowerment.
"Sec. 230. Protection for private blocking and screening of offensive material."

Subtitle B - Violence

Sec. 551. Parental choice in television programming.
Sec. 552. Technology fund.

Subtitle C - Judicial Review

Sec. 561. Expedited review.

TITLE VI - EFFECT ON OTHER LAWS

Sec. 601. Applicability of consent decrees and other law.
Sec. 602. Preemption of local taxation with respect to direct-to-home services.

TITLE VII - MISCELLANEOUS PROVISIONS

Sec. 701. Prevention of unfair billing practices for information or services provided over toll-free telephone calls.
Sec. 702. Privacy of customer information.
"Sec. 222. Privacy of of customer information."
Sec. 703. Pole attachments.
Sec. 704. Facilities siting; radio frequency emission standards.
Sec. 705. Mobile services direct access to long distance carriers.
Sec. 706. Advanced telecommunications incentives.
Sec. 707. Telecommunications Development Fund.
"Sec. 714. Telecommunications Development Fund."
Sec. 708. National Education Technology Funding Corporation.
Sec. 709. Report on the use of advanced telecommunications services for medical purposes.
Sec. 710. Authorization of appropriations.

SEC. 3. DEFINITIONS.

(a) ADDITIONALDEFINITIONS- Section 3 (47 U.S.C. 153) is amended

(1) in subsection (r) -
(A) by inserting "(A)" after "means"; and

(B) by inserting before the period at the end the following: ", or (B) comparable service provided through a system of switches, transmission equipment, or other facilities (or combination thereof) by which a subscriber can originate and terminate a telecommunications service"; and

(2) by adding at the end thereof the following:

"(33) AFFILIATE - The term 'affiliate' means a person that (directly or indirectly) owns or controls, is owned or controlled by, or is under common ownership or control with, another person. For purposes of this paragraph, the term 'own' means to own an equity interest (or the equivalent thereof) of more than 10 percent.

"(34) AT&T CONSENT DECREE - The term 'AT&T Consent Decree' means the order entered August 24, 1982, in the antitrust action styled United States v. Western Electric, Civil. Action No. 82-0192, in the United States District Court for the District of Columbia, and includes any judgment or order with respect to such action entered on or after August 24, 1982.

"(35) BELL OPERATING COMPANY - The term 'Bell operating company' -

"(A) means any of the following companies: Bell Telephone Company of Nevada, Illinois Bell Telephone Company, Indiana Bell Telephone Company, Incorporated, Michigan Bell Telephone Company, New England Telephone and Telegraph Company, New Jersey Bell Telephone Company, New York Telephone Company, US West Communications Company, South Central Bell Telephone Company, Southern Bell Telephone and Telegraph Company, Southwestern Bell Telephone Company, The Bell Telephone Company of Pennsylvania, The Chesapeake and Potomac Telephone Company, The Chesapeake and Potomac Telephone Company of Maryland, The Chesapeake and Potomac Telephone Company of Virginia, The Chesapeake and Potomac Telephone Company of West Virginia, The Diamond State Telephone Company, The Ohio Bell Telephone Company, The Pacific Telephone and Telegraph Company, or Wisconsin Telephone Company; and

"(B) includes any successor or assign of any such company that provides wireline telephone exchange service; but

"(C) does not include an affiliate of any such company, other than an affiliate described in subparagraph (A) or (B).

"(36) CABLE SERVICE - The term 'cable service' has the meaning given such term in section 602.

"(37) CABLE SYSTEM - The term 'cable system' has the meaning given such term in section 602.

"(38) CUSTOMER PREMISES EQUIPMENT - The term 'customer premises equipment' means equipment employed on the premises of a person (other than a carrier) to originate, route, or terminate telecommunications.

"(39) DIALING PARITY - The term 'dialing parity' means that a person that is not an affiliate of a local exchange carrier is able to provide telecommunications services in such a manner that customers have the ability to route automatically, without the use of any access code, their telecommunications to the telecommunications services provider of the customers designation from among 2 or more telecommunications services providers (including such local exchange carrier).

"(40) EXCHANGE ACCESS - The term 'exchange access' means the offering of access to telephone exchange services or facilities for the purpose of the origination or termination of telephone toll services.

"(41) INFORMATION SERVICE - The term 'information service' means the offering of a capability for generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information via telecommunications, and includes electronic publishing, but does not include any use of any such capability for the management, control, or operation of a telecommunications system or the management of a telecommunications service.

"(42) INTERLATA SERVICE - The term 'interLATA service' means telecommunications between a point located in a local access and transport area and a point located outside such area.

"(43) LOCAL ACCESS AND TRANSPORT AREA - The term 'local access and transport area' or 'LATA' means a contiguous geographic area -

"(A) established before the date of enactment of the Telecommunications Act of 1996 by a Bell operating company such that no exchange area includes points within more than 1 metropolitan statistical area, consolidated metropolitan statistical area, or State, except as expressly permitted under the AT&T Consent Decree; or

"(B) established or modified by a Bell operating company after such date of enactment and approved by the Commission.

"(44) LOCAL EXCHANGE CARRIER - The term 'local exchange carrier' means any person that is engaged in the provision of telephone exchange service or exchange access. Such term does not include a person insofar as such person is engaged in the provision of a commercial mobile service under section 332(c), except to the extent that the Commission finds that such service should be included in the definition of such term.

"(45) NETWORK ELEMENT - The term 'network element' means a facility or equipment used in the provision of a telecommunications service. Such term also includes features, functions, and capabilities that are provided by means of such facility or equipment, including subscriber numbers, databases, signaling systems, and information sufficient for billing and collection or used in the transmission, routing, or other provision of a telecommunications service.

"(46) NUMBER PORTABILITY- The term 'number portability' means the ability of users of telecommunications services to retain, at the same location, existing telecommunications numbers without impairment of quality, reliability, or convenience when switching from one telecommunications carrier to another.

"(47) RURAL TELEPHONE COMPANY- The term 'rural telephone company' means a local exchange carrier operating entity to the extent that such entity -

"(A) provides common carrier service to any local exchange carrier study area that does not include either -

"(i) any incorporated place of 10,000 inhabitants or more, or any part thereof, based on the most recently available population statistics of the Bureau of the Census; or

"(ii) any territory, incorporated or unincorporated, included in an urbanized area, as defined by the Bureau of the Census as of August 10, 1993;

"(B) provides telephone exchange service, including exchange access, to fewer than 50,000 access lines;

"(C) provides telephone exchange service to any local exchange carrier study area with fewer than 100,000 access lines; or

"(D) has less than 15 percent of its access lines in communities of more than 50,000 on the date of enactment of the Telecommunications Act of 1996.

"(48) TELECOMMUNICATIONS- The term 'telecommunications' means the transmission, between or among points specified by the user, of information of the users choosing, without change in the form or content of the information as sent and received.

"(49) TELECOMMUNICATIONS CARRIER- The term 'telecommunications carrier' means any provider of telecommunications services, except that such term does not include aggregators of telecommunications services (as defined in section 226). A telecommunications carrier shall be treated as a common carrier under this Act only to the extent that it is engaged in providing telecommunications services, except that the Commission shall determine whether the provision of fixed and mobile satellite service shall be treated as common carriage.

"(50) TELECOMMUNICATIONS EQUIPMENT- The term 'telecommunications equipment' means equipment, other than customer premises equipment, used by a carrier to provide telecommunications services, and includes software integral to such equipment (including upgrades).

"(51) TELECOMMUNICATIONS SERVICE- The term 'telecommunications service' means the offering of telecommunications for a fee directly to the public, or to such classes of users as to be effectively available directly to the public, regardless of the facilities used."

(b) COMMON TERMINOLOGY- Except as otherwise provided in this Act, the terms used in this Act have the meanings provided

in section 3 of the Communications Act of 1934 (47 U.S.C. 153), as amended by this section.

(C) STYLISTIC CONSISTENCY - Section 3 (47 U.S.C. 153) is amended -

(1) in subsections (e) and (n), by redesignating clauses (1), (2) and (3), as clauses (A), (B), and (C), respectively;

(2) in subsection (w), by redesignating paragraphs (1) through (5) as subparagraphs (A) through (E), respectively;

(3) in subsections (y) and (z), by redesignating paragraphs (1) and (2) as subparagraphs (A) and (B), respectively;

(4) by redesignating subsections (a) through (ff) as paragraphs (1) through (32);

(5) by indenting such paragraphs 2 em spaces;

(6) by inserting after the designation of each such paragraph -
(A) a heading, in a form consistent with the form of the heading of this subsection, consisting of the term defined by such paragraph, or the first term so defined if such paragraph defines more than one term; and

(B) the words "The term";

(7) by changing the first letter of each defined term in such paragraphs from a capital to a lower case letter (except for "United States", "State", "State commission", and "Great Lakes Agreement"); and

(8) by reordering such paragraphs and the additional paragraphs added by subsection (a) in alphabetical order based on the headings of such paragraphs and renumbering such paragraphs as so reordered.

(d) CONFORMING AMENDMENTS- The Act is amended -

(1) in section 225(a)(1), by striking "section 3(h)" and inserting "section 3";

(2) in section 332(d), by striking "section 3(n)" each place it appears and inserting "section 3"; and

(3) in sections 621(d)(3), 636(d), and 637(a)(2), by striking "section 3(v)" and inserting "section 3".

