Strasbourg, juin 1998 CC-Cult (98) 18

Conseil de l'Europe
Conseil de la Co-operation Culturelle -- http://culture.coe.fr

La Liberté d'Expression et les Reseaux de Communication

Document établi pour le Projet "Edition électronique, livre et archives"

Report établi par Paul Sturges

Département de l'information et de la bibliothéconomie
Université de Loughborough, Royaume-Uni

Remerciements

Nous prions les personnes dont les noms suivent de trouver ici l'expression de notre gratitude pour l'aide qu'ils nous ont apportée de diverses manières, mais toujours à titre personnel et non pas au nom de leurs organisations.

Barbara Buckley, British Library, Research and Innovation Centre, and Coalition for Public Information (CoPI).
Alan Cooper, Library Association.
Graham Cornish, IFLA Universal Availability of Publications Office.
Michael Day, UK Office for Library and Information Networking (UKOLN).
John Feather, Loughborough University.
John Lindsay, Kingston University and British Computer Society.
Ian Murray, Loughborough University.
Andrew Oldfield, International Electronic Publishing Research Centre (IEPRC).
Franck Parry, Loughborough University Library.
Mark Perkins, Overseas Development Institute.
Alan Poulter, Loughborough University.
Ross Shimmon, Library Association.

Nos remerciements s'adressent en particulier à *Goff Sargent* pour ses précieux conseils et appuis.

Premiere Partie:
La Liberté d'expression et les points d'accès publics

1. Introduction

L'apparition des réseaux électroniques a transformé l'environnement dans lequel s'effectue la communication d'informations aux utilisateurs de manières qui ne sont pas sans préoccuper vivement les acteurs de l'économie traditionnelle du Livre. On entend exprimer couramment le sentiment que l'information et les idées sont plus que jamais une libre monnaie d'échange qui ne peut ni ne doit faire l'objet d'aucune intervention. Cependant, la capacité de plus en plus répandue

du public d'accéder à la technologie et à en faire usage ne laisse pas d'inquiéter les gouvernements, les organismes responsables de la sécurité, les défenseurs des diverses orthodoxies et des conceptions établies de la morale publique qui voient dans ces réseaux une menace pour leur vision de la société. Les questions du contrôle des communications électroniques et des interventions portant atteinte à la liberté d'expression font l'objet d'amples débats et des restrictions sont souvent proposées.

On trouve d'ailleurs sur Internet nombre de sites Web et de groupes de discussion consacrés à ce thème. Des organisations professionnelles ou autres ont produit des codes de pratique et des documents sur la question, qui a été discutée dans maints articles de revues et de bulletins et, à un moindre degré, dans des ouvrages et journaux d'informatique, de droit, de politique, de gestion de l'information et de bibliothéconomie, de science et de technologie, sans parler des journaux et revues populaires. Certains de ces écrits peuvent à juste titre être considérés comme contribuant à semer la panique sous couvert de moralité. Il importe donc qu'une organisation telle que le Conseil de l'Europe puisse former une opinion dûment fondée sur la question.

La Cinquième Conférence ministérielle européenne sur la politique des communications de masse, tenue à Thessalonique, en Grèce, les 11 et 12 décembre 1997, a donné suite à l'engagement pris lors du Deuxième Sommet du Conseil de l'Europe, à Strasbourg les 10 et 11 octobre 1997, de chercher des réponses communes aux problèmes posés par le développement des nouvelles technologies de l'information en prenant pour thème "La société de l'information : un défi pour l'Europe". La Conférence a produit une déclaration et deux résolutions riches en implications pour les communications et les réseaux d'information. Ces documents soulignent la nécessité d'une auto-régulation des fournisseurs et opérateurs des services d'information et d'une éducation du public aux nouvelles technologies. A cette insistance se mêle l'inquiétude suscitée par l'exploitation de la technologie par des personnes et organisations qui encouragent la violence et l'intolérance et ne montrent aucun respect pour la dignité humaine. La notion de "service universel communautaire", invoquée à titre de principe directeur dans les résolutions, pourrait également être considérée comme le principe qui, implicitement, sous-tend le contenu du présent rapport.

Le rapport part de l'idée que tous les citoyens doivent avoir librement accès à l'information et la capacité d'exprimer leurs opinions aussi librement que possible, afin que la société, réagissant de façon dynamique aux changements, puisse continuer à mûrir. L'auteur du rapport estime également que ce principe vaut presque autant pour les enfants que pour les adultes. Les enfants ont besoin de trouver des réponses aux questions qui les préoccupent et doivent donc, à un stade donné de leur développement, être autorisés à juger par eux-mêmes des connaissances dont ils ont besoin. Il est toutefois naturel que certaines personnes souhaitent éviter d'être exposées à certaines formes d'expression ou d'y exposer leurs enfants. Ce désir ne justifie pas que l'on supprime totalement une catégorie ou un mode quelconque d'expression. Il constitue en revanche une raison valable pour accepter, à titre d'exercice légitime de leur liberté de choix, que des individus, des familles et des organisations telles qu'écoles, groupes de jeunes, voire même bibliothèques pour autant qu'elles assument le rôle de famille, recherchent des moyens de limiter le risque de se trouver exposés à certaines formes d'expression.

1.1 Buts et objectifs

Le présent rapport a pour but :

> D'examiner l'état et les perspectives de la liberté d'expression sur les réseaux de communication afin de mettre en lumière les problèmes qui influent sur la pratique actuelle et forment le contenu du débat.
>
> D'attirer l'attention sur les expériences, initiatives et propositions pratiques qui ont affecté ou pourraient affecter la capacité des utilisateurs de réseaux à exercer cette liberté d'expression.

De rendre compte autant que possible des expériences et des opinions, à travers le monde et dans les divers secteurs (et notamment dans les industries de l'édition, des multimédia et des communications, dans le monde des bibliothèques et de l'information et dans les autres domaines professionnels et intellectuels pertinents).

1.2 Définitions

Il peut ne pas y avoir entièrement accord, en matière de terminologie, entre fournisseurs et utilisateurs de l'information qui opèrent par l'intermédiaire de médias tels qu'Internet et les personnes ou organisations dont les préoccupations sont essentiellement d'ordre éthique et touchent aux droits de l'homme. Aussi trouvera-t-on ici une description un peu plus détaillée de ce que l'on entend par "réseaux" (et notamment par l'Internet) aux fins du présent rapport ainsi qu'une indication du sens dans lequel des termes tels que "liberté d'expression" et "censure" sont utilisés.

1.2.1 Réseaux

Les réseaux relient des ordinateurs, à l'intérieur d'un site unique (réseau local ou LAN) ou par l'intermédiaire de systèmes de télécommunications connectant des sites géographiquement épars (réseau grande distance ou WAN). Ces réseaux peuvent permettre aux utilisateurs d'accéder non seulement à des équipements partagés (fichiers, logiciels, bases de données, imprimantes, télécopieurs), mais aussi à des services de communication (messagerie électronique et conférence). Les réseaux peuvent être raccordés à d'autres réseaux par l'intermédiaire de passerelles. Lorsqu'est utilisé un protocole et un système d'adressage tcp/ip commun, un Internet est créé. Le réseau global et public d'accès connu sous le nom d'Internet est la somme de tous les réseaux de ce type en communication les uns avec les autres. La caractéristique de l'Internet en tant que véhicule de l'information est qu'il n'a ni centre, ni autorité de contrôle. Il croît de façon organique, à mesure que de nouveaux réseaux y sont ajoutés. A l'origine, aux Etats-Unis, l'Internet avait une fonction essentiellement militaire et sa structure distribuée, tant en ce qui concerne les canaux de communication que l'introduction de l'information, en faisait un outil à l'épreuve de toute attaque ou contrôle militaire. Sa robustesse, conjuguée à son caractère international, en fait aussi un moyen de communication difficile à contrôler pour les autorités civiles.

Les questions concernant les protocoles Internet et autres questions touchant à l'ensemble du réseau, telles que les noms de domaines, les adresses IP des ordinateurs interconnectés, sont traitées par la Société Internet. L'efficacité de l'ensemble du système de communication dépend de l'acceptation par les utilisateurs des directives de la Société. L'utilisateur a accès à Internet par l'intermédiaire d'un fournisseur d'accès, qui est en règle générale une institution universitaire ou une organisation commerciale qui se consacrent à cette forme de service. La navigation sur Internet des utilisateurs est facilitée par l'existence de divers fournisseurs qui peuvent offrir une sorte d'annuaire, ou de catalogue de référence, des sites qui donnent des informations sur des fournisseurs de services, ou des moteurs de recherche qui permettent à l'utilisateur de trouver des informations sur le contenu de son choix à partir de mots-clés. L'information stockée sur Internet est mise à la disposition des utilisateurs par une gamme variée de fournisseurs de contenu : individus enthousiastes, groupes ou grosses organisations commerciales dont beaucoup voient dans l'Internet une source de profit. Bien que la majeure partie des contenus se présentent sous forme de textes, on observe une quantité croissante de contenus en modes plus sophistiqués sur le plan technique tels que l'audio, l'animation ou la vidéoconférence. Le contenu est soit accessible en temps réel, soit par téléchargement sur l'ordinateur personnel de l'utilisateur. Les problèmes de propriété intellectuelle, de responsabilité quant au contenu de l'information, de moyens de contrôler ce contenu et de facturation des transactions commerciales sont les principales questions liées au contenu de l'Internet. Les ordinateurs d'Internet, ou serveurs, informent leur propriétaire de la capacité de l'ordinateur ou, comme dans le cas des serveurs de Usenetnews, fournissent des ressources supplémentaires à des tiers.

Pour la plupart des utilisateurs, certaines des sources d'information et de communication disponibles par l'intermédiaire d'Internet ont plus d'importance que d'autres. Les "newsgroups" ou groupes de discussion présentent un immense intérêt en tant que moyen de communication publique. Les utilisateurs postent des articles, c'est-à-dire adressent des messages à un ou plusieurs des milliers de groupes qui traitent de domaines spécifiques, à titre souvent de contribution à un débat suivi sur le thème en question. C'est là un mode relativement éphémère de communication, car le matériel est en général éliminé après un certain laps de temps. Les messages sont toutefois fréquemment réaffichés, habituellement sans le consentement explicite de leurs auteurs, et adressés à un ou plusieurs autres groupes. Les sources publiques d'information de caractère plus permanent se trouvent généralement sur le World Wide Web (WWW). Les sites du Web donnent accès à des fichiers HTML (acronyme désignant le Hypertext Markup Language, c'est-à-dire le langage de description de page utilisé dans le WWW) et sont connectés par des liens en hypertexte. Il est relativement facile à toute personne ayant accès à un serveur et capable de travailler en HTML de publier des textes électroniquement. C'est dire que les communications informelles et la publication sur Internet sont des activités démocratiques accessibles au grand public à un degré inhabituel. Cette facilité est, à son tour, à l'origine des craintes exprimées dans les milieux officiels et populaires au sujet d'Internet en tant que moyen d'expression.

L'Internet est toutefois un outil de recherche individuelle à des fins précises. Bien que la découverte accidentelle d'informations y soit chose fréquente, elle ne peut être assimilée à l'exposition fortuite à des idées et à des images qui se produit inévitablement avec les mass media. Cette possibilité d'exposition inattendue et occasionnelle est une des principales raisons invoquées à l'appui d'un contrôle du contenu des mass media, mais elle ne saurait valoir pour l'information acheminée par réseau dans la même mesure. Plutôt que de se fixer sur les dangers découlant de certaines des informations transmises par réseau, il vaudrait mieux souligner la valeur de l'accès à des informations détaillées sur une vaste gamme de sujets, sans pratiquement de restrictions, qu'offre Internet. Le fait qu'on puisse trouver des informations fausses, trompeuses, inappropriées ou préjudiciables aux yeux de certains présente certes des risques. Ces risques doivent toutefois être acceptés comme étant l'envers des avantages qu'offre la liberté d'expression dans toute société, Internet ne constituant pas une exception à cet égard.

1.2.2 Liberté d'expression et censure

La liberté d'expression est définie de manière positive à l'article 10 de la Convention européenne des droits de l'homme, dans d'autres conventions internationales et dans les constitutions et législations de divers pays. Elle l'est au premier chef dans la Constitution des Etats-Unis, dont le premier amendement interdit au Congrès de "restreindre la liberté de parole, ou de la presse". La protection de la vie privée, telle que prévue à l'article 8 de la Convention européenne, présente également une très haute importance, notamment en ce qui concerne l'élaboration et l'articulation d'opinions peu conformes à l'orthodoxie et aux vues officielles. Les déclarations en faveur de la liberté d'expression visent manifestement à protéger les idées tant populaires qu'impopulaires mais prévoient presque invariablement certaines limites au champ des libertés offertes. L'article 10 de la Convention européenne mentionne dans ce contexte la sécurité nationale, la prévention des atteintes à l'ordre public et la délinquance, la protection de la santé et de la moralité, etc.

Les exceptions à l'universalité du principe peuvent toujours être étayées par de solides arguments; il convient toutefois de ne pas perdre de vue que ce sont précisément là les arguments invoqués pour justifier les systèmes de censure officiels. S'agissant des bibliothèques, l'"American Library Association" (Comité des libertés intellectuelles de l'Association, 1986) a défini la censure comme étant :

> les modifications apportées par l'autorité ou par ses représentants au droit d'accès à certains matériaux. Sont considérées comme de telles modifications l'exclusion, la restriction, la suppression et tout changement

de l'âge ou du niveau ouvrant droit à l'accès.

La censure officielle peut être l'expression formelle de craintes populaires, fort communes, touchant à la liberté d'expression. Ces craintes se manifestent avec une vigueur particulière à propos de certains sujets (la pornographie impliquant des enfants, par exemple), ou de modes donnés de communication (tels l'Internet). Sous l'empire de ces craintes, des groupes associés à une religion, à un mode de vie, à une philosophie, à des intérêts économiques ou à une tendance politique déterminée peuvent chercher à persuader les législateurs, les tribunaux ou le public de supprimer une certaine forme d'expression. Le présent rapport appellera l'attention sur diverses organisations, groupes de pression et censeurs putatifs. Il s'attachera également au travail des organisations qui militent en faveur de la liberté d'expression.

Il convient également de ne pas perdre de vue que nombre de contraintes autres que la censure pèsent sur la liberté d'expression et d'information. Bien que dans une société mûre et démocratique, elles puissent ne pas avoir l'influence déterminante qu'elles ont dans des pays moins développés, elles sont toujours présentes. Parmi elles figurent, au premier rang, les droits de propriété intellectuelle et autres servitudes découlant de la propriété de l'information, de la propriété des media par l'intermédiaire desquels l'information est diffusée et des coûts afférents à l'accès à l'information pour les utilisateurs. Vus sous l'angle d'un environnement futur où les communications seront soumises à davantage de contraintes commerciales, l'accessibilité et le coût relativement faible d'Internet, ainsi que sa presque totale liberté d'utilisation pourraient fort bien apparaître comme un âge d'or. Cette question liée à celle de l'accès en général soulève un ensemble trop vaste et complexe de questions pour être mentionnées autrement qu'en passant dans le présent rapport.

1.3 Méthodes

Le présent rapport a été établi à partir d'un échantillon des sources actuelles d'opinion et d'informations comportant :

- Une revue des articles et ouvrages publiés (y compris des articles de presse pertinents) et des sites web;
- Des consultations avec des membres des organisations pertinentes et des observateurs indépendants, et des dialogues divers menés par l'intermédiaire du courrier électronique, du téléphone et de la poste;
- Un examen de documents des organismes professionnels, associations commerciales et groupes de pression intéressés;
- Une évaluation de l'état d'avancement des propositions (d'ordre juridique ou relevant de l'auto-règlementation) visant à modérer le flot de l'information acheminée par l'intermédiaire des réseaux.

1.4 Résultats escomptés

Notre propos était de produire un rapport contenant :

- Un aperçu des questions essentielles soulevées par l'exercice de la liberté d'expression sur les réseaux de communication, illustré par des exemples concrets lorsque faire se pouvait;
- Une discussion et une évaluation des initiatives, propositions et menaces, notamment celles se présentant sous forme de législation, et des efforts d'auto-régulation au moyen de systèmes de filtrage et de codification;

Des suggestions sur la poursuite des recherches, des expériences et des discussions de nature à contribuer à l'élaboration d'une Recommandation ou "Charte" de la liberté d'expression dans l'édition électronique.

2. Le Debat "Liberte ou Controle"

2.1 Historique du débat

Les réseaux sont généralement perçus comme étant dans une large mesure entre les mains des utilisateurs, et cela d'autant plus qu'Internet n'est pas soumis à un contrôle central. En cela, ils ressemblent à la presse imprimée dont l'accès entièrement décentralisé en a toujours fait le moyen d'expression des opinions dissidentes. Les réseaux diffèrent toutefois sensiblement des médias audio-visuels qui, dépendant d'un moyen central de transmission, ont habituellement été soumis avec succès à un degré ou un autre de règlementation. Le fait que la majorité de la population, même dans les pays industrialisés, ne connaisse Internet que de réputation, ou n'en ait qu'une connaissance personnelle limitée, signifie que les craintes et les paniques que le réseau suscite peuvent librement se développer. Une partie des journalistes et autres auteurs qui en commentent le contenu et des agents de la puissance publique dont les compétences englobent les questions de communication, témoignent eux aussi d'une connaissance et d'une compréhension très limitées de ce nouvel outil. La brève histoire d'Internet a de ce fait été assez turbulente.

Parmi les craintes exprimées à son sujet figurent :

la menace qu'Internet présente pour la sécurité du pays et celle des entreprises du fait des activités de pirates;

l'utilisation du réseau pour des causes politiques extrêmes, qu'il s'agisse de la circulation publique de certaines opinions ou des communications privées cryptées;

la mise à disposition du public de matériel dangereux sur des questions telles que la drogue, les armes, etc.;

la diffusion de matériel attentant à la pudeur, et notamment de pornographie impliquant des enfants;

l'utilisation des réseaux pour porter atteinte aux droits de propriété intellectuelle, sous la forme de textes, de matériel audio-visuel, de logiciels et sous d'autres formes;

la diffusion d'attaques et d'insultes de caractère personnel adressées à des individus, à des organisations, à des groupes sociaux, ethniques ou autres.

Ces craintes ont trouvé une expression dans quelques affaires publiques célèbres, dont un ou deux exemples donneront une idée.

A la fin des années 1980, les services secrets américains suivaient régulièrement les "Bulletin Boards" électroniques pour déceler les communications ayant trait aux activités des groupes de pirates, dont ils pensaient qu'ils voulaient monter une opération de sabotage contre les réseaux de télécommunication (Sterling, 1992). Un faux "Bulletin Board" avait également été créé dans l'espoir de recueillir des messages incriminants qui révéleraient des activités soupçonnées d'être illégales. Dans ce cadre, avait été organisée, sous le nom de code Sun Devil, une descente de police contre des personnes soupçonnées d'être des pirates, descente durant laquelle on avait fouillé 28 locaux et confisqué plus de 40 ordinateurs et 23.000 disquettes. Une société, la Steve Jackson Games, qui semblait n'avoir qu'un lien des plus lointains avec le délit présumé, avait fait l'objet d'une enquête et, dans ses locaux, un jeu en cours d'élaboration avait été qualifié par les enquêteurs de

"manuel de délinquance informatique". La société et ses employés avaient ensuite dû engager une longue et coûteuse procédure pour obtenir la restitution des biens confisqués sur la base de ces soupçons.

En 1991, un "newsgroup" (groupe de discussion) a été créé sous le titre alt.religion.scientology pour discuter des questions touchant à ce culte ou à la religion. Des membres, opposés à cette initiative, ont commencé, à partir de décembre 1994, à mener, par divers moyens, une action hostile contre le groupe. Prétendant notamment que les messages postés au groupe contenaient du matériel relevant du droit d'auteur, ils ont tenté de mettre un terme aux activités du groupe. Des actions judiciaires ont également été intentées contre des individus qui avaient participé aux critiques formulées à l'encontre de la scientologie par l'intermédiaire du groupe. Malgré le peu de succès rencontré auprès des tribunaux, les séries complexes d'actions menées par les scientologistes constituaient une menace susceptible de porter atteinte à la liberté de discussion et de critique. Elles ont, en fait, eu un résultat assez opposé, la notoriété de l'affaire contribuant à multiplier et à propager les débats et les citations de documents relatifs à la scientologie (Wallace et Mangan, 1996).

En juillet 1993, deux citoyens californiens, Robert et Carleen Thomas, qui fournissaient des matériaux pornographiques par l'intermédiaire de leur "Amateur Action Bulletin Board System", ont fait l'objet d'une enquête de la part de fonctionnaires des services postaux du Tennessee. Ils ont ensuite été accusés d'avoir commis un certain nombre de délits dans cet Etat, et notamment d'avoir transporté d'un Etat à un autre des dossiers contenant des matériaux obscènes. L'affaire, et la condamnation des accusés, ont soulevé un certain nombre de questions, portant sur le point de savoir si ce matériel était effectivement obscène, s'il risquait ou non d'être vu à leur corps défendant par des membres du public et si le matériel acheminé par un réseau est en fait "envoyé" à ceux qui en obtiennent possession (Wallace et Mangan, 1996).