TITLE I - TELECOMMUNICATION SERVICES

Subtitle A - Telecommunications Services

SEC. 101. ESTABLISHMENT OF PART II OF TITLE II.

(a) AMENDMENT- Title II is amended by inserting after section 229 (47 U.S.C. 229) the following new part:

"Part II - Development of Competitive Markets

"SEC.251. INTERCONNECTION.

"(a) GENERAL DUTY OF TELECOMMUNICATIONS CARRIERS - Each telecommunications carrier has the duty -

"(1) to interconnect directly or indirectly with the facilities and equipment of other telecommunications carriers; and
[...]

TITLE V - OBSCENITY AND VIOLENCE

Subtitle A - Obscene, Harassing, and Wrongful Utilization of Telecommunications Facilities

SEC. 501. SHORT TITLE.

This title may be cited as the "Communications Decency Act of 1996".

SEC. 502. OBSCENE OR HARASSING USE OF TELECOMMUNICATIONS FACILITIES UNDER THE COMMUNICATIONS ACT OF 1934.

Section 223 (47 U.S.C. 223) is amended -

(1) by striking subsection (a) and inserting in lieu thereof:

"(a) Whoever -

"(1) in interstate or foreign communications -

"(A) by means of a telecommunications device knowingly -

"(i) makes, creates, or solicits, and

"(ii) initiates the transmission of,

any comment, request, suggestion, proposal, image, or other communication which is obscene, lewd, lascivious, filthy, or indecent, with intent to annoy, abuse, threaten, or harass another person;

"(B) by means of a telecommunications device knowingly -

"(i) makes, creates, or solicits, and

"(ii) initiates the transmission of,

any comment, request, suggestion, proposal, image, or other communication which is obscene or indecent, knowing that the recipient of the communication is under 18 years of age, regardless of whether the maker of such communication placed the call or initiated the communication;

"(C) makes a telephone call or utilizes a telecommunications device, whether or not conversation or communication ensues, without disclosing his identity and with intent to annoy, abuse, threaten, or harass any person at the called number or who receives the communications;

"(D) makes or causes the telephone of another repeatedly or continuously to ring, with intent to harass any person at the called number; or

"(E) makes repeated telephone calls or repeatedly initiates communication with a telecommunications device, during which conversation or communication ensues, solely to harass any person at the called number or who receives the communication ; or

"(2) knowingly permits any telecommunications facility under his control to be used for any activity prohibited by paragraph (1) with the intent that it be used for such activity, shall be fined under title 18, United States Code, or imprisoned not more than two years, or both."; and

(2) by adding at the end the following new subsections:

"(d) Whoever -

"(1) in interstate or foreign communications knowingly -

"(A) uses an interactive computer service to send to a specific person or persons under 18 years of age, or

"(B) uses any interactive computer service to display in a manner available to a person under 18 years of age, any comment, request, suggestion, proposal, image, or other communication that, in context, depicts or describes, in terms patently offensive as measured by contemporary community standards, sexual or excretory activities or organs, regardless of whether the user of such service placed the call or initiated the communication; or

"(2) knowingly permits any telecommunications facility, under such persons control to be used for an activity prohibited by paragraph (1) with the intent that it be used for such activity, shall be fined under title 18, United States Code, or imprisoned not more than two years, or both.

"(e) In addition to any other defenses available by law:

"(1) No person shall be held to have violated subsection (a) or (d) solely for providing access or connection to or from a facility, system, or network not under that persons control, including transmission, downloading, intermediate storage, access software, or other related capabilities that are incidental to providing such access or connection that does not include the creation of the content of the communication.

"(2) The defenses provided by paragraph (1) of this subsection shall not be applicable to a person who is a conspirator with an entity actively involved in the creation or knowing distribution of communications that violate this section, or who knowingly advertises the availability of such communications.

"(3) The defenses provided in paragraph (1) of this subsection shall not be applicable to a person who provides access or connection to a facility, system, or network engaged in the violation of this section that is owned or controlled by such person.

"(4) No employer shall be held liable under this section for the actions of an employee or agent unless the employees or agents conduct is within the scope of his or her employment or agency and the employer (A) having knowledge of such conduct, authorizes or ratifies such conduct, or (B) recklessly disregards such conduct.

"(5) It is a defense to a prosecution under subsection (a)(1)(B) or (d), or under subsection (a)(2) with respect to the use of a facility for an activity under subsection (a)(1)(B) that a person -
"(A) has taken, in good faith, reasonable, effective, and appropriate actions under the circumstances to restrict or prevent access by minors to a communication specified in such subsections, which may involve any appropriate measures to restrict minors from such communications, including any method which is feasible under available technology; or
"(B) has restricted access to such communication by requiring use of a verified credit card, debit account, adult access code, or adult personal identification number.

"(6) The Commission may describe measures which are reasonable, effective, and appropriate to restrict access to prohibited communications under subsection (d). Nothing in this section authorizes the Commission to enforce, or is intended to provide the Commission with the authority to approve, sanction, or permit, the use of such measures. The Commission shall have no enforcement authority over the failure to utilize such measures. The Commission shall not endorse specific products relating to such measures. The use of such measures shall be admitted as evidence of good faith efforts for purposes of paragraph (5) in any action arising under subsection (d). Nothing in this section shall be construed to treat interactive computer services as common carriers or telecommunications carriers.

"(f)(1) No cause of action may be brought in any court or administrative agency against any person on account of any activity that is not in violation of any law punishable by criminal or civil penalty, and that the person has taken in good faith to implement a defense authorized under this section or otherwise to restrict or prevent the transmission of, or access to, a communication specified in this section.

"(2) No State or local government may impose any liability for commercial activities or actions by commercial entities, nonprofit libraries, or institutions of higher education in connection with an activity or action described in subsection (a)(2) or (d) that is inconsistent with the treatment of those activities or actions under this section: *Provided, however,* That nothing herein shall preclude any State or local government from enacting and enforcing complementary oversight, liability, and regulatory systems, procedures, and requirements, so long as such systems, procedures, and requirements govern only intrastate services and do not result in the imposition of

inconsistent rights, duties or obligations on the provision of interstate services. Nothing in this subsection shall preclude any State or local government from governing conduct not covered by this section.

"(g) Nothing in subsection (a), (d), (e), or (f) or in the defenses to prosecution under subsection (a) or (d) shall be construed to affect or limit the application or enforcement of any other Federal law.

"(h) For purposes of this section -

"(1) The use of the term 'telecommunications device' in this section -

"(A) shall not impose new obligations on broadcasting station licensees and cable operators covered by obscenity and indecency provisions elsewhere in this Act; and

"(B) does not include an interactive computer service.

"(2) The term 'interactive computer service' has the meaning provided in section 230(e)(2).

"(3) The term 'access software' means software (including client or server software) or enabling tools that do not create or provide the content of the communication but that allow a user to do any one or more of the following:

"(A) filter, screen, allow, or disallow content;

"(B) pick, choose, analyze, or digest content; or

"(C) transmit, receive, display, forward, cache, search, subset, organize, reorganize, or translate content.

"(4) The term 'institution of higher education' has the meaning provided in section 1201 of the Higher Education Act of 1965 (20 U.S.C. 1141).

"(5) The term 'library' means a library eligible for participation in State-based plans for funds under title III of the Library Services and Construction Act (20 U.S.C. 355e et seq.)."

SEC. 503. OBSCENE PROGRAMMING ON CABLE TELEVISION.

Section 639 (47 U.S.C. 559) is amended by striking "not more than \$10,000" and inserting "under title 18, United States Code,".

SEC. 504. SCRAMBLING OF CABLE CHANNELS FOR NONSUBSCRIBERS.

Part IV of title VI (47 U.S.C. 551 et seq.) is amended by adding at the end the following:

"SEC. 640. SCRAMBLING OF CABLE CHANNELS FOR NONSUBSCRIBERS.

"(a) SUBSCRIBER REQUEST- Upon request by a cable service subscriber, a cable operator shall, without charge, fully scramble or otherwise fully block the audio and video programming

of each channel carrying such programming so that one not a subscriber does not receive it.

"(b) DEFINITION- As used in this section, the term 'scramble' means to rearrange the content of the signal of the programming so that the programming cannot be viewed or heard in an understandable manner."

SEC. 505. SCRAMBLING OF SEXUALLY EXPLICIT ADULT VIDEO SERVICE PROGRAMMING.

(a) REQUIREMENT- Part IV of title VI (47 U.S.C. 551 et seq.), as amended by this Act, is further amended by adding at the end the following:

"SEC. 641. SCRAMBLING OF SEXUALLY EXPLICIT ADULT VIDEO SERVICE PROGRAMMING.

"(a) REQUIREMENT- In providing sexually explicit adult programming or other programming that is indecent on any channel of its service primarily dedicated to sexually-oriented programming, a multichannel video programming distributor shall fully scramble or otherwise fully block the video and audio portion of such channel so that one not a subscriber to such channel or programming does not receive it.

"(b) IMPLEMENTATION- Until a multichannel video programming distributor complies with the requirement set forth in subsection (a), the distributor shall limit the access of children to the programming referred to in that subsection by not providing such programming during the hours of the day (as determined by the Commission) when a significant number of children are likely to view it.

"(C) DEFINITION- As used in this section, the term 'scramble' means to rearrange the content of the signal of the programming so that the programming cannot be viewed or heard in an understandable manner."

(b) EFFECTIVE DATE- The amendment made by subsection (a) shall take effect 30 days after the date of enactment of this Act.