La conclusion qui se dégage de ce genre d'affaires est que les communications transmises sur des réseaux par certains individus, ou par des groupes réduits ou insignifiants, tendent à attirer l'attention des organismes publics ou de puissantes organisations. Les mesures prises ensuite sur la base des dispositions de diverses lois et règlements aboutissent à de prétendues injustices qui suscitent l'intérêt d'organisations créées pour défendre la liberté d'expression. Le cas de la société Steve Jackson Games soulevant tout un groupe de questions touchant à la liberté de parole, aux informations prétendument dangereuses et à la délinquance informatique, l'association "Computer Professionals for Social Responsibility" s'est prévalue des dispositions de l'"US Freedom of Information Act" (Loi américaine relative à la liberté de l'information) pour obtenir des détails sur les activités des services secrets. Bien que, dans le cas de Robert et Carleen Thomas, les accusés aient ouvertement reconnu qu'ils gagnaient leur vie en vendant de la pornographie, l'affaire a été prise en main par des organismes tels que Electronic Frontier Foundation (EFF) et l'American Civil Liberties Union (ACLU). La condamnation prononcée donnait en effet à entendre que les communications sur Internet considérées comme légales dans une juridiction pouvaient être jugées illégales dans une autre. Dans l'affaire de l'Eglise de la scientologie, la EFF est intervenue pour dire qu'il valait mieux éviter de poursuivre l'affaire en justice en raison de ses effets dommageables pour les petits fournisseurs.

L'affaire qui probablement a le plus conduit à une polarisation de l'opinion publique a pour origine une étude sur le matériel pornographique disponible sur Internet faite par Martin Rimm du Département du génie électrique de l'Université Carnegie Mellon. Alléguant en 1994 qu'il avait identifié plus de 900.000 images à contenu sexuel sur le réseau durant une courte période, Martin Rimm a porté le fait à l'attention de l'administration de l'Université, qui a réagi en barrant l'accès via les ordinateurs de l'Université à divers secteurs du système, et notamment aux groupes Usenet désignés par alt.sex. Cette mesure s'est heurtée à l'opposition de l'ACLU et d'autres groupes de pression œuvrant en faveur de la liberté d'expression pour des raisons de principe et parce qu'elle avait pour effet de dénier aussi au public l'accès à nombre de matériaux fort intéressants et

parfaitement légaux (tels que ceux ayant trait aux rapports sexuels protégés). La mesure avait de surcroît suscité des inquiétudes en raison de son effet possible sur d'autres institutions, l'Université Carnegie Mellon occupant une position charnière dans les activités informatiques menées en coopération par diverses universités (Faucette, 1995). En dépit des doutes qui ont été publiquement exprimés sur la validité des chiffres de Rimm, ces chiffres et la réaction de l'Université servent désormais en quelque sorte de référence lors de tous les débats publics sur le sujet (Hoffman et Novak, 1995).

La presse a fréquemment publié des articles inflammatoires sur les prétendus dangers d'Internet, faisant souvent état de cas tels que celui de l'Université Carnegie Mellon. Ici encore quelques exemples suffiront. La revue Time a publié en première page un article de Philip Elmer-DeWitt, fondé sur les observations de Rimm, qui a été cité comme un des principaux documents suscitant l'inquiétude du public aux Etats-Unis (Elmer-DeWitt, 1995). L'Observer (Royaume-Uni) a publié, dans son numéro du 25 août 1996, le nom de personnes qu'il a accusées d'être de "vils marchands colportant une culture de violence à l'encontre des enfants" sur Internet. Il a violemment rejeté les arguments avancés par les fournisseurs qui prétendaient vouloir éviter une "censure inadmissible" en disant :

> Ils plaident non pas pour la liberté, mais pour que la société leur donne licence de propager de parfaites horreurs. Cet argument est inadmissible. L'Observer apporte sans hésiter son appui à tous ceux qui, de la police aux groupes de protection de l'enfance, appellent à un contrôle et à une totale interdiction (Pedlars, 1996).

Le Daily Mail (Royaume-Uni) a soutenu, dans son numéro du 6 octobre 1997, qu'Internet portait atteinte à la souveraineté de la nation et constituait une menace pour le commerce, la morale, la paix, l'application des lois et la cohésion sociale. L'auteur de l'article soutenait que :

> Les entrepreneurs qui gagnent des milliards grâce à Internet devraient dépenser une fraction plus grande de leurs bénéfices pour contrôler et filtrer les matériaux qui passent par leurs systèmes. S'ils manquent à le faire, il nous faudra créer une police des mondes virtuels qui ait le pouvoir de regarder partout et d'effacer la saleté (Jeffreys, 1997).

Ces affaires ont donné naissance à un énorme volume de commentaires. Quelques mesures ont été prises contre les délinquants présumés par les organismes chargés de l'application des lois, ou par ceux qui estimaient avoir subi quelque préjudice du fait d'activités sur Internet. On a souvent entendu exprimer le sentiment que quelque chose devrait être fait à ce sujet.

2.2 Le "Communications Decency Act" des Etats-Unis

Le "Communications Decency Act" (CDA), introduit en 1995, dans le cadre d'une série de réformes des télécommunications, l'a été explicitement en réaction aux préoccupations exprimées dans la presse et par divers groupes de pression. Cette mesure, parrainée par les Sénateurs Exon et Gorton, a eu pour effet de criminaliser l'acheminement de matériaux obscènes sur des réseaux électroniques et prévu l'imposition d'amendes à hauteur de 10.000 dollars et de peines d'emprisonnement allant jusqu'à deux ans. Elle interdit expressément d'utiliser sciemment "un service informatique interactif" pour "envoyer" ou "afficher" tout matériau "de caractère manifestement offensant" à une personne de moins de 18 ans. La loi a été adoptée le 1er février 1996 et signée pour entrée en vigueur par le Président Clinton le 8 février. Le même jour, un groupe d'organisations ayant à sa tête l'American Civil Liberties Union (ACLU), intitulé la Citizens Internet Empowerment Coalition (CIEC), a introduit une instance en contestant la constitutionnalité. On trouvera une analyse détaillée de son argumentation dans Lapin (1996). L'affaire s'est conclue sur une décision de la Cour suprême, connue sous le nom de Reno versus ACLU qui, le 26 juin 1997, a déclaré la CDA inconstitutionnelle en vertu des dispositions du

premier amendement de la Constitution des Etats-Unis fondée au motif suivant :

> Conformément à la tradition en matière constitutionnelle et en l'absence de preuve contraire, nous présumons que la règlementation par les pouvoirs publics du contenu de la liberté de parole est davantage de nature à interférer avec le libre échange d'idées qu'à l'encourager. L'intérêt qu'il y a à encourager la liberté d'expression dans une société démocratique l'emporte sur les avantages théoriques mais non avérés que peut présenter la censure.

Le débat suscité par la CDA et les actions judiciaires qui l'ont suivie ont été à l'origine de discussions sur la question de la règlementation des réseaux non seulement aux Etats-Unis, mais dans le reste du monde. Après la décision jugeant la Loi inconstitutionnelle, le Président a immédiatement réuni à la Maison Blanche un "Internet Decency Summit" le 16 juillet 1997. A cette réunion, la discussion a essentiellement porté sur des formes de régulation telles que systèmes d'étiquetage, de codification (rating), de filtrage et de blocage. Une tentative a presque aussitôt été faite de renforcer cette démarche par voie législative lorsque le sénateur McDade de Pennsylvanie a présenté un projet de loi intitulé "Family Friendly Internet Access" qui obligerait les fournisseurs de services Internet à fournir à leurs clients un logiciel de filtrage du contenu gratuitement ou au prix coûtant. La phase de la discussion suivant le rejet de la loi CDA semble constituer une éclatante victoire du groupe de pression en faveur de la liberté d'expression, mais la nouvelle insistance sur l'étiquetage, le filtrage et le blocage des sites a été décrite comme étant plus insidieuse et tout aussi dangereuse (ACLU, 1997; Lessig, 1997).

2.3 Principaux acteurs

Le débat se déroule avec la participation des parties suivantes : pouvoirs publics, organismes chargés de l'application des lois, divers groupes d'intérêts politiques de caractère libertaire (comprenant notamment des défenseurs de la liberté d'expression), églises, groupes de pression détenteurs de la morale, media, sociétés appartenant à l'industrie des télécommunications et de l'informatique et leurs organes représentatifs, bibliothécaires et autres professionnels de l'information. En ce qui concerne les gouvernements, le désir de parer aux dangers de l'information sur les réseaux n'est pas limité aux Etats-Unis. Le 30 juillet 1996, le Groupe G7 des pays industrialisés et la Russie sont convenus en principe de soumettre Internet à des contrôles et notamment de mener une action contre les cryptages que les gouvernements ne peuvent pénétrer.

L'opinion politique peut se diviser de manière inattendue. Une conférence sur "L'espace cybernétique et le rêve américain" s'est tenue à Aspen, dans le Colorado, en août 1995, sous les auspices de la fondation "Progrès et liberté", groupe de réflexion très proche du Président de la Chambre des représentants américaine, Newt Gingrich, et de la tendance libertaire de droite du Parti républicain (Right turn, 1995). Parmi les intervenants figuraient des membres de l'Electronic Freedom Foundation (EFF), précédemment liés aux milieux gouvernementaux du Parti démocrate du Président Clinton, qui toutefois avaient été déçus par la politique officielle sur toute une gamme de questions touchant à la liberté d'expression. L'analyse et les conclusions des participants étaient dans leur énorme majorité opposées à toute réglementation et à toute ingérence gouvernementale.

L'idée de règlementation du réseau est fortement encouragée par des groupes religieux ou à vocation familiale qui se disent préoccupés par le type de matériel auquel pourraient avoir accès des enfants. Ainsi, la réaction d'un de ces groupes, le Family Research Council, à la décision prise dans l'affaire Reno v. ACLU a été que :

> Les portes restent grandes ouvertes à tous les marchands d'ordures. En l'absence de loi prévoyant la responsabilité juridique de ceux qui poursuivent les enfants au moyen d'images et d'un langage des plus

> explicites sur Internet, il nous faut agir rapidement et fermement pour veiller à ce que notre pays ne donne pas à la pornographie de droits spéciaux (Family Research Council, 1997).

Des groupes féministes appuient eux aussi vigoureusement l'idée d'une règlementation d'Internet. Estimant que la doctrine de la liberté de parole prédomine sur Internet, ils demandent une stricte règlementation d'un support qui, à leur sens, peut conduire à une escalade des violations des droits des femmes. Il est vrai aussi qu'il existe des féministes opposées à cette démarche qui estiment qu'en donnant à quiconque le pouvoir de censurer une forme donnée d'expression, soit en l'occurrence la pornographie, ou en entérinant un tel pouvoir, elles accordent le pouvoir de censurer le discours féministe aux même sources officielles où, disent-elles, domine une opinion sexiste et antiféministe (Carol, 1996).

Le groupe de pression anti-censure est constitué par un certain nombre de groupes de pression aux liens assez lâches, dont certains sont occupés à défendre la liberté d'expression en tant que droit de la personne humaine, tandis que d'autres sont préoccupés par les questions d'information et de communication. L'ACLU est un exemple du premier groupe et l'EFF du deuxième. L'ACLU, fondée en 1920 pour protéger et élargir les droits constitutionnels et libertés civiles américaines, a à son actif nombre de campagnes importantes et d'instances devant les tribunaux. La "People for the American Way", créée en 1980 pour surveiller les activités du mouvement politique de la droite religieuse et les contrer, est une organisation du même genre, mais à vocation plus large, qui prend vivement fait et cause pour la liberté sur Internet.

L'EFF, qui a joué un rôle important dans la présentation des arguments en faveur d'une non-règlementation d'Internet, se définit comme "une organisation d'intérêt public et de défense des libertés civiles à but non lucratif œuvrant pour protéger la liberté d'expression, la vie privée et l'accès aux ressources et à la formation en ligne". Elle est d'orientation entièrement libertaire, et ses déclarations reflètent souvent la pensée de John Perry Barlow, auteur de "Une déclaration de l'indépendance de l'espace virtuel", rédigée le 8 février 1996, c'est-à-dire à la date à laquelle le Président Clinton a signé la loi portant création de la CDA (Dority, 1996). L'EFF compte des branches locales dans diverses parties du monde et a lancé la campagne du Blue Ribbon (le Ruban bleu) qui vise à encourager les sites favorables à la liberté d'expression à arborer ce motif. Une organisation qui lui est associée, la Global Internet Liberty Campaign" (GILC), se veut plus explicitement internationale et relie 38 organisations membres, situées principalement aux Etats-Unis et en Europe.

Les poursuites judiciaires menées contre la CDA ont rassemblé un groupe composé d'organismes du même genre ainsi que d'organisations commerciales intéressées. La liste qui suit est instructive à cet égard :

> American Library Association
> America Online Inc
> American Booksellers Association
> American Booksellers Foundation for Free Expression
> American Society of Newspaper Editors
> Apple Computers Inc
> Association of American Publishers
> Association of Publishers, Editors and Writers
> Citizens Internet Empowerment Coalition
> Commercial Internet Exchange Association
> CompuServe Inc
> Families Against Internet Censorship
> Freedom to Read Foundation
> HotWired Ventures
> Interactive Services Association

Microsoft Corporation
Microsoft Network
Netcom Online Communication Services Inc
Newspaper Association of America
Opnet Inc
Prodigy Services Co
Society of Professional Journalists
Wired Ventures Ltd

Il existe entre ces organisations des liens plus étroits dans certains cas. L'EFF partage un espace d'ordinateur avec Computers and Academic Freedom, qui tient des dossiers sur l'accès à l'information dans le monde universitaire. Le "Center for Democracy and Technology" s'intéresse aux politiques qui tendent à promouvoir les libertés civiles constitutionnelles et les valeurs démocratiques dans les nouvelles technologies de l'information et de la communication. Le Centre partage une adresse à Washington D.C. avec la Citizens Internet Empowerment Coalition. Cette Coalition, qui a été créée en février 1996 dans le but exprès de combattre la CDA, se définit comme une coalition assez lâche de bibliothèques et de groupes de défense des libertés civiles, de fournisseurs de services en ligne et d'associations des industries de la presse, du livre et du disque, et plus de 56.000 membres individuels.

3. Diffusion de Contenu Pretant a Controverse sur les Reseaux

3.1 Contenu sexuel

Il ressort de tous les travaux d'analyse et de recherche faits sur Internet que les matériaux à teneur sexuelle sont les plus fréquemment recherchés. Le terme "sexe" est le plus fréquemment utilisé pour les recherches et diverses permutations des termes "pornographie", "érotique" et les titres de revues telles que *Playboy* et *Penthouse* ainsi que d'autres termes apparentés y prédominent (Markkula Center, 1977). Dès 1994, trois des groupes les plus fréquentés sur Usenet avaient un contenu sexuel (Faucette, 1995). Il est indéniable que l'on peut trouver sur Internet des textes et des images suffisamment explicites pour satisfaire toutes les formes et fantaisies imaginables en matière de curiosité sexuelle. Le fait ne devrait pas être pour surprendre. D'après une estimation récente, le chiffre d'affaires annuel de l'industrie américaine du sexe (en incluant dans cette rubrique le matériel imprimé, enregistré sur video ou autre) serait de huit milliards de dollars. Une fraction de ce chiffre correspondrait à des activités illégales, mais une bonne partie aussi à une activité parfaitement légale menée par l'intermédiaire de boutiques, éventaires de livres, cinémas et sociétés de vente par correspondance. Il convient également de noter que bien que la télévision américaine n'autorise généralement pas la diffusion de matériel à contenu sexuel explicite, celui à contenu pornographique représente un élément de plus en plus important des émissions de stations de télévision dans des pays tels que l'Allemagne et la France. Le type de matériel diffusé sur Internet n'est donc pas différent en principe de celui qui l'est dans les autres media.

Il n'en reste pas moins que le contenu sexuel est le principal problème soulevé dans la campagne visant à contrôler les communications sur Internet. Des groupes tels que la National Campaign to Combat Internet Pornography ou People against Pornography (voir liste des sites Web) se focalisent sur ce point qui était au centre des dispositions de la CDA. Ces groupes sont surtout préoccupés par la pornographie impliquant des enfants, mais les groupes féministes élèvent également de vigoureuses objections contre la pornographie considérée par eux comme un moyen de rabaisser et de contrôler les femmes. Ce thème a été développé dans les contributions présentées à la Conference on Policing the Internet tenue à Londres en février 1997, par Gerstendorfer, Hugues, Kelly, Butterworth et Muhonen (Policing the Internet, 1997).

L'argument principal avancé en faveur d'un contrôle du matériel de caractère offensant véhiculé sur Internet est que ce matériel est intrinsèquement mauvais et nocif, et particulièrement insidieux dans le cas d'Internet du fait de la manière dont il pénètre dans les foyers, les écoles et les

bibliothèques. Les partisans d'un contrôle soutiennent en outre que les utilisateurs, et notamment les enfants, peuvent tomber accidentellement sur un matériel à contenu sexuel explicite. Il ne fait certes pas de doute que les principaux moteurs de recherche permettent à ceux qui le désirent de récupérer sans difficulté le matériel à teneur sexuelle. La mesure dans laquelle les images les plus explicites, c'est-à-dire celles qui suscitent les objections les plus vigoureuses, peuvent être trouvées par l'utilisateur imprudent ou simplement curieux prêtent davantage à discussion (Faucette, 1995). En fait, cela pourrait plutôt sembler un argument commode pour ceux qui, craignant la liberté, cherchent à justifier des restrictions.

3.2 Discours de haine

Il ne fait pas de doute qu'Internet est utilisé par les personnes et organisations qui veulent s'épancher et déverser des insultes et menaces, qui souvent sont dirigées contre une race, une religion ou une orientation sexuelle particulière. Ainsi, les sentiments antisémites y sont chose commune et exprimés de façon virulente. Le matériel de l'Institute for Historical Review (IHR), organisation révisionniste qui a son siège en Californie et dont l'activité consiste à nier l'Holocauste nazi, qui a entraîné la mort de millions de Juifs et autres membres de minorités, est largement disponible sur divers sites Web. Divers groupes Usenet accordent une place importante à ce thème et l'un d'eux (alt.revisionism) s'y consacre entièrement. Des termes et expressions injurieuses sont habituellement utilisées pour parler du peuple Juif dans les échanges entre membres de ces groupes, et diverses versions de l'accusation de meurtre rituel y apparaissent, souvent sous des formes devenues familières depuis la diffusion sous forme imprimée depuis des décennies du "Protocole des Sages de Sion", qui est connu pour être un faux (Capitanchik et Whine, 1996). On peut également trouver sans difficulté d'autres formes de racisme, de misogynie, de discours anti-homosexuel, anti-religieux et autres propos injurieux sur Internet. Bien que ce soit là un problème d'intérêt général, il a davantage été soulevé par les organisations représentant les groupes victimes de ces propos que par celles faisant campagne pour un contrôle d'Internet.

3.3 Opinions politiques hétérodoxes

L'utilisation d'Internet pour inciter à la haine contre certains groupes est étroitement liée à son utilisation pour des débats et un travail d'organisation politique par des groupes marginaux et extrémistes. Les groupes néo-nazi communiquent par l'intermédiaire de serveurs BBS et de newsgroups tels que le Resistance Bulletin Board Service; aux Etats-Unis, le Liberty Lobby, organisation groupant des associations racistes, parraine le BBS Logoplex (Capitanchik et Whine, 1996). La droite religieuse américaine utilise abondamment Internet et la page d'accueil de Pat Buchanan (ancien candidat à la présidence des Etats-Unis), qui contient ses idées sur la famille, la foi et la liberté, est accessible grâce aux liens fournis par les sites Web sur le contrôle des armes manuelles, la suprématie des Blancs, l'avortement et autres grands thèmes de l'extrême-droite (Newey, 1996). Le *Euskal Herria Journal*, journal en ligne soutenant l'indépendance basque, a été accusé de favoriser l'organisation terroriste ETA (Watson, 1997). Les groupes anarchistes sont des utilisateurs enthousiastes d'Internet, dont ils aiment la structure distribuée et incontrôlée, si conforme à leurs convictions (Atton, 1996). On pourrait multiplier ainsi les exemples de contenu politique prêtant à controverse.

L'utilisation d'Internet à des fins politiques et son efficacité lors des troubles de 1996-1997 en Serbie a été vivement discutée (Bennahum, 1997). Une campagne d'action politique et de désobéissance civile menée dans le pays et baptisée du nom de "Révolution par l'Internet" s'y heurtait au contrôle rigoureux des moyens établis de communication exercé par le gouvernement Milosevic. Bien que le pays n'ait probablement compté qu'une dizaine de milliers d'utilisateurs d'Internet, d'après les estimations leur impact politique a été infiniment supérieur à leur nombre, d'autant que la plupart étaient des étudiants. Ils ont utilisé Internet de diverses manières, dont des appels aux manifestations lancées et coordonnées par l'intermédiaire d'un service appelé SezamPro, qui ne disposait que de 22 lignes téléphoniques et ne comptait que 3.000 utilisateurs. Une station de radio, Rédio B92, qui soutenait l'opposition, a été interdite, mais ses émissions ont

été reroutées par l'intermédiaire d'Internet, en utilisant RealAudio. Les compte rendus à l'étranger des événements survenus dans le pays ont été sensiblement améliorés grâce aux informations communiquées sur Internet, ce qui a permis d'exercer des pressions sur le régime.