SEC. 506. CABLE OPERATOR REFUSAL TO CARRY CERTAIN PROGRAMS.

(a) PUBLIC EDUCATIONAL AND GOVERNMENTAL CHANNELS - Section 611(e) (47 U.S.C. 531(e)) is amended by inserting before the period the following: ", except a cable operator may refuse to transmit any public access program or portion of a public access program which contains obscenity, indecency, or nudity".

(b) CABLE CHANNELS FOR COMMERCIAL USE - Section 612(c)(2) (47 U.S.C. 532(c)(2)) is amended by striking "an operator" and inserting "a cable operator may refuse to transmit any

leased access program or portion of a leased access program which contains obscenity, indecency, or nudity and".

SEC. 507. CLARIFICATION OF CURRENT LAWS REGARDING COMMUNICATION OF OBSCENE MATERIALS THROUGH THE USE OF COMPUTERS.

(a) IMPORTATION OR TRANSPORTATION - Section 1462 of title 18, United States Code, is amended -

(1) in the first undesignated paragraph, by inserting "or interactive computer service (as defined in section 230(e)(2) of the Communications Act of 1934)" after "carrier"; and

(2) in the second undesignated paragraph -

(A) by inserting "or receives," after "takes";

(B) by inserting "or interactive computer service (as defined in section 230(e)(2) of the Communications Act of 1934)" after "common carrier", and

(C) by inserting "or importation" after "carriage".

(b) TRANSPORTATION FOR PURPOSES OF SALE OR DISTRIBUTION - The first undesignated paragraph of section 1465 of title 18, United States Code, is amended -

(1) by striking "transports in" and inserting "transports or travels in, or uses a facility or means of,";

(2) by inserting "or an interactive computer service (as defined in section 230(e)(2) of the Communications Act of 1934) in or affecting such commerce" after "foreign commerce" the first place it appears;

(3) by striking ", or knowingly travels in" and all that follows through "obscene material in interstate or foreign commerce," and inserting "of."

(C) INTERPRETATION - The amendments made by this section are clarifying and shall not be interpreted to limit or repeal any prohibition contained in sections 1462 and 1465 of title 18, United States Code, before such amendment, under the rule established in *United States v. Alpers*, 338 U.S. 680 (1950).

SEC. 508. COERCION AND ENTICEMENT OF MINORS.

Section 2422 of title 18, United States Code, is amended -

(1) by inserting "(a)" before "Whoever knowingly"; and

(2) by adding at the end the following:

"(b) Whoever, using any facility or means of interstate or foreign commerce, including the mail, or within the special maritime and territorial jurisdiction of the United States, knowingly persuades, induces, entices, or coerces any individual who has not attained the age of 18 years to engage in prostitution or any sexual act for which any person may be criminally prosecuted, or attempts to do so, shall be fined under this title or imprisoned not more than 10 years, or both."

SEC. 509. ONLINE FAMILY EMPOWERMENT.

Title II of the Communications Act of 1934 (47 U.S.C. 201 et seq.) is amended by adding at the end the following new section:

"SEC. 230. PROTECTION FOR PRIVATE BLOCKING AND SCREENING OF OFFENSIVE MATERIAL.

"(a) FINDINGS - The Congress finds the following:

"(1) The rapidly developing array of Internet and other interactive computer services available to individual Americans represent an extraordinary advance in the availability of educational and informational resources to our citizens.

"(2) These services offer users a great degree of control over the information that they receive, as well as the potential for even greater control in the future as technology develops.

"(3) The Internet and other interactive computer services offer a forum for a true diversity of political discourse, unique opportunities for cultural development, and myriad avenues for intellectual activity.

"(4) The Internet and other interactive computer services have flourished, to the benefit of all Americans, with a minimum of government regulation.

"(5) Increasingly Americans are relying on interactive media for a variety of political, educational, cultural, and entertainment services.

"(b) Policy. - It is the policy of the United States -

"(1) to promote the continued development of the Internet and other interactive computer services and other interactive media;

"(2) to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by Federal or State regulation;

"(3) to encourage the development of technologies which maximize user control over what information is received by individuals, families, and schools who use the Internet and other interactive computer services;

"(4) to remove disincentives for the development and utilization of blocking and filtering technologies that empower parents to restrict their childrens access to objectionable or inappropriate online material; and

"(5) to ensure vigorous enforcement of Federal criminal laws to deter and punish trafficking in obscenity, stalking, and harassment by means of computer.

"(c) PROTECTION FOR 'GOOD SAMARITAN' BLOCKING AND SCREENING OF OFFENSIVE MATERIAL -

"(1) TREATMENT OF PUBLISHER OR SPEAKER - NO provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.

"(2) CIVIL LIABILITY - No provider or user of an interactive computer service shall be held liable on account of -

"(A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or

"(B) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1).

"(d) EFFECT ON OTHER LAWS -

(1) NO EFFECT ON CRIMINAL LAW - Nothing in this section shall be construed to impair the enforcement of section 223 of this Act, chapter 71 (relating to obscenity) or 110 (relating to sexual exploitation of children) of title 18, United States Code, or any other Federal criminal statute.

"(2) NO EFFECT ON INTELLECTUAL PROPERTY LAW - Nothing in this section shall be construed to limit or expand any law pertaining to intellectual property.

"(3) STATE LAW - Nothing in this section shall be construed to prevent any State from enforcing any State law that is consistent with this section. No cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with this section.

"(4) NO EFFECT ON COMMUNICATIONS PRIVACY LAW - Nothing in this section shall be construed to limit the application of the Electronic Communications Privacy Act of 1986 or any of the amendments made by such Act, or any similar State law.

"(e) DEFINITIONS - As used in this section:

"(1) INTERNET - The term 'Internet' means the international computer network of both Federal and non-Federal interoperable packet switched data networks.

"(2) INTERACTIVE COMPUTER SERVICE - The term 'interactive computer service' means any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions.

"(3) INFORMATION CONTENT PROVIDER - The term 'information content provider' means any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service.

"(4) ACCESS SOFTWARE PROVIDER - The term 'access software provider' means a provider of software (including client or server software), or enabling tools that do any one or more of the following:

"(A) filter, screen, allow, or disallow content;

"(B) pick, choose, analyze, or digest content; or

"(C) transmit, receive, display, forward, cache, search, subset, organize, reorganize, or translate content."

Subtitle B - Violence

SEC. 551. PARENTAL CHOICE IN TELEVISION PROGRAMMING.

- (a) FINDINGS - The Congress makes the following findings:
- (1) Television influences childrens perception of the values and behavior that are common and acceptable in society.
 - (2) Television station operators, cable television system operators, and video programmers should follow practices in connection with video programming that take into consideration that television broadcast and cable programming has established a uniquely pervasive presence in the lives of American children.
 - (3) The average American child is exposed to 25 hours of television each week and some children are exposed to as much as 11 hours of television a day.
 - (4) Studies have shown that children exposed to violent video programming at a young age have a higher tendency for violent and aggressive behavior later in life than children not so exposed, and that children exposed to violent video programming are prone to assume that acts of violence are acceptable behavior.
 - (5) Children in the United States are, on average, exposed to an estimated 8,000 murders and 100,000 acts of violence on television by the time the child completes elementary school.
 - (6) Studies indicate that children are affected by the pervasiveness and casual treatment of sexual material on television, eroding the ability of parents to develop responsible attitudes and behavior in their children.
 - (7) Parents express grave concern over violent and sexual video programming and strongly support technology that would give them greater control to block video programming in the home that they consider harmful to their children.
 - (8) There is a compelling governmental interest in empowering parents to limit the negative influences of video programming that is harmful to children.
 - (9) Providing parents with timely information about the nature of upcoming video programming and with the technological tools that allow them easily to block violent, sexual, or other programming that they believe harmful to their children is a nonintrusive and narrowly tailored means of achieving that compelling governmental interest.
- (b) ESTABLISHMENT OF TELEVISION RATING CODE -
- (1) AMENDMENT - Section 303 (47 U.S.C. 303) is amended by adding at the end the following:
"(w) Prescribe -

"(1) on the basis of recommendations from an advisory committee established by the Commission in accordance with section 551(b)(2) of the Telecommunications Act of 1996, guidelines and recommended procedures for the identification and rating of video programming that contains sexual, violent, or other indecent material about which parents should be informed before it is displayed to children: *Provided*, That nothing in this paragraph shall be construed to authorize any rating of video programming on the basis of its political or religious content; and

"(2) with respect to any video programming that has been rated, and in consultation with the television industry, rules requiring distributors of such video programming to transmit such rating to permit parents to block the display of video programming that they have determined is inappropriate for their children."

(2) ADVISORY COMMITTEE REQUIREMENTS - In establishing an advisory committee for purposes of the amendment made by paragraph (1) of this subsection, the Commission shall -

(A) ensure that such committee is composed of parents, television broadcasters, television programming producers, cable operators, appropriate public interest groups, and other interested individuals from the private sector and is fairly balanced in terms of political affiliation, the points of view represented, and the functions to be performed by the committee;

(B) provide to the committee such staff and resources as may be necessary to permit it to perform its functions efficiently and promptly; and

(C) require the committee to submit a final report of its recommendations within one year after the date of the appointment of the initial members.