3.4 Thèmes dangereux (drogue, armes, etc.)

Internet diffuse une partie non négligeable de l'information portant sur des sujets et des dispositifs dangereux. Les groupes de pression en faveur de la vente libre d'armes à feu et autres groupes américains du même genre affichent souvent des informations relatives aux armes. Le service de renseignements israélien Shin Bet pense que le groupe terroriste palestinien Hamas transmet des instructions cryptées à ses militants sur les attentats en préparation, y compris des cartes, des photographies, des directives, des codes, voire même des détails techniques sur le mode d'emploi des bombes par l'intermédiaire d'Internet (Borger, 1997).

On peut également trouver des informations manifestement dangereuses et parfaitement publiques sur Internet. Ainsi, un manuel de fabrication de bombes, *The big bok of mischief - the terrorists'handbook*, était disponible par l'intermédiaire du newsgroup rec.pyrotechnics (Capitanchik et Whine, 1996). Un site Web, fourni par quelqu'un utilisant le pseudonyme Candyman, offre une collection de renseignements sur des sujets tels que la drogue, le piratage des communications téléphoniques, les techniques permettant de tuer à main nue et de confectionner des bombes. Il justifie son activité, au nom de la liberté d'expression, dans les termes suivants :

> Mes actions sont celles d'un biliothécaire ou d'un archiviste. L'acte de créer, d'archiver et de publier de l'information est protégé par la Constitution des Etats-Unis, en vertu du premier amendement (Wallace et Mangan, 1996).

En dépit de telles assurances, ces exemples expliquent l'anxiété qui se fait jour.

3.5 Contenu diffamatoire

L'Internet et notamment les groupes Usenet sont connus pour la liberté avec laquelle les opinions individuelles y sont exprimées et le langage injurieux qui y est souvent employé. La pratique du "flaming" (ou envoi de torpilles) consiste à adresser aux personnes qui, pour une raison quelconque, ont offensé un tiers, des messages publics les accablant sans retenue d'injures. Ces messages peuvent aisément être diffamatoires. Bien qu'on ne compte jusqu'ici qu'un petit nombre d'actions en diffamation faisant suite à des déclarations transmises sur Internet, ces quelques cas ne permettent pas de se faire une idée du volume réel de matériel à contenu diffamatoire. Toute personne suffisamment résolue à diffuser des déclarations diffamatoires en se servant du réseau peut aisément échapper à toute poursuite en raison du caractère pratiquement omniprésent du matériel.

Ainsi, McDonalds' a intenté une action en diffamation au Royaume-Uni contre deux personnes qui avaient distribué des brochures critiquant la société. Pendant que l'action était en cours, les déclarations originelles et maints autres matériaux de caractère diffamatoire ont été postés sur un site Web intitulé McSpotlight. L'information a été maintenue sur des serveurs en Hollande, en Australie, en Nouvelle-Zélande et aux Etats-Unis qui pouvaient en assurer la diffusion plus largement encore si besoin était (Katz, 1997). Dans un autre cas, un poème de James Kirkup, condamné par les tribunaux britanniques en raison de son caractère diffamatoire et blasphématoire (il s'agissait d'une méditation homosexuelle sur la crucifixion du Christ), a paru sur un site Web aux Etats-Unis. Le Ministère public britannique a tenté d'intenter une action contre le Lesbian and Gay Christian Movement au motif que leur site Web contenait un lien avec le site américain où était diffusé le poème. Faute d'arguments fondés en droit, il a dû renoncer à son action.

3.6 Secrets officiels

De même, la capacité d'Internet à rendre publics des secrets officiels dépasse de loin celle des media qui l'ont précédé. Une fois posté, un message tend à l'être à nouveau sur d'autres groupes Usenet ou sites Web. Des "sites miroirs" dans des pays autres que celui où le message a été posté à l'origine sont fréquemment utilisés pour faire échec à toute tentative de supprimer une information donnée. Cette possibilité a été exploitée par Richard Tomlinson, un ancien membre des services secrets britanniques M16 qui souhaitait publier un ouvrage sur son activité auprès du service. Lorsque la loi britannique relative aux secrets officiels a été invoquée pour l'en empêcher, il a menacé de publier le texte sur Internet en utilisant pour se faire un ordinateur secret où le texte était conservé prêt à être diffusé (Katz, 1997).

Dans un autre cas, le rapport de la commission d'enquête du Conseil de Nottingham au Royaume-Uni sur une affaire de violence rituelle satanique intervenue à Broxtowe en 1988 n'a pas été porté à la connaissance du public. Il a toutefois été diffusé à titre non officiel sur Internet par un groupe qui jugeait important que le public en connaisse le contenu. Le Comté de Nottingham a intenté des poursuites judiciaires pour infraction au droit d'auteur en 1997, immédiatement après l'affichage du rapport sur Internet. 35 sites miroirs ayant été créés à travers le monde à la suite de cette action, le Conseil de Nottingham a été obligé de retirer son action, faute de pouvoir la faire aboutir (UK Jet Report Controversy, 1997).

3.7 Contenu touchant à la vie privée

Il convient de ne pas oublier que les réseaux contiennent aussi une masse de communications de caractère privé, sous forme de courrier électronique et sous d'autres formes telles que les conférences tenues sur réseau informatique. Une partie des controverses relatives aux messages électroniques circulant sur le réseau a trait à la liberté de préserver le domaine privé plutôt qu'à la liberté d'expression publique.

3.7.1 Surveillance

Le caractère privé des communications sur les réseaux est protégé par le droit américain et par des lois et règlements du même ordre dans quelques autres pays. Dans les pays où la primauté du droit est précaire, ces textes sont habituellement violés par les organismes chargés de l'application des lois et par les services de renseignements; dans les pays où prévaut le respect du droit, l'autorisation de recourir à des tables d'écoute peut être légalement obtenue s'il est prouvé que ce recours est nécessaire pour un motif sérieux. La National Security Agency (NSA) américaine et le GCHQ britannique sont réputés intercepter un nombre énorme de messages internationaux tous les ans sous prétexte d'empêcher l'utilisation des réseaux à des fins criminelles telles que le trafic de drogue, la pédophilie et le terrorisme. Un haut fonctionnaire de la police britannique a ainsi soutenu que

> Les personnes qui diffusent de la pornographie sur Internet y joignent des instructions sur la manière de les crypter pour se munir contre des poursuites. Il faut posséder la clé pour les déchiffrer (Elliott, 1995).

3.7.2 Cryptage

Dans la citation ci-dessus, l'auteur se référait à l'encryptage avec une clé publique, système par lequel le destinataire potentiel de messages peut générer une clé publique permettant d'encrypter les messages. Il détient lui-même une clé privée qui est le seul moyen de décoder un message encrypté au moyen de la clé publique. Le recours à ce type de méthode est une réaction naturelle au sentiment réel ou imaginaire que les organismes surveillant Internet peuvent pénétrer le secret d'un message quelconque. Le logiciel PGP (Pretty Good Privacy), qui est disponible gratuitement sur Internet, a mis l'encryptage à la portée des utilisateurs ordinaires à l'aide d'une clé publique sûre. Il est significatif de noter que le créateur de ce logiciel, Phil Zimmermann, a été arrêté et poursuivi en justice par le FBI qui craignait que ce programme ne soit à la disposition des ennemis

des Etats-Unis qui pourraient l'utiliser à des fins d'espionnage.

Pour persuader ou obliger les utilisateurs du réseau à renoncer en partie à la sécurité que leur assurerait le logiciel PGP, le Gouvernement américain leur a offert un autre moyen de cryptage, encore plus sûr. Le Congrès américain étudie actuellement une mesure intitulée Security and Freedom through Encryption ou "SAFE", qui est destinée à assurer la sécurité et la liberté au moyen de l'encryptage. Elle consisterait à imposer des contrôles sur la fabrication et l'utilisation des outils d'encryptage aux Etats-Unis. Aucun logiciel d'encryptage ne pourrait être commercialisé s'il ne contenait un dispositif permettant de décrypter immédiatement les messages de l'utilisateur à son insu (New FBI Draft, 1997) (Nouveau projet de loi FBI, 1997). Le Gouvernement britannique, avant le changement de pouvoir en mai 1997, avait publié un Document consultatif sur l'octroi de licences à des tiers dignes de confiance pour la fourniture de services d'encryptage (Licensing of Trusted Third Parties for the Provision of Encryption Services) qui, dans ses grandes lignes, était sensiblement le même (Premier rapport, 1997).

4. Le Droit et les Reseaux

Trois catégories de réponses ont été données aux problèmes posés par les contenus sujets à controverse évoqués à la section 3, à savoir d'abord la législation, puis, en deuxième et troisième lieu, les systèmes de filtrage et d'étiquetage (section 5) et les approches éthiques (section 6). A la suite de l'échec de la CDA américaine, l'attention s'est reportée sur les autres approches, ce qui ne veut pas dire que la législation ne présente pas d'importance, ni qu'on ne continue pas à rechercher des solutions fondées sur l'élaboration de nouvelles lois.

4.1 Pertinence de la législation en vigueur

L'assertion de John Perry Barlow que le cyberespace est indépendant et que les gouvernements existants n'ont aucun droit de le régir, exprime un sentiment commun, voire une crainte. ,

> Nous créons un monde où tout un chacun et partout peut exprimer sa ou ses croyances, pour singulières qu'elles soient, sans craindre d'être contraint au silence ou au conformisme. Vos notions juridiques de propriété, d'expression, d'identité, de mouvement et de contexte ne s'appliquent pas à nous. Elles sont fondées sur la matière; or il n'est pas de matière ici (Dority, 1996).

Ce propos est toutefois l'expression d'une vision romantique de l'espace virtuel. Le juriste britannique Graham Smith décrit une réalité sensiblement plus dure :

> L'idée qu'Internet n'est soumis à aucune loi procède d'un vœu pieux plutôt que d'une mûre réflexion. Les lois locales de chaque juridiction s'appliquent aux activités menées en utilisant Internet. Bien que l'application de ces lois pose de nouveaux défis, la nature panpolitique d'Internet l'expose en fait plus à tomber sous le coup des lois des diverses juridictions du globe plutôt qu'elle ne le met à l'abri de ces lois (Smith, 1996).

Il est vrai que dans nombre de cas, les juridictions compétentes peuvent être extrêmement difficiles à identifier. Tentant de remédier à cette difficulté, le Computer Misuse Act britannique (Loi sur l'usage impropre de l'informatique) de 1990 donne expressément compétence aux tribunaux britanniques pour juger de l'infraction présumée, que ce soit l'accusé ou l'ordinateur qui se soient trouvés ou l'infraction qui y ait été commise en Grande-Bretagne au moment considéré. Aucune des lois qui pourrait être invoquée dans les nombreuses juridictions où Internet est utilisé ne l'a été. Aussi les actions en justice ayant trait à des communications sur Internet n'ont-elles produit qu'une jurisprudence relativement peu abondante (Diamond et Bates, 1995). Les principaux textes sur l'applicabilité des lois en vigueur au cyberespace ont paru et d'autres sans doute sont en cours

d'élaboration (Cavazos et Morin, 1994; Smith, 1996). Qui plus est, en dépit de l'échec de la CDA, on observe un renouveau de l'activité législative et réglementaire.

4.2 Législation et systèmes réglementaires proposés

4.2.1 Etats-Unis

Le niveau d'activité législative touchant aux réseaux est tellement élevé dans les Etats américains que l'on ne saurait faire un tour d'horizon complet ici. Quelques exemples illustreront la nature de l'activité menée par les parlements de ces Etats :

> L'Alabama a adopté une loi interdisant la transmission électronique de matériel obscène aux mineurs;
>
> Le Connecticut a adopté une loi criminalisant divers aspects des communications sur Internet, y compris le type de langage injurieux utilisé lors de l'envoi de torpilles ("flaming");
>
> La Floride a adopté des amendements aux lois existantes sur la pornographie qui pourraient, éventuellement, avoir pour effet d'obliger les personnes transmettant du matériel à teneur sexuelle en ligne à indemniser les victimes de délits sexuels quand il est prouvé que l'utilisation de ce matériel était un élément du délit;
>
> Le Maryland a adopté une loi réaffirmant le caractère délictuel de la distribution de matériel obscène en ligne aux mineurs, et imputant aux opérateurs de systèmes la responsabilité des actions des utilisateurs desdits systèmes;
>
> Le New Jersey a adopté une loi sur la pornographie impliquant des enfants qui s'applique même aux images dans lesquelles il n'est pas effectivement utilisé d'enfants réels.

D'autres Etats ont également adopté des mesures présentant des traits communs avec les exemples énumérés plus haut. Jusqu'ici, il semble ne pas avoir été possible de faire appliquer les mesures adoptées par les parlements des Etats. Des recours ont en fait été introduits devant les tribunaux pour les motifs déjà invoqués contre la CDA.

4.2.2 Union européenne

L'Union européenne a réussi à ne pas perdre de vue les questions essentielles en jeu en dépit de la force des sentiments qui ont influé sur l'action des législateurs dans d'autres pays. Des préoccupations ont été exprimées au Parlement européen en avril 1997, les membres appelant à une action européenne et internationale pour éliminer la pornographie, la pédophilie et le matériel raciste d'Internet. L'Union européenne a toutefois évité jusqu'ici d'émettre sur ce sujet des directives qui auraient force de loi dans les Etats membres. Le débat intervenu en avril a débouché sur un appel aux membres de l'Union les invitant à s'accorder sur une définition juridique commune de la notion de contenu illégal, afin que ce contenu puisse faire l'objet de poursuites indépendamment du

lieu où est établi celui qui le fournit.

Dans un document de politique générale intitulé "Communication sur la diffusion de matériel

préjudiciable et illégal sur Internet" publié en février 1996, la Commission européenne a déjà exprimé ses vues sur la question (Commission européenne, 1996). Décrivant en termes succincts

la complexité de la situation juridique en Europe et les problèmes à résoudre, la Commission énonçait clairement l'importance qu'elle attache au rôle économique des fournisseurs de services Internet et réaffirmait que la responsabilité des contenus incombe aux auteurs et aux fournisseurs de contenus. Toute tentative de poursuite contre les fournisseurs de services était considérée comme portant atteinte à la capacité des utilisateurs d'accéder à d'autres contenus bénéficiant d'une protection légale. La Commission indiquait que :

> "Il peut être nécessaire de modifier ou de clarifier la législation pour venir en aide aux fournisseurs d'accès dont le métier de base est de fournir un service aux clients."

Cette conception a été développée en juillet 1997 lors d'une Conférence ministérielle européenne tenue en Allemagne, où a été publié un texte intitulé "la Déclaration de Bonn" qui énonce clairement les contrôles juridiques applicables à Internet. La Déclaration souligne l'importance d'une claire définition des responsabilités légales incombant en matière de contenu aux divers acteurs d'Internet. Elle reconnaît en particulier qu'il y a lieu de distinguer clairement entre les responsabilités des auteurs et fournisseurs de contenu et celles des prestataires de services Internet qui agissent à titre d'intermédiaires. Depuis, le Parlement européen, à sa session du 24 octobre, a recommandé de mettre à l'essai des dispositifs de filtrage et de sélection du contenu et demandé l'élaboration d'un programme informant les parents des moyens de protéger les enfants contre des contenus préjudiciables.

Depuis, divers aspects de cette politique européenne en cours d'élaboration ont été groupés dans un document exhaustif intitulé "Plan d'action visant à promouvoir une utilisation sûre d'Internet" (Commission européenne,1997). Après avoir présenté dans leurs grandes lignes les problèmes et les mesures élaborées en la matière au sein de l'Union, ce texte expose un plan comportant quatre lignes d'action, à savoir :

1. Créer un environnement sûr (en encourageant l'auto-réglementation de l'industrie);

2. Développer des systèmes de filtrage et de classification (dans le but notamment de promouvoir leur utilisation en Europe et d'encourager l'établissement de systèmes européens);

3. Encourager les actions de sensibilisation (afin de promouvoir une utilisation sûre d'Internet dans les familles, établissements scolaires, etc.);

4. Des actions de soutien (comportant notamment le suivi et l'évaluation du droit et de la procédure en cours d'élaboration).

Ce Plan d'action a été publié le 26 novembre 1997 et le Parlement européen ainsi que le Conseil des ministres devront en être saisis avant qu'il ne puisse être adopté.

Il vaut d'être noté que la Conférence ministérielle du Conseil de l'Europe tenue à Thessalonique en décembre 1997 (voir section 1) a adopté des résolutions et approuvé un Plan d'action qui, en gros, complète celui de l'Union européenne. Alors que le Plan d'action de l'UE est centré sur l'"utilisation sûre d'Internet", celui du Conseil de l'Europe vise à "la liberté d'expression et d'information". Le Plan d'action de l'Union européenne manifeste un vif intérêt pour les questions commerciales, dans la mesure notamment où il cherche à protéger les fournisseurs de services. Ce souci conduit à insister sur la sécurité de la communauté et à mettre l'accent sur la mise à l'essai de dispositifs de filtrage. Le Plan d'action de Thessalonique, davantage centré sur les moyens de promouvoir la liberté d'expression, étudie cependant la question de l'usage impropre des réseaux et des moyens éventuels de se prémunir contre ces abus. L'un et l'autre plan prônent vivement l'auto-

réglementation, la sensibilisation du public et la prise de mesures de soutien par le biais d'un développement de la législation. Bien que les deux plans abordent des questions telles que le filtrage et les lois et règlements nouveaux de points de vues assez différents, ils invitent tous deux les parties concernées à s'attacher aux mêmes domaines et ne formulent aucune proposition ou indication qui ne soit conciliables.

4.2.3 Gouvernements européens

Les gouvernements européens ont abordé la question au moyen d'une action légale et en encourageant l'auto-réglementation. Le Gouvernement allemand s'est senti obligé, en vertu des lois contre la propagation de la haine raciale et contre certains aspects de la pornographie, de poursuivre certains groupes Usenet. En décembre 1995, sur l'initiative des services du Procureur bavarois, il a ordonné à CompuServe d'empêcher l'accès à diverses sources de matériel pornographique illégal et de matériel d'incitation à la haine raciale. Pour se conformer à cette injonction, CompuServe a dû suspendre à titre temporaire les newsgroups concernés sur toute l'étendue du globe. Tous les groupes, à l'exception d'un petit nombre dont le contenu a été spécifiquement identifié comme étant illégal, ont par la suite été rétablis. CompuServe a commencé, à l'époque, à offrir à ses clients l'utilisation du logiciel de filtrage CyberPatrol pour permettre aux parents et aux établissements scolaires de contrôler l'accès au contenu en général. Le Gouvernement allemand a aussi tenté d'interdire l'accès à du matériel d'incitation à la haine diffusé par des sites Web canadiens, mais a dû y renoncer lorsqu'un certain nombre de sites miroirs aux Etats-Unis ont offert au public une solution de rechange . A la suite de cette affaire et d'autres de même nature, le Gouvernement fédéral allemand a élaboré une loi visant à réglementer les conditions régissant les services d'information et de communication. Cette loi pose le principe de la responsabilité des fournisseurs de services d'information pour ce qui est du matériel transitant par leurs services (Kuner, 1996).

Les Pays-Bas et la Grande-Bretagne, en revanche, ont favorisé l'auto-réglementation, sous une forme parfois à laquelle s'appliquerait mieux l'expression d'auto-contrôle. Aux Pays-Bas, on a jugé nécessaire de tenter de limiter la propagation de matériel pédophile et les autorités ont cherché à le faire dans le cadre des dispositions de la législation en vigueur. En janvier 1996, le NILP, une association de fournisseurs hollandais de services, a été encouragé à créer une fondation pour contrôler le matériel de caractère offensant. Cette fondation cherche à persuader les fournisseurs contrevenant à la législation de retirer le matériel illégal et signale les délinquants à la police s'ils n'obtempèrent pas (Vitiello, 1997). On retrouve plus ou moins ce même équilibre entre un constant respect de la liberté d'expression et la défense de la loi en Grande-Bretagne. L'Internet Watch Foundation (intitulée à l'origine Safety Net Foundation) a été créée en septembre 1996 par les deux principales associations de fournisseurs de services, ISPA et LINX (voir liste des sites Web pour URL). Elle poursuit activement les trois buts d'évaluation, de dénonciation du matériel de caractère offensant et de responsabilité. Le deuxième des buts ainsi poursuivis est d'encourager le public à signaler les sites offensants à la Fondation qui demandera à la police de prendre des mesures, le cas échéant. Le nombre de sites britanniques ainsi signalés a été réduit et il n'y a pas eu à ce jour de poursuite devant les tribunaux. Dans le cadre de son programme, la Fondation continue également à insister pour la mise au point de systèmes d'évaluation (Watson, 1997).

4.2.4 Pays asiatiques

L'Asie fournit des exemples de toute la gamme des politiques à l'égard d'Internet. La Thaïlande, à l'un des extrêmes, n'impose pratiquement pas de restriction et a des taux les plus élevés d'utilisation de l'Asie du Sud-Est. La Birmanie, à l'autre extrême, proscrit totalement l'accès à Internet. Les politiques restrictives sont plus communes en Asie que les approches libérales. En novembre 1997, le Vietnam a octroyé des licences à quatre organisations les autorisant à vendre des services Internet à partir d'un fournisseur unique soumis au contrôle de l'Etat. Avant que ce stade ne soit atteint, le politburo du parti avait hésité parce qu'il craignait à la fois l'introduction au Vietnam d'informations sur des "cultures et styles de vie malsains" et le vol de secrets nationaux.