(c) REQUIREMENT FOR MANUFACTURE OF TELEVISIONS THAT BLOCK PROGRAMS - Section 303 (47 U.S.C. 303), as amended by subsection (a), is further amended by adding at the end the following:

"(x) Require, in the case of an apparatus designed to receive television signals that are shipped in interstate commerce or manufactured in the United States and that have a picture screen 13 inches or greater in size (measured diagonally), that such apparatus be equipped with a feature designed to enable viewers to block display of all programs with a common rating, except as otherwise permitted by regulations pursuant to section 330(c)(4)."

(d) SHIPPING OF TELEVISIONS THAT BLOCK PROGRAMS -

(1) REGULATIONS - Section 330 (47 U.S.C. 330) is amended -

(A) by redesignating subsection (c) as subsection (d); and

(B) by adding after subsection (b) the following new subsection (c):

"(c)(1) Except as provided in paragraph (2), no person shall ship in interstate commerce or manufacture in the United States any apparatus described in section 303(x) of this Act except in accordance with rules prescribed by the Commission pursuant to the authority granted by that section.

"(2) This subsection shall not apply to carriers transporting apparatus referred to in paragraph (1) without trading in it.

"(3) The rules prescribed by the Commission under this subsection shall provide for the oversight by the Commission of the adoption of standards by industry for blocking technology. Such rules shall require that all such apparatus be able to receive the rating signals which have been transmitted by way of line 21 of the vertical blanking interval and which conform to the signal and blocking specifications established by industry under the supervision of the Commission.

"(4) As new video technology is developed, the Commission shall take such action as the Commission determines appropriate to ensure that blocking service continues to be available to consumers. If the Commission determines that an alternative blocking technology exists that -

"(A) enables parents to block programming based on identifying programs without ratings,

"(B) is available to consumers at a cost which is comparable to the cost of technology that allows parents to block programming based on common ratings, and

"(C) will allow parents to block a broad range of programs on a multichannel system as effectively and as easily as technology that allows parents to block programming based on common ratings,

the Commission shall amend the rules prescribed pursuant to section 303(x) to require that the apparatus described in such section be equipped with either the blocking technology described in such section or the alternative blocking technology described in this paragraph."

(2) CONFORMING AMENDMENT- Section 330(d), as redesignated by subsection (d)(1)(A), is amended by striking "section 303(s), and section 303(u)" and inserting in lieu thereof "and sections 303(s), 303(u), and 303(x)".

(e) APPLICABILITY AND EFFECTIVE DATES -

(1) APPLICABILITY OF RATING PROVISION- The amendment made by subsection (b) of this section shall take effect 1 year after the date of enactment of this Act, but only if the Commission determines, in consultation with appropriate public interest groups and interested individuals from the private sector, that distributors of video programming have not, by such date -

(A) established voluntary rules for rating video programming that contains sexual, violent, or other indecent material about which parents should be informed before it is displayed to children, and such rules are acceptable to the Commission; and

(B) agreed voluntarily to broadcast signals that contain ratings of such programming.

(2) EFFECTIVE DATE OF MANUFACTURING PROVISION - In prescribing regulations to implement the amendment made by subsection (c), the Federal Communications Commission shall, after consultation with the television manufacturing industry, specify the effective date for the applicability of the requirement to the apparatus covered by such amendment, which date shall not be less than two years after the date of enactment of this Act.

SEC. 552. TECHNOLOGY FUND.

It is the policy of the United States to encourage broadcast television, cable, satellite, syndication, other video programming distributors, and relevant related industries (in consultation with appropriate public interest groups and interested individuals from the private sector) to -

- (1) establish a technology fund to encourage television and electronics equipment manufacturers to facilitate the development of technology which would empower parents to block programming they deem inappropriate for their children and to encourage the availability thereof to low income parents;
- (2) report to the viewing public on the status of the development of affordable, easy to use blocking technology; and
- (3) establish and promote effective procedures, standards, systems, advisories, or other mechanisms for ensuring that users have easy and complete access to the information necessary to effectively utilize blocking technology and to encourage the availability thereof to low income parents.

Subtitle C - Judicial Review

SEC. 561. EXPEDITED REVIEW.

(a) THREE-JUDGE DISTRICT COURT HEARING - Notwithstanding any other provision of law, any civil action challenging the constitutionality, on its face, of this title or any amendment made by this title, or any provision thereof, shall be heard by a district court of 3 judges convened pursuant to the provisions of section 2284 of title 28, United States Code.

(b) APPELLATE REVIEW - Notwithstanding any other provision of law, an interlocutory or final judgment, decree, or order of the court of 3 judges in an action under subsection (a) holding this title or an amendment made by this title, or any provision thereof, unconstitutional shall be reviewable as a matter of right by direct appeal to the Supreme Court. Any such appeal shall be filed not more than 20 days after entry of such judgment, decree, or order.

TITLE VI - EFFECT ON OTHER LAWS

SEC. 601. APPLICABILITY OF CONSENT DECREES AND OTHER LAW.

(a) APPLICABILITY OF AMENDMENTS TO FUTURE CONDUCT -

(1) AT&T CONSENT DECREE - Any conduct or activity that was, before the date of enactment of this Act, subject to any restriction or obligation imposed by the AT&T Consent Decree shall, on and after such date, be subject to the restrictions and obligations imposed by the Communications Act of 1934 as amended by this Act and shall not be subject to the restrictions and the obligations imposed by such Consent Decree.

(2) GTE CONSENT DECREE - Any conduct or activity that was, before the date of enactment of this Act, subject to any restriction or obligation imposed by the GTE Consent Decree shall, on and after such date, be subject to the restrictions and obligations imposed by the Communications Act of 1934 as amended by this Act and shall not be subject to the restrictions and the obligations imposed by such Consent Decree.

(3) MCCA W CONSENT DECREE - Any conduct or activity that was, before the date of enactment of this Act, subject to any restriction or obligation imposed by the McCaw Consent Decree shall, on and after such date, be subject to the restrictions and obligations imposed by the Communications Act of 1934 as amended by this Act and subsection (d) of this section and shall not be subject to the restrictions and the obligations imposed by such Consent Decree.

(b) ANTITRUST LAWS -

(1) SAVINGS CLAUSE - Except as provided in paragraphs (2) and (3), nothing in this Act or the amendments made by this Act shall be construed to modify, impair, or supersede the applicability of any of the antitrust laws.

(2) REPEAL - Subsection (a) of section 221 (47 U.S.C. 221(a)) is repealed.

(3) CLAYTON ACT - Section 7 of the Clayton Act (15 U.S.C. 18) is amended in the last paragraph by striking "Federal Communications Commission,".

(c) FEDERAL, STATE, AND LOCAL LAW -

(1) NO IMPLIED EFFECT - This Act and the amendments made by this Act shall not be construed to modify, impair, or supersede Federal, State, or local law unless expressly so provided in such Act or amendments.

(2) STATE TAX SAVINGS PROVISION - Notwithstanding paragraph (1), nothing in this Act or the amendments made by this Act shall be construed to modify, impair, or supersede, or authorize the modification, impairment, or supersession of, any State or local law pertaining to taxation, except as provided in sections 622 and 653(c) of the Communications Act of 1934 and section 602 of this Act.

(d) COMMERCIAL MOBILE SERVICE JOINT MARKETING- Notwithstanding section 22.903 of the Commissions regulations (47 C.F.R. 22.903) or any other Commission regulation, a Bell operating company or any other company may, except as provided in sections 271(e)(1) and 272 of the Communications Act of 1934 as amended by this Act as they relate to wireline service, jointly market and sell commercial mobile services in conjunction with telephone exchange service, exchange access, intra-LATA telecommunications service, interLATA telecommunications service, and information services.

(e) DEFINITIONS- As used in this section:

(1) AT&T CONSENT DECREE - The term "AT&T Consent Decree" means the order entered August 24, 1982, in the antitrust action styled United States v. Western Electric, Civil Action No. 82-0192, in the United States District Court for the District of Columbia, and includes any judgment or order with respect to such action entered on or after August 24, 1982.

(2) GTE CONSENT DECREE - The term "GTE Consent Decree" means the order entered December 21, 1984, as restated January 11, 1985, in the action styled United States v. GTE Corp., Civil Action No. 83-1298, in the United States District Court for the District of Columbia, and any judgment or order with respect to such action entered on or after December 21, 1984.

(3) MCCAW CONSENT DECREE - The term "McCaw Consent Decree" means the proposed consent decree filed on July 15, 1994, in the antitrust action styled United States v. AT&T Corp. and McCaw Cellular Communications, Inc., Civil Action No. 94-01555, in the United States District Court for the District of Columbia. Such term includes any stipulation that the parties will abide by the terms of such proposed consent decree until it is entered and any order entering such proposed consent decree.

(4) ANTITRUST LAWS - The term "antitrust laws" has the meaning given it in subsection (a) of the first section of the Clayton Act (15 U.S.C. 12(a)), except that such term includes the Act of June 19, 1936 (49 Stat. 1526; 15 U.S.C. 13 et seq.), commonly known as the Robinson-Patman Act, and section 5 of the Federal Trade Commission Act (15 U.S.C. 45) to the extent that such section 5 applies to unfair methods of competition.

SEC. 602. PREEMPTION OF LOCAL TAXATION WITH RESPECT TO DIRECT-TO-HOME SERVICES.

(a) PREEMPTION- A provider of direct-to-home satellite service shall be exempt from the collection or remittance, or both, of any tax or fee imposed by any local taxing jurisdiction on direct-to-home satellite service.

(b) DEFINITIONS- For the purposes of this section -

(1) DIRECT-TO-HOME SATELLITE SERVICE - The term "direct-to-home satellite service" means only programming transmitted or broadcast by satellite directly to the subscribers premises without the use of ground receiving or distribution equipment, except at the subscribers premises or in the uplink process to the satellite.

(2) PROVIDER OF DIRECT-TO-HOME SATELLITE SERVICE - For purposes of this section, a "provider of direct-to-home satellite service" means a person who transmits, broadcasts, sells, or distributes direct-to-home satellite service.

(3) LOCAL TAXING JURISDICTION - The term "local taxing jurisdiction" means any municipality, city, county, township, parish, transportation district, or assessment jurisdiction, or any other local jurisdiction in the territorial jurisdiction of the United States with the authority to impose a tax or fee, but does not include a State.

(4) STATE - The term "State" means any of the several States, the District of Columbia, or any territory or possession of the United States.

(5) TAX OR FEE - The terms "tax" and "fee" mean any local sales tax, local use tax, local intangible tax, local income tax, business license tax, utility tax, privilege tax, gross receipts tax, excise tax, franchise fees, local telecommunications tax, or any other tax, license, or fee that is imposed for the privilege of doing business, regulating, or raising revenue for a local taxing jurisdiction.

(C) PRESERVATION OF STATE AUTHORITY- This section shall not be construed to prevent taxation of a provider of direct-to-home satellite service by a State or to prevent a local taxing jurisdiction from receiving revenue derived from a tax or fee imposed and collected by a State.

TITLE VII - MISCELLANEOUS PROVISIONS

SEC. 701. PREVENTION OF UNFAIR BILLING PRACTICES FOR INFORMATION OR SERVICES PROVIDED OVER TOLL-FREE TELEPHONE CALLS.

(a) PREVENTION OF UNFAIR BILLING PRACTICES -

(1) IN GENERAL - Section 228(c) (47 U.S.C. 228(c)) is amended -
(A) by striking out subparagraph (C) of paragraph (7) and inserting in lieu thereof the following:

"(C) the calling party being charged for information conveyed during the call unless -

"(i) the calling party has a written agreement (including an agreement transmitted through electronic medium) that meets the requirements of paragraph (8); or

"(ii) the calling party is charged for the information in accordance with paragraph (9); or";

(B)(i) by striking "or" at the end of subparagraph (C) of such paragraph;

(ii) by striking the period at the end of subparagraph (D) of such paragraph and inserting a semicolon and "or"; and

(iii) by adding at the end thereof the following:

"(E) the calling party being assessed, by virtue of being asked to connect or otherwise transfer to a pay-per-call service, a charge for the call.":

[...]

Annexe 4

Mission à Bruxelles (13 et 14 mai 1996)

Liste des personnes rencontrées à la Commission des Communautés européennes

Michel Catinat, DG III A/5, conseiller du directeur-général : Relations industrie-recherche

Jean-Michel Baer, directeur DG X/D : Action culturelle et politique audiovisuelle

Jean-Éric de Cocborne, chef d'unité DG XIII : Aspects réglementaire d'accès aux réseaux communications par satellites, mobiles et fréquences

M. Argyris, directeur DG XIII/A : Télécommunications, réseaux et services transeuropéens : postes

Alain Stekke, DG XIII : Télécommunications, marché de l'information et valorisation de la recherche

M. Bruhann, chef d'unité DG XV/D 1 : Libre circulation de l'information, protection des données et aspects internationaux s'y référant

M^{me} Froehlinger, chef d'unité DG XV/E 5 : Médias, communication commerciale et concurrence déloyale

Jan Colaes, DG XXI/1 A : Douane et fiscalité indirecte

Jan Allix, administrateur principal DG XXIV A/4 : Politique des consommateurs

Code de déontologie de l'Internet service providers association (ISPA)

DRAFT Code of Practice
Revised: 10 April 1996
ISPA Draft Code of Practice

Preamble

This Code of Practice ("Code") shall govern the conduct of the members of the Internet Service Providers Association ("Members"). The adoption of the Code by Members shall be voluntary for the first twelve months following its adoption by the ISPA. Thereafter the application of the Code shall be uniform and obligatory to all Members without modification or exception. A Member may not then, by contract or otherwise, evade the application of the Code.

The Code shall be applied and enforced by the chief executive of the ISPA, ("the Secretariat"), who shall be independent from the Members. The application of the Code shall be reactive.

From time to time ISPA shall issue policy statements regarding matters relating to the regulation of the Internet in the UK. After due and proper consultation with the Members such policy statements may be adopted as a Practice Statement by ISPA. Such Practice Statements shall be incorporated into the Code and shall thereby be binding on Members. The Code may be further amended from time to time by a majority vote of the Members.

The Member agrees that in subscribing to the ISPA it shall abide by the Code (when adopted) and support the ISPA policies, the legitimate activities of the other Members and the Secretariat. Members must comply with the spirit as well as the letter of the Code.

Members recognise that compliance with the Code does not necessarily guarantee that they are acting within the law.

1.1.CODE OF PRACTICE

1. General Requirements

1.1 Legality

Members shall use their reasonable endeavours to ensure the following:

1.1.1 Services and promotional material do not contain anything which is in the breach of the law, nor omit anything which the law requires.

1.1.2 Members, their services and promotional material do not encourage anything which is in any way unlawful.

1.2 Decency

Members shall use their reasonable endeavours to ensure the following:

1.2.1 Services and promotional material do not contain material inciting violence, sadism, cruelty, or racial hatred.

1.2.2 Services and promotional material are not used to promote or facilitate prostitution.

1.3 Honesty

1.3.1 Members shall use their reasonable endeavours to ensure services and promotional material are not of a kind that are likely to mislead by inaccuracy, ambiguity, exaggeration, omission or otherwise.

1.4 Data Protection

1.4.1 When registering with the Data Protection registrar, all Members must in their application state that the data may be used for regulatory purposes and that ISPA is a potential user of that information.

1.4.2 No undertaking given by a Member to its customers, suppliers, information providers or others shall preclude any information pertinent to a complaint being given to ISPA in confidence.

1.4.3 The Members shall use its reasonable endeavours to ensure that services which involve the collection of personal information, such as name and addresses, must make it clear to the relevant party the purpose for which the information is required. The Members must also identify the data user (if different from the Members or information provider). The service must also give that party the opportunity to prevent such usage.

1.5 Fair trading

1.5.1 In its dealings with consumers, other businesses and each other, Members must act decently, fairly and reasonably at all times.

2. Promotion

2.1 Scope

2.1.1 In the case of promotions that appear in editorial material, Members must use all reasonable endeavours to ensure that promotions transmitted by radio, television, teletext, telephone, facsimile or any other form of communication must observe the provisions of this Code and the Codes of Practice published by the Independent Television Commission and the Radio Authority (where relevant) in the manner most reasonable and appropriate to the technology employed.

2.1.2 Members must also comply with the provisions of the British Codes of Advertising and Sales Promotion which is supervised by the Advertising Standards Authority.

2.2 Pricing Information

2.2.1 The Members must ensure that the charge for the service is clearly stated in relevant promotional material. The price quoted should include VAT (where applicable). Where additional charges, for example on-line charges are payable, this be stated.

2.2.2 Textual pricing information should be legible, prominent, horizontal and presented in such a way that does not require close examination.

3. Procedures and Sanctions

3.1 Complaint initiation - The exact procedure for complaint initiation is unclear at this time. Without reliable statistics on the number of likely complaints it is premature for the ISPA to determine a precise method. However, the ISPA anticipate that complaints will largely be presented by members of the general public, authoritative bodies (for example the Police, The Office of Fair Trading etc.) and other Members. Such complaints may be of an informal, formal or advisory nature. The procedure for complaints will be reviewed by the ISPA Committee at regular intervals and Members will be updated accordingly.

3.2 Standard Procedure - The ISPA Committee envisage that the procedure for the processing of those complaints will depend upon the complaint initiation. Essentially there are three possible routes for dealing with a complaint:

a. A complaint is made by, for example, a member of the public directly to a Member. The Member acts on that complaint and remedies the complaint to the satisfaction of the complainant.

b. A complaint is made by, for example, a member of the public directly to a Member. The Member fails to act. The complainant refers the complaint to the Secretariat of the ISPA.

c. A complaint is made by, for example, a member of the public directly to the Secretariat of the ISPA.

The procedure once the matter has been referred to the Secretariat of the ISPA will depend on the nature of the complaint. The Secretariat will be responsible for considering the full nature and extent of the complaint and will consult with the Member concerned. The Secretariat shall be entitled to consult relevant parties (for example the Office of Fair Trading) prior to determining the complaint. The Member agrees to co-operate fully with the Secretariat. The Secretariat shall be responsible for communicating his determination of the complaint to the Member and the complainant.

Where a complaint is upheld by the Secretariat, the Secretariat may seek to claim, at its sole discretion, the reasonable administrative costs incurred by the Secretariat in processing that complaint.

The Secretariat acknowledges that the Member in many circumstances will not have direct knowledge of the complaint referred and will initially contact the Member on an informal basis.

Where the Member is able to act on the advice of the Secretariat but unreasonably refuses to do so, or where Member is found repeatedly to be in breach of this Code, the Secretariat will be entitled to register the complaint as a formal complaint against the Member. Written notification of this will be forwarded to the Member by the Secretariat.