Le trafic sur Internet sera contrôlé et filtré par des organismes gouvernementaux et l'échange d'informations cryptées est proscrite (Jellinek, 1997). Singapour a adopté une approche conçue de manière à concilier le but qu'elle s'est fixée d'être le pays le plus connecté de la planète et une attitude autoritaire à l'égard de toutes les formes de dissension. Depuis 1996, les fournisseurs de services doivent être dûment enregistrés, les utilisateurs sont légalement responsables du matériel qu'ils reçoivent et envoient et une bonne partie du contenu diffusé est bloqué pour des motifs d'ordre politique, moral ou religieux. Le développement d'Internet à Singapour est une sorte d'expérience de laboratoire où l'on tend à contrôler l'information tout en cherchant à obtenir les avantages d'un accès aussi large que possible aux ressources d'information (Ang et Nadarajan, 1996).

En Chine, depuis 1996, tous les utilisateurs d'Internet ont dû s'inscrire auprès de la police suivant une procédure complexe et coûteuse pour les bourses chinoises. En outre, l'unique fournisseur de services, China Internet, bloque le matériel politique et maintient un haut niveau de surveillance de l'activité d'Internet, accompagnée d'une intervention lorsque cette activité est jugée inappropriée. Le nombre de personnes possédant des ordinateurs, les ressources financières nécessaires pour accéder à Internet et la maîtrise de l'anglais nécessaire pour pouvoir l'utiliser est à l'heure actuelle réduit, si bien qu'il est relativement facile d'en contrôler l'utilisation. Ce mode de restriction de l'accès au contenu d'Internet est généralement connu sous le nom de "firewall" ou "pare-feu". L'objectif à long terme de cette politique semble être de combiner ces restrictions avec une alternative chinoise au WWW, à savoir le Chine Wide Web, qui sera un réseau commercial mais également soumis à des contrôles (Usdin, 1997; Barme et Ye, 1997).

4.3 Rôle des organismes d'application des lois

Dans certains des exemples mentionnés plus haut, la police et d'autres organismes d'application des lois jouent un rôle dans l'administration au jour le jour de l'accès à Internet. Dans d'autres cas, la police n'est impliquée que lorsqu'une plainte spécifique est déposée et portée devant les tribunaux. Ces deux approches mises à part, il est des cas où la police est appelée à jouer un rôle. Le Service des clubs et de la police des mœurs de la police métropolitaine londonienne (Clubs and Vice Unit of London's Metropolitan Police) a encouragé activement les fournisseurs de services Internet à empêcher la diffusion de matériel obscène, et notamment de matériel à contenu pédophile. En août 1996, le Service a réuni les prestataires de services en question à New Scotland Yard. D'après le Superintendant Martin Jauch, on les a informés que la police pensait qu'ils enfreignaient la loi et qu'il était temps que l'industrie s'attaque à ce problème (Policing the Internet, 1997, p.30). Cette démarche, qui fait peser une menace sur les fournisseurs de services, semble conçue pour les encourager à faire fonction de censeurs quand l'Etat lui-même ne veut pas s'arroger des pouvoirs de censure et que les tribunaux ne se sont pas prononcés sur la question de savoir si le matériel considéré est illégal ou non. D'après les informations dont on dispose, un certain nombre de newsgroups ont été supprimés par les fournisseurs de services comme suite à ces pressions, et cela bien que la majeure partie du contenu diffusé par eux soit probablement légale en Grande-Bretagne (Rodrigues, 1997).

Cette forme de contrôle est censée encourager l'auto-régulation, mais elle revient en fait à déléguer le rôle de censeur à des organisations commerciales. Même s'il était en principe raisonnable de leur demander d'assumer une telle tâche, les fournisseurs de services n'ont ni la volonté, ni une compétence juridique voulue pour s'en acquitter efficacement. Une approche légèrement différente semble avoir désormais remplacé ces formes d'interventions indirectes de la police. Il s'agit de la création de la Internet Watch Foundation, mentionnée sous 4.2.3 ci-dessus. Bien que ce soit un organisme qui s'auto-règlemente, contrôlé par un conseil d'administration composé de membres de l'industrie et de groupes éducatifs, de consommateurs et de libertaires, il reste aux yeux de certains une menace permanente et une incitation aux fournisseurs de services à pratiquer une censure. Qui plus est, l'intervention de la police semble n'avoir pas cessé. La Campaign for Internet Freedom UK (la Campagne pour la liberté d'Internet au Royaume-Uni) a vu

fermer son site par les fournisseurs Easynet en septembre 1997, apparemment à la demande de la "Branche anti-terrorisme" de la police (Watson, 1997). Ce site est désormais accessible par l'intermédiaire d'un fournisseur américain (voir la liste des URL); il convient toutefois de ne pas oublier qu'il a été fermé non pas suite à la censure directe des pouvoirs publics, ou par voie d'accord conclu en bonne et due forme au sein de l'organe auto-régulateur de l'industrie, mais sous l'effet des pressions exercées sur un fournisseur de services.

5. Filtrage et Etiquetage

5.1 Les métadonnées

Le présent chapitre s'intéresse essentiellement aux moyens de filtrage et d'étiquetage employés pour empêcher l'accès à certains types de matériel. Pour autant, ils sont aussi, de plus en plus souvent, exploités aux fins d'adjoindre des métadonnées aux informations diffusées sur l'Internet et, partant, pour en faciliter l'accès. (Dempsey et Heery, à paraître en 1998) Le World Wide Web Consortium(W3C), principal forum normatif du Web, a travaillé sur une architecture qui permettrait d'accueillir les métadonnées. Ce "Cadre de description des ressources" (*Resource Description Framework - RDF*) entend répondre aux besoins, extrêmement divers et variés, que rencontrent en la matière ceux qui créent et utilisent du matériel sur le Web. Il devrait pouvoir gérer toute une série de modèles de descriptions de ressources censés satisfaire à ces différentes exigences. Pour la "syntaxe de transfert", le RDF fera appel au XML, le langage de balisage en passe de succéder au SGML, de sorte que l'on pourra tirer parti des divers outils qui seront bientôt issus de cette technologie. La PICS – dont nous parlerons plus avant – constitue à cet égard un exemple d'activité fondée sur les métadonnées. Autre illustration importante des modèles de descriptions de ressources: le "Dublin Core", actuellement en cours d'élaboration.

Le "Dublin Core" est un ensemble de métadonnées comportant quinze éléments, qui vise à donner aux chercheurs la possibilité de débusquer des ressources électroniques sur le Web. Ses objectifs et critères sont les suivants: simplicité (davantage que les systèmes bibliothécaires comme l'AACR2), de façon à pouvoir être utilisé par des personnes non spécialisées dans les techniques de catalogage; interfonctionnement entre plusieurs disciplines ayant chacune leurs propres normes pour la description des ressources; agrément international; souplesse suffisante pour qu'il puisse être utilisé en combinaison avec des formes de description de structure plus sophistiquée (renvoyant, par exemple, au caractère confidentiel des ressources ou à leurs conditions juridiques d'exploitation au regard de la propriété intellectuelle). Ces caractéristiques sont très souvent requises lorsque l'on souhaite avoir un système de métadonnées efficace, et il serait tout à fait légitime qu'on les retrouve dans un système tel que PICS, précisément conçu pour identifier les documents qu'un utilisateur ne veut pas voir ou n'entend pas être consultés par d'autres personnes.

Les modalités d'application des métadonnées sont multiples. La plus évidente consiste à les intégrer dans les documents HTML proprement dits, à l'aide de l'étiquette <META> prévue à cet effet. La version HTML 4.0 sortie en juin 1997 autorise une forme de description plus riche que ne le permettait jusqu'alors l'étiquette <META>. Les données ainsi incluses font partie intégrante des ressources Web en question et sont reprises par ceux qui les indexent, en même temps que tous leurs autres éléments distinctifs. Autre possibilité: les organismes qui collationnent et gèrent des métadonnées non intégrées aux ressources proprement dites (comme les bibliothèques qui cataloguent leurs titres) peuvent étiqueter lesdites ressources à d'autres fins; ils pourraient notamment s'en servir pour procéder à une évaluation du contenu des ouvrages en indiquant s'il est ou non adapté à telle ou telle catégorie de lecteurs. Enfin, on peut envisager que les enregistrements de métadonnées soient gérés par un seul service qui s'assurerait de l'interfonctionnement des divers modèles descriptifs, en veillant à ce que les usagers puissent cerner avec précision la forme et le contenu des ressources qu'ils ont demandées par le biais d'un masque d'interrogation unique.

5.2 Systèmes de filtrage et de recommandation du contenu

Examinons, à présent que nous avons vu ce qu'il en était de l'étiquetage au regard des métadonnées, dans quelle mesure celles-ci peuvent contribuer, le cas échéant, à mettre en place un processus de filtrage - lequel va bien au-delà de la simple détection d'un contenu déplaisant (même si c'est là le sens qui lui est généralement conféré dans le cadre des débats sur la liberté d'expression). L'extraordinaire profusion de ressources sur l'Internet et la difficulté qu'il y a à en apprécier la pertinence et la qualité ont fait que l'on a cherché à mettre au point des systèmes de filtrage en s'aidant des outils logiciels développés à cet effet, capables par divers moyens d'identifier des ressources pour le compte de ceux qui les installent ou de ceux qui ont recours à des services d'aide au filtrage des informations. Les premiers instruments de ce genre ont souvent été dénommés "systèmes coopératifs de filtrage"(*collaborative filtering systems*); aujourd'hui, on les désigne davantage sous le vocable de "systèmes recommandeurs" (*recommender systems*), étant donné qu'il y a dans le terme "filtrage" une idée d'exclusion et que, par ailleurs, la notion de coopération n'est pas présente dans la totalité desdits systèmes. (Recommender Systems, 1997)

5.2.1 Filtrage aux fins de recommandation

Les "systèmes recommandeurs" sont comparables, dans leur philosophie, aux ouvrages qui testent et évaluent divers services et produits de consommation tels que restaurants et hôtels; ils entendent faire profiter autrui des appréciations énoncées par une ou plusieurs individus, profanes ou experts en la matière. Souvent, ils attribuent des récompenses symboliques, sous forme d'étoiles ou autres macarons, qui résument à elles seules le résultat final de ce processus. Quelle que soit la façon dont elles sont exprimées, les recommandations constituent un type de métadonnées.