Members must comply with any conclusion reached by the Secretariat, including a decision to impose a sanction on the Member as a result of the Members breach of the Code.

The sanctions to be imposed by the Secretariat on behalf of the ISPA shall be regularly reviewed.

In the event the Member is found to be repeatedly breaching the Code the Secretariat may expel the Member from the ISPA.

Annexe 5

Recommandation du Conseil de l'Europe 95 R 13 (extraits)

Recommandation n° R (95) 13 relative aux problèmes de procédure pénale liés à la technologie de l'information

*(adoptée par le Comité des Ministres le 11 septembre 1995,
lors de la 543^e réunion des Délégués des Ministres)*

Le Comité des ministres, en vertu de l'article 15.b du Statut du Conseil de l'Europe,

Rappelant que le but du Conseil de l'Europe est de réaliser une union plus étroite entre ses membres ;

Eu égard au développement sans précédent de la technologie de l'information et de son application dans tous les secteurs de la société contemporaine ;

Réalisant que le développement des systèmes électroniques d'information va accélérer la transformation de la société traditionnelle en une société de l'information en créant un nouvel espace pour tout type de communications et de relations ;

Conscient de l'impact de la technologie de l'information sur la manière dont la société est organisée et sur la façon dont les individus communiquent et se mettent en relation ;

Conscient du fait qu'une partie croissante des relations économiques et sociales aura lieu à travers ou à l'aide de systèmes électroniques d'information ;

Préoccupé par le risque que les systèmes électroniques d'information et l'information électronique puissent également être utilisés pour commettre des infractions criminelles ;

Préoccupé par le fait que les preuves d'infractions pénales peuvent être stockées et transmises par le biais de ces systèmes ;

Notant que le droit de procédure pénale des États membres ne prévoit pas encore souvent les pouvoirs appropriés pour perquisitionner dans ces systèmes et y recueillir des preuves au cours des enquêtes pénales ;

Rappelant qu'au vu du développement de la technologie de l'information, le manque de pouvoirs spéciaux appropriés peut porter atteinte à la bonne exécution des fonctions assignées aux autorités chargées de l'enquête ;

Reconnaissant la nécessité d'adapter les moyens légaux dont disposent les autorités chargées de l'enquête en vertu du droit de procédure pénale au caractère spécifique des enquêtes dans les systèmes électroniques de l'information ;

Préoccupé par le risque potentiel que les États membres ne soient pas en mesure de fournir une entraide judiciaire de manière adéquate lorsqu'ils sont requis de recueillir des preuves électroniques, sur leur territoire, dans des systèmes électroniques d'information ;

Persuadé de la nécessité de renforcer la coopération internationale et de parvenir à une meilleure compatibilité des droits de procédure pénale en la matière ;

Rappelant la Recommandation n° R (81) 20 du Comité des Ministres relative à l'harmonisation des législations en matière d'exigence d'un écrit et en matière d'admissibilité des reproductions de documents et des enregistrements informatiques, la Recommandation n° R (85) 10 sur les commissions rogatoires pour la surveillance des télécommunications, la Recommandation n° R (87) 15 visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police et la recommandation n° R (89) 9 sur la criminalité informatique,

Recommande aux gouvernements des États membres :

1°) de s'inspirer, lorsqu'ils révisent leurs législation et pratique internes, des principes qui se trouvent en annexe à cette recommandation ; et
2°) de faire connaître ces dispositions aux autorités chargées de l'enquête et à d'autres services professionnels, en particulier dans le secteur de la technologie de l'information, qui peuvent être impliqués dans leur mise en oeuvre.

Annexe à la Recommandation n° R (95) 13 relative aux problèmes de procédure pénale liés à la technologie de l'information

I. Perquisition et saisie

1. La distinction opérée par le droit entre la perquisition de systèmes informatiques ainsi que la saisie des données qu'ils renferment et l'interception de données au cours de la transmission devrait être clairement délimitée et appliquée.

2. Les lois de procédure pénale devraient permettre aux autorités chargées de l'enquête de perquisitionner dans les systèmes informatiques et d'y saisir des données, dans les mêmes conditions que dans le cadre des pouvoirs traditionnels de perquisition et de saisie. La personne en charge du système devrait être informée que le système a fait l'objet d'une perquisition et de la nature des données saisies. Les recours juridiques prévus par la législation en général contre la perquisition et la saisie devraient être également applicables en cas de perquisition d'un système informatique et de saisie des données y contenues.

3. Dans l'exécution de la perquisition, les autorités chargées de l'enquête devraient avoir le pouvoir, sous réserve de garanties appropriées, d'étendre la perquisition à d'autres systèmes informatiques dans leur juridiction qui sont connectés par le biais d'un réseau et d'y saisir des données, à condition qu'une action immédiate soit requise.

4. S'il y a équivalence fonctionnelle entre les données faisant l'objet de traitement automatisé et un document traditionnel, les dispositions du droit de procédure pénale se rapportant aux documents devraient également s'appliquer aux données.

II. Surveillance technique

5. Étant donnée la convergence des technologies de l'information et des télécommunications, les législations concernant la surveillance technique employée à des fins d'enquêtes pénales, comme l'interception des communications, devraient être, là où cela s'avère nécessaire, révisées et amendées pour assurer leur applicabilité.

6. Les lois devraient permettre aux autorités chargées de l'enquête d'appliquer toute mesure technique permettant la collecte de données de trafic dans la poursuite des infractions pénales.

7. Lorsqu'elles sont collectées au cours d'une enquête pénale et en particulier quand elles sont obtenues par des moyens d'interception des télécommunications, les données protégées par la loi et faisant l'objet du traitement automatisé par un système informatique devraient être sauvegardées de manière appropriée.

8. Les droits de procédure pénale devraient être révisés en vue de rendre possible l'interception de télécommunications et la collecte de données de trafic dans le cadre d'enquêtes sur des infractions graves comme la confidentialité, l'intégrité et la disponibilité des systèmes de télécommunications ou informatiques.

III. Obligations de coopération avec les autorités chargées de l'enquête

9. Sous la réserve des protections ou privilèges prévus par la loi, la plupart des législations permettent aux autorités chargées de l'enquête d'ordonner à des personnes de remettre des objets qui sont sous leur contrôle et qui sont requis pour servir de preuve. Le droit de

procédure pénale devrait, de la même manière, accorder le pouvoir d'ordonner à des personnes de leur présenter toute donnée spécifique qui se trouve sous leur contrôle, dans un système informatique, dans la forme requise par les autorités chargées de l'enquête.

10. Sous la réserve des protections ou privilèges prévus par la loi, les autorités chargées de l'enquête devraient avoir le pouvoir d'ordonner aux personnes qui ont des données spécifiques sous leur contrôle de fournir toutes les informations nécessaires pour permettre l'accès au système informatique et aux données qu'il renferme. Le droit de procédure pénale devrait assurer que les autorités chargées de l'enquête puissent donner une instruction similaire à d'autres personnes ayant une connaissance du fonctionnement du système informatique ou de toute mesure employée pour préserver les données y contenues.

11. Des obligations spécifiques devraient être établies pour les opérateurs de réseaux publics et de réseaux privés lorsqu'ils offrent des services de télécommunication au public, d'appliquer toute mesure technique nécessaire permettant l'interception des télécommunications par les autorités chargées de l'enquête.

12. Des obligations spécifiques devraient être établies pour les fournisseurs de services qui offrent des services de télécommunication au public via des réseaux de communication publics ou privés, de délivrer l'information nécessaire lorsque les autorités compétentes chargées de l'enquête l'ordonnent, pour identifier l'utilisateur.

IV. La preuve électronique

13. L'intérêt commun de recueillir, de sauvegarder et de présenter des preuves électroniques de manière à garantir au mieux leur caractère irréfutable et leur intégrité devrait être reconnu tant pour les fins des poursuites nationales que pour celles de la coopération internationale. Cette fin, des procédures et méthodes techniques du traitement des preuves électroniques devraient être développées davantage de manière à assurer leur compatibilité entre les États. Les dispositions du droit de procédure pénale concernant les preuves et se rapportant aux documents traditionnels devraient également s'appliquer aux données stockées dans un système informatique.

V. Utilisation du chiffrement

14. Des mesures devraient être examinées afin de minimiser les effets négatifs de l'utilisation du chiffrement sur les enquêtes des infractions pénales, sans toutefois avoir des conséquences plus que strictement nécessaires sur son utilisation légale.

VI. Recherche, statistiques et formation

15. Le risque qu'impliquent le développement et l'utilisation de la technologie de l'information sur la perpétration des infractions

pénales devrait faire l'objet d'une évaluation continue. Afin de permettre aux autorités compétentes de rester familiarisées avec de nouveaux phénomènes en matière de criminalité informatique et de pouvoir développer des contre-mesures adéquates, la collecte et l'analyse des données concernant ces infractions, y compris les *modi operandi* et les aspects techniques, devraient être favorisées.

16. La création d'unités spécialisées pour la répression d'infractions dont la poursuite requiert une expérience spéciale en matière de technologie de l'information, devrait être examinée. Des programmes de formation permettant au personnel de la justice pénale d'approfondir leurs connaissances en la matière devrait être promus.

VII. Coopération internationale

17. Le pouvoir d'étendre la perquisition à d'autres systèmes informatiques devrait être également applicable lorsque le système se trouve sous une juridiction étrangère, à condition qu'une action immédiate soit requise. En vue d'éviter d'éventuelles violations de la souveraineté des États ou du droit international, une base légale explicite devrait être créée pour de telles perquisitions ou saisies étendues. Par conséquent, il y a un besoin urgent de négocier des instruments internationaux quant à la question de savoir comment, quand et dans quelle mesure de telles perquisitions ou saisies peuvent être permises.

18. Des procédures accélérées et appropriées ainsi qu'un système de liaison devraient être disponibles selon lesquelles les autorités chargées de l'enquête pourraient demander aux autorités étrangères de recueillir promptement des preuves. Cette fin, les autorités requises devraient être autorisées à perquisitionner dans un système informatique et d'y saisir des données en vue de leur transfert ultérieur. Les autorités requises devraient également être autorisées à délivrer des données de trafic se rapportant à une télécommunication spécifique, à intercepter une telle télécommunication ou à identifier sa source. Cette fin, les instruments d'entraide judiciaire existants devraient être complétés.

Annexe 6

Quelques exemples de « smileys »

:-) smiley de base	:-# je ne peux rien dire	:- surtout ne dites rien	%-) ne regardez pas la télé	+:-) smiley est un prêtre	:-{} smiley et son rouge à lèvres	!-(smiley à mal à la tête
:8) smiley est un cochon	*<:o) smiley est un clown	X-(smiley a très mal à la tête	:#) smiley a trop bu	==:-) smiley est un punk	,-) smiley est content	:-* smiley fait un bisou
:-\ smiley est indécis	3:] grand-mère smiley	0:-) smiley est un saint	:-© cantatrice smiley	:-[smiley est un vampire	:-) smiley aime REM et UZ	([(smiley est Robocop
~~:-(j'ai si mal que ma tête fume	:-% smiley les a là	==:-(les vrais punks ne courent pas	(:-) smiley est gaucher	:-/ smiley est septique	:-} smiley est gêné	:-& motus et bouche...
:- smiley fume un peu	:= smiley est un babouin	(:-(le smiley le plus triste	:/\) smiley joue Cyrano	:-(* c'est à gerber !	:-----} menteur comme Pinocchio	:-' smiley a de la fièvre
:-# smiley porte un appareil	(:-) smiley a la grosse tête	:-> smiley sarcastique	:-] allez Paris St Germain	8:-) la petite fille smiley	:-Q smiley fume beaucoup	@:-) smiley a été chez le coiffeur
:-" smiley sait siffler	7:^] smiley en Ronald R.	&- j'en ai pleuré	 -o smiley s'embête	8<:-) smiley est un magicien	:-~) smiley a le nez qui coule	(:-(pas du tout content
:-V smiley crie fort	:-(smiley verse une larme	:-)8< la grande fille smiley	:-? smiley fume la pipe	C==:-) smiley sait cuisiner	P-(smiley est un pirate	8-) smiley en Steve Wonder
:-r smiley tire la langue)0-) smiley fait de la plongée	8:-) vous aimez mes lunettes	:-X un gros bisou baveux	8-O oh ! mon Dieu !	:-@ smiley crie très fort	;-^) smiley est satisfait
:-o smiley parle beaucoup	0-) smiley fume quelque chose	[::-) smiley a un walkman	?-(oeil au beurre noir	8(:-) smiley aime Mickey	:-§ smiley a mal à la gorge	:-{ smiley porte la moustache

Annexe 7

Glossaire

AFCEE : Association française pour le commerce et les échanges électroniques. Créée en 1996, elle est un forum d'échange au service des acteurs qui la composent.

BAL : Boîte aux lettres servant à la messagerie électronique, lieu de conservation des messages avant que le client ne les rapatrie sur son terminal.

Codage numérique : Codage purement binaire des informations à transmettre ou à diffuser.

Compression numérique : Méthode consistant à réduire le nombre de bits par signal en supprimant les informations redondantes.

CRTC : Conseil de la radiodiffusion et des télécommunications canadien.

CSA, Conseil Supérieur de l'Audiovisuel : Autorité administrative indépendante chargée d'assurer la régulation du secteur de l'audiovisuel en application de la loi du 30 septembre 1986 sur la liberté de communication.

CST : Conseil supérieur de la télématique, chargé jusqu'en 1996 de la régulation de la télématique française, le Minitel et l'Audiotel.

CTA : Conseil de la télématique anonyme, subordonné au CST.

DAVIC ou Digital Audio-Video Council : Groupe de travail créé en 1994 pour normaliser les systèmes de télévision interactive.

Débit : Le signal à transmettre étant codé en symboles binaires ou bits, le débit mesure la quantité de bits transmis par seconde dans le signal.

Domaine : Ensemble des ressources regroupées sous un même nom (par exemple *telecom. gov.fr*). Y sont rattachés les utilisateurs sur le mode *xxxtelecom. gov. fr* ; et l'arborescence accessible sur le mode *www. telecom. gov. fr/français/activ/...*

FCC, Federal Communication Commission : Instance américaine de régulation des télécommunications et de l'audiovisuel.

Firewall : Passerelle sécurisée entre le réseau local d'une entreprise et l'Internet, permettant de prévenir les éventuelles attaques de pirates extérieurs à travers cet accès.

FTP : « File transfer protocol », protocole spécifique de l'Internet pour le téléchargement de fichiers.

G7 : Groupe des 7 pays les plus industrialisés, dont les gouvernements se réunissent périodiquement pour exprimer de grandes orientations politiques communes.

GIX, Global Internet Exchange : Plateforme permettant l'échange de trafic entre les grands fournisseurs d'accès à l'Internet.

HTML, Hypertext Markup Language : Langage définissant le format des informations mises sur le Web, par exemple la place du texte et des images, la définition des liens hypertexte, la procédure de remplissage de formulaires...

HTTP, Hypertext Transfer Protocol : Protocole de communication client-serveur utilisé pour les échanges de données sur le Web.

IAB, Internet, Architecture Board : Instance de supervision technique de l'Internet Society, qui oriente et utilise à des fins normatives les travaux effectués au sein de l'Internet Engineering Task Force.

IAP, Internet Access Provider : Fournisseur d'accès à l'Internet, offrant un service de connexion à la demande sur abonnement.

IETF, Internet Engineering Task Force : Subordonné à l'Internet Architecture Board, cet organe fédère les groupes techniques qui développent les technologies et les protocoles de l'Internet. L'Internet Research Task Force prépare quant à lui les évolutions de long terme.

INRIA, Institut national de recherche en informatique et en automatique : Organisme de recherche français le plus proche des instances de l'Internet.

Internet : Cette appellation a sans doute son origine dans l'un de ses groupes fondateurs, l'InternetNetwork Working Group, qui évoque l'interconnexion entre réseaux. Par extension, l'Internet désigne aujourd'hui l'ensemble des réseaux interconnectés grâce aux protocoles de l'Internet.

Intranet : Par opposition à l'Internet, l'Intranet désigne l'utilisation des technologies et des protocoles de l'Internet dans un milieu fermé, typiquement une entreprise, qui souhaite interconnecter ses réseaux internes.

Internaute : Désigne un utilisateur (assidu) de l'Internet.

IP, adresse IP : Internet Protocol, protocole de routage de l'Internet (niveau 3 dans la modélisation OSI), qui assure l'acheminement des paquets de données de proche en proche. *L'adresse IP* attachée aux paquets désigne son destinataire et permet donc que ce routage soit effectué.

ISOC, Internet Society : Organisme ouvert à tous se donnant pour mission le développement de l'Internet, utilisant l'IAB et ses sous-groupes pour gérer l'évolution technique de l'Internet. Cet organisme a un correspondant français, le « chapitre français » de l'ISOC présidé par M. Bruno Oudet.

ISO ou Organisation Internationale de Normalisation : Organisme de normalisation international, qui a notamment institué une modélisation des protocoles de communication en 7 couches, qui constituent un outil d'ouverture des systèmes d'information.

Java, Javascript : Langage, proche du langage C, qui permet d'intégrer des applications aux pages Web, qui seront activées chez le client quel que soit son terminal. Ceci permet par exemple de contrôler le remplissage d'un formulaire et d'en supprimer les erreurs chez le client, avant de l'envoyer au serveur. Javascript est une version simplifiée de Java.

kbits/s : Kilobit par seconde, débit unitaire de transmission de 1000 informations binaires par seconde. Les modems téléphoniques ont aujourd'hui une vitesse de 14,4 ou 28,8 kbits, le réseau numérique RNIS offre de 64 kbits à 384 kbits selon la ligne.

Lien hypertexte : Principe qui permet en sélectionnant sur une page Web un choix qui y est proposé, de passer instantané à une autre page ou à un autre serveur. Ceci permet une navigation de proche en proche, qui est à la base du succès du Web.

Mbits/s : Mégabit par seconde, débit unitaire de transmission d'un million d'informations binaire par seconde. Les modems câble offrent jusqu'à 10 Mbits, la télévision numérique compressée au standard européen DVB exige de 3,5 à 5 Mbits.

Moteur de recherche : Service accessible sur des serveurs du Web, donnant la liste des serveurs correspondant à la requête exprimée par les clients, en général par mots clés. Les plus connus sont Altavista, Lycos, Webcrawler, Netsearch de Netscape, et Yahoo, qui s'apparente plus à l'annuaire.