Le principe des systèmes électroniques de recommandation consiste à réunir des informations recueillies auprès de personnes intéressées pour les diffuser ensuite à ceux qui souhaitent se faire conseiller. Leur originalité tient précisément au fait qu'ils rassemblent de multiples renseignements ou qu'ils sont capables d'établir les correspondances adéquates entre ces deux catégories d'usagers. Les recommandations figurent parfois de manière explicite; d'autres systèmes en revanche préfèrent travailler sur des évaluations extraites implicitement de l'exploitation des ressources par ceux qui formulent les recommandations (sur la base des références à des URL contenues dans des enregistrements Usenet, des listes de signets personnels, ou encore du temps que passent les utilisateurs sur une ressource donnée). Les recommandations peuvent être anonymes; elles peuvent aussi recourir à des pseudonymes ou renseigner clairement le nom de l'auteur. La somme des informations consignées peut résulter de votes pondérés selon des modalités déterminées (accord passé préalablement entre les personnes dont on prend l'avis, par exemple) ou selon des critères individuels. Certains systèmes combinent les évaluations et les analyses de contenu pour aboutir à une recommandation.

Les recommandations peuvent ensuite avoir de nombreuses applications; elles peuvent ainsi servir à filtrer des ressources non recommandées, à trier et dresser des listes de ressources établies selon des évaluations numériques, ou encore à présenter des évaluations en faisant apparaître à l'écran les produits et services auxquels elles se réfèrent. On aurait tendance à penser que l'usage le plus intéressant qui peut en être fait est de s'en inspirer pour s'orienter dans les sites Web; pour autant, d'aucuns affirment que des articles diffusés dans le cadre du réseau Usenet ont pu eux aussi faire l'objet d'évaluations et de recommandations fort efficaces. Divers produits et services fournissent d'ores et déjà des recommandations fondées sur une combinaison des différentes méthodes exposées ci-dessus. C'est notamment le cas pour GroupLens, Fab, Referral Web, PHOAKS et Siteseer – tous décrits et analysés par le menu dans un numéro de *Communications of the ACM.* (Recommender Systems, 1997)

5.2.2 Filtrage visant à exclure un contenu déterminé

La démonstration ayant été faite que le filtrage est simplement une application des métadonnées et un aspect seulement de la fonction de filtrage et de recommandation, la question centrale n'en reste pas moins comment traiter le contenu choquant diffusé sur les réseaux. Avant même que la Cour suprême des Etats-Unis ait rejeté la CDA en juin 1997, le filtrage apparaissait comme une sérieuse alternative à l'intervention des pouvoirs publics par voie législative. Il est maintenant au cœur des débats. Cette approche, qui a été qualifiée de "privatisation de la censure" (Lasica, 1997), peut être réalisée par deux voies principales.

> La première est l'application de logiciels de blocage au niveau des utilisateurs individuels. Divers produits tels que Cyber Patrol, Cyber Sitter, Net Nanny, Net Shepherd, Smart Filter, Surfwatch et Websense sont disponibles sur le marché. Quand ils emploient ce type de produit, les utilisateurs dépendent pour l'essentiel des méthodes et des standards choisis par le fournisseur de logiciels. Ces derniers, qui auraient pu être fondés sur un quelconque système d'évaluation, tendent à l'heure actuelle à l'être sur l'exclusion de mots-clés, de sites et de types d'images graphiques déterminés. Les utilisateurs ont une certaine latitude et peuvent ajuster le logiciel en fonction de leurs préférences particulière mais, à les en croire, cela n'est en général pas particulièrement facile ou commode.
>
> La deuxième voie consiste à se fier aux évaluations jointes au contenu par les fournisseurs de contenu et de services, ou par quelque organisme extérieur. Cet organisme peut créer lui-même l'échelle qu'il emploie aux fins d'évaluation et de codification ou utiliser une échelle-type offerte par un bureau de rating, tel que le Recreational Software Advisory Council's (RSACi) américain ou le système offert par SafeSurf. Les utilisateurs peuvent fixer leurs préférences en se servant de l'échelle offerte par le système de codification choisi.

L'outil utilisé pour se faire est la Platform for Internet Content Selection (PICS). PICS est un standard HTML qui permet de filtrer le matériel sur Internet (Resnick, 1997). Il établit un moyen constant d'exprimer les évaluations de contenu, qui peut ensuite être attaché à des ressources spécifiques suivant un des systèmes disponibles le cas échéant. L'utilisateur peut alors éliminer par filtrage tout contenu qui se révèle ne pas satisfaire aux critères de sélection qu'il a lui-même fixés. PICS n'est pas en soi un outil dirigé contre l'un ou l'autre type de matériel; il constitue une plate-forme permettant de faire fonctionner des systèmes d'évaluation de contenu à partir de toutes les sources possibles. Le but recherché est de permettre aux individus, aux familles, aux organisations, aux prestataires de services Internet, voire même aux nations, de sélectionner les systèmes d'évaluation qu'ils préfèrent et d'utiliser le PICS pour les mettre en œuvre (Resnick, 1997). C'est aussi là la position de la Commission européenne, qui a débattu des systèmes d'évaluation et de codification des contenus en 1996 et reconnu l'intérêt que présente une multiplicité de systèmes dans la mesure où elle permet aux utilisateurs de choisir celui qui reflète leurs valeurs (Commission européenne, 1996).

Les créateurs de logiciels de navigation (browsers) et de moteurs de recherche, y compris Netscape et Microsoft, se sont mis d'accord, lors de la Cinquième Conférence internationale WWW à Paris en 1996, pour munir leurs systèmes des capacités de PICS. CompuServe a également exprimé l'intention d'utiliser PICS pour évaluer et codifier son contenu à mesure qu'il passe au Web et de fournir à ses membres pour utilisation le logiciel CyberPatrol. La rapide acceptation de PICS par l'ensemble de l'industrie conduit à étudier la possibilité d'en étendre l'utilisation à la gestion de la signature de code, des droits au respect de la vie privée et des droits de propriété intellectuelle. Les pages Web de PICS (voir la liste des URL) fournissent les détails essentiels, relient le lecteur à d'autres renseignements apparentés et traitent d'un certain nombre de clés FAQ.

Le logiciel de filtrage qui utilise les évaluations présentées par PICS de manière à bloquer l'accès à certaines ressources est un élément central de l'ensemble du système. Un certain nombre de produits ont été cités ci-dessus. Un des premiers et des plus connus est SurfWatch. Il a sa propre page Web proclamant qu'il constitue une véritable alternative à la censure d'Internet en donnant aux parents et aux éducateurs la possibilité de limiter la circulation de matériel jugé indésirable localement sans restreindre les droits d'accès d'autres utilisateurs d'Internet (Internet Censorship, 1997).

Deux objections principales peuvent être opposées aux logiciels de filtrage. La première est que les méthodes précises par lesquelles les produits identifient le matériel à bloquer peuvent n'être pas pleinement transparentes. La deuxième est que ces produits sont réputés bloquer souvent un matériel de valeur en raison simplement du caractère rudimentaire de ces méthodes. Ainsi, des sites Web de pubs anglais ont été bloqués parce qu'ils faisaient mention de l'alcool; un site consacré à la propriété immobilière l'a été parce qu'il utilisait le même fournisseur d'accès à Internet qu'un site pornographique; une partie du site de la Maison Blanche américaine a été bloqué parce qu'il utilisait le terme de "couples" à propos des Clinton et des Gore (Robot as censor, 1997).

Il est apparent qu'un grand nombre de sites sont bloqués par une bonne partie des produits. Une liste du nombre des sites qui sont censés avoir été bloqués a été postée sur un site Web (encore que cette information puisse ne pas être fiable). D'après la liste, à différentes périodes d'essai, CyberPatrol aurait bloqué 13.000 sites, SurfWatch 4.500, Internet Filter 107, NetNanny 801 et CyberSitter 820 (Censorware Search Engine, 1997). L'organisation qui souscrit au principe du filtrage, Filtering Facts, a testé et (à ce jour) recommande quatre produits, Bess, CyberPatrol, SurfWatch et Websense, qui répondent à ses critères, à savoir :

1. Le mécanisme de la liste d'arrêt doit être suffisamment exact et capable de bloquer efficacement la pornographie;

2. Il doit pouvoir être ajusté de manière à ne bloquer que le contenu pornographique;

3. On doit pouvoir ajouter et retrancher des sites à la liste d'arrêt;

4. On doit pouvoir passer outre le filtre;

5. On doit pouvoir désactiver le mot-clé permettant le blocage;

6. On doit pouvoir débloquer rapidement les sites qui ont été bloqués par erreur;

7. Le vendeur doit être capable de démontrer que les affirmations touchant à la performance et aux qualités de son produit sont fondées et qu'il mène sa campagne de relations publiques de manière responsable.

5.3 Systèmes d'évaluation et d'étiquetage

L'évaluation, la codification ou l'étiquetage des ressources peuvent être faits soit par quelque bureau désigné à cette fin (une tierce partie), soit l'être à titre volontaire par les créateurs ou distributeurs de ces ressources.

5.3.1 Evaluation par un tiers

Les créateurs de PICS envisagent dans W3C l'existence de multiples services d'évaluation, correspondant à différentes nuances d'opinion couvrant toute la gamme des préférences

humaines; ce qui permettrait à chacun de choisir celui qui reflète ses propres valeurs. Il semble tout-à-fait possible que toutes sortes d'organismes ayant un point de vue religieux, moral, politique ou idéologique seront intéressés à mettre au point une échelle ou une matrice d'évaluation. C'est toutefois là une démarche foncièrement différente de celle qui consiste à concrètement examiner des ressources et décider de la cote à attribuer dans chaque cas. Il semble peu probable qu'un organisme relativement mineur, qui ne soit pas financé par l'industrie ou les pouvoirs publics, puisse faire plus qu'attribuer des cotes (ratings) à une fraction des sites les plus permanents, à profil élevé (Marshall, 1997). Les petites organisations ne disposeront ni du temps ni des fonds nécessaires pour évaluer les dizaines de milliers de sites Web, sans même parler des contributions Usenet. Les systèmes existants, qui évaluent des produits audio-visuels, n'ont à juger qu'un nombre beaucoup plus restreint de produits, tels que les longs métrages destinés à une distribution cinématographique, les cassettes vidéo destinées à la vente ou à la location et les jeux et simulations informatiques.

L'évaluation par une tierce partie est chose courante de longue date dans les industries audio-visuelles. Ainsi, le British Board of Film Certification (BBFC), précédemment connu sous le nom de British Board of Film Censors, a appliqué un système de codification (rating) aux films destinés à être projetés dans les salles de cinéma depuis des décennies. Le système n'a pas force légale, mais il constitue une norme pour les autorités locales chargées de l'octroi de licences d'exploitation qui ne décident qu'occasionnellement, dans des cas d'espèce, d'autoriser la projection d'un film non classé, ou de ne pas autoriser celle d'un film ayant une cote. L'application du système est en théorie assurée par les cinémas. Le Conseil (Board) visionne les films et leur attribue un certificat de distribution qui, pour l'essentiel, indique l'âge -12 à 15 ans- à partir duquel de jeunes spectateurs peuvent, à son avis, le voir, ou encore comporte une mention PG (Parental Guidance) quand la présence de parents