NIC, Network Information Center : Ces organismes, répartis par pays, gèrent une partie des adresses IP et les noms de domaines. Le NIC France, hébergé par l'INRIA, adresse les noms ayant le suffixe « . fr »

OCDE, Organisation de Coopération et de Développement Economique : Organisation intergouvernementale entre pays avancés chargée de promouvoir, par des recommandations, l'ouverture des marchés à des fins de développement économique.

PICS, platform for Internet Content Selection : Système de classification des contenus de l'Internet à partir des terminaux, soutenu par le RSAC, Recreational Software Advisory Council, organisme américain à but « non lucratif ».

PC, personal computer : Terminal dont il faut aujourd'hui disposer pour accéder au Web. On parle pour l'avenir du NC, Network Computer, moins cher mais plus dépendant du réseau pour ses ressources.

Protocole de communication : Désigne l'ensemble des échanges informatiques permettant aux différentes composantes d'un réseau d'interfonctionner. Ils sont modélisés en 7 niveaux par l'OSI (couches physique, liaison, réseau, transport, session, application - données, application - interface).

RENATER : Réseau National de télécommunications pour la Technologie, l'Enseignement et la Recherche, relie les universités et les centres de recherche français entre elles, et à l'Internet à travers une infrastructure à haut débit.

RIPE NCC : Réseaux IP Européens, Network Coordination Center, association des fournisseurs de réseaux Internet européens, attribuant notamment les adresses IP aux correspondants nationaux.

Routeur : Machine informatique effectuant le routage des paquets de données Internet à l'aide de leur adresse IP. Ils utilisent des tables de routage qu'ils mettent à jour périodiquement en échangeant des informations avec les autres routeurs.

TCP : « Transmission Control Protocol », couche transport des protocoles Internet (niveau 4 dans la modélisation ISO)

TCP/IP : « Transmission control protocol over Internet Protocol » désigne les protocoles utilisés par l'Internet, garants de l'interconnexion généralisée.

TSF : Directive européenne « Télévision sans Frontières » adoptée en 1989.

Smileys : Pictogrammes constitués par une suite de caractères alphanumérique du type :-) permettant aux internautes de donner la tonalité d'un message.

UIT, Union internationale des télécommunications : Organisation spécialisée de l'ONU, située à Genève, chargée de promouvoir les services de télécommunication dans le monde.

URL, Universal Resource Locator : Syntaxe informatique du Web indiquant la localisation d'une ressource sur l'Internet.

Usenet : Réseau offrant un service de discussion mondial en différé appelé usenet news.

VRML, Virtual Reality Modelling Language : Langage de modélisation d'objets graphiques permettant l'introduction sur les pages Web d'images artificielles animées en 3 dimensions. Ce langage est à la base des premières applications de « rencontres virtuelles », et pourrait être un outil puissant pour les jeux en réseau.

World Wide Web, W3, Web : Désigne l'ensemble des logiciels, protocoles, serveurs et contenus constituant le monde accessible à partir des logiciels de navigation Netscape, Mosaic,... et qui permettent aux clients d'accéder à des serveurs multimédia interactifs reliés entre eux par liens hypertexte, en utilisant l'Internet. Cette nouvelle offre semble être le facteur déclenchant de l'explosion de l'utilisation de l'Internet.

Table des matières

Sommaire	5
Synthèse	7
- Préférer l'autocontrôle au contrôle <i>a priori</i>	9
- Clarifier les responsabilités des acteurs	10
- Développer la coopération internationale	10
- Favoriser le développement du commerce électronique	11
- Créer un organisme de veille, le Comité des services en ligne	11
- Favoriser l'information, la formation et la mobilisation des acteurs	12
- Favoriser la présence française et francophone sur le réseau	12
Conclusion	13
Chapitre 1	
Présentation du réseau Internet	15
Historique du réseau : de la recherche militaire au réseau international	17
Structure physique et logique du réseau	18
Ressources physiques de transport de l'information	18
Outils logiques de transport de l'information : protocoles, adresses et noms	18
Services offerts par le réseau	21
Les services les plus répandus	21
Les nouveaux services	22
Le mode d'évolution des normes de l'Internet	23
Les acteurs en présence	24
Les opérateurs Internet	24
Les éditeurs de contenu	25
Le serveur d'hébergement	25
L'utilisateur	25
Internet et la télématique anonyme	25
L'état de l'Internet en France et les recommandations pour son développement	26
Conclusion	28

Chapitre 2	
Le droit positif	29
La spécificité de l'Internet	31
Distinction communication audiovisuelle/correspondance privée	31
- Conclusion	35
La délicate application à l'Internet	35
- En tant que service audiovisuel utilisant un réseau de télécommunication	35
- En tant que service dont la nature est de la correspondance privée	37
Le dispositif législatif actuel	39
Les dispositions sanctionnant les atteintes à la vie privée	40
Les dispositions protégeant les mineurs	41
- Il existe des dispositions non pénales protégeant les mineurs	41
<i>Réglementations spécifiques à chaque média</i>	42
- Le Code pénal comporte plusieurs infractions relatives à la mise en péril des mineurs	45
Les principales dispositions encadrant le droit de la consommation s'appliquent quel que soit le support	45
Deux lois garantissent la protection des données	46
- La protection des données à caractère personnel : loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés	46
- Protection contre la fraude informatique	46
Adaptation du dispositif législatif aux spécificités de l'Internet	47
La transnationalité de l'Internet	47
- Le droit pénal	47
- Droit commercial	49
- Protection des données de caractère personnel	50
Fugacité et volatilité des contenus	50
- Difficulté de l'enquête	50
Difficulté d'application de certains textes	50
Évolution très rapide des techniques et des stratégies	52
Conclusion	53
Chapitre 3	
L'enseignement des exemples étrangers	55
Les USA	57
Les principales dispositions du Decency Act	57
- Protection des mineurs	57
<i>Les services audiovisuels</i>	57
<i>Les réseaux câblés</i>	58
<i>Les services de télécommunications et les services en ligne</i>	58
- Le régime de responsabilité	59
- Conclusion	59
Les principaux enseignements de l'expérience américaine relative à l'Internet	60

- Une initiative prématurée	60
<i>Un concept en pleine évolution</i>	60
<i>Un concept nouveau</i>	60
- Auto-régulation	61
Conclusion	62
Le Canada	62
L'approche canadienne de l'Internet : liberté et présence sur le réseau	62
La méthodologie canadienne : une démarche non juridique, modeste et ciblée	63
Conclusion	63
La Communauté européenne	64
Compétence de la Communauté	64
Approche générale d'Internet	65
Des textes spécifiques protégeant les objectifs d'intérêt général	66
- La protection du consommateur	66
- Protection de la propriété intellectuelle	67
- Protection de la vie privée	67
Conclusion	67
Deux exemples européens : l'Allemagne et la Grande-Bretagne	67
En Allemagne	67
- Le débat constitutionnel	68
- L'approche de l'Internet	68
En Grande-Bretagne	69
Chapitre 4	
Les propositions et les pistes de réflexion	73
Préférer l'autocontrôle au contrôle <i>a priori</i>	76
Un contrôle <i>a posteriori</i> efficace	76
Favoriser l'autocontrôle des acteurs	77
- Le contrôle par les utilisateurs	77
- Les codes de déontologie	78
- Les contrats	79
Clarifier les responsabilités des acteurs	80
Les principes de mise en jeu de la responsabilité pénale	80
- Le régime de responsabilité de la presse et de l'audiovisuel se distingue du droit commun par un certain nombre de caractères spécifiques	80
- La télématique a emprunté le régime de responsabilité du droit de la presse et de l'audiovisuel	82
Les options possibles	83
- Transposition du droit spécifique de la presse et de l'audiovisuel	83
- Avantages du système	84
- Inconvénients du système	85
- Application aux services en ligne des règles de droit commun	85

Conclusion	86
Développer la coopération internationale	86
Dans le cadre de la coopération judiciaire	86
Dans le cadre de la coopération politique	87
- Au sein de la communauté européenne	87
- En dehors de la Communauté européenne	88
Dans les instances de l'Internet	89
Le commerce électronique	89
Créer un organisme de veille :	
le Comité des services en ligne	91
Favoriser l'information, la formation	
et la mobilisation des acteurs publics et privés	91
Favoriser la présence française et francophone	
sur le réseau	93
Annexes	95
Annexe 1	
Personnalités françaises auditionnées	97
Annexe 2	
Situation de l'Internet en France	
et dans le monde	99
Annexe 3	
Mission aux USA 6 au 9 mai 1996	103
Liste des personnes rencontrées	103
Decency Act of 1996	104
Annexe 4	
Mission à Bruxelles (13 et 14 mai 1996)	129
Liste des personnes rencontrées	
à la Commission des Communautés européennes	129
Code de déontologie de l'Internet service	
providers association (ISPA)	130
Preamble	130
Annexe 5	
Recommandation du Conseil de l'Europe	
95 R 13 (extraits)	135
Recommandation n° R (95) 13 relative	
aux problèmes de procédure pénale liés	
à la technologie de l'information	135
Annexe à la Recommandation n° R (95) 13	
relative aux problèmes de procédure pénale liés	
à la technologie de l'information	136
- I. Perquisition et saisie	136
- II. Surveillance technique	137
- III. Obligations de coopération avec les autorités chargées	
de l'enquête	137

- IV. La preuve électronique	138
- V. Utilisation du chiffrement	138
- VI. Recherche, statistiques et formation	138
- VII. Coopération internationale	139
Annexe 6	
Quelques exemples de « smileys »	141
Annexe 7	
Glossaire	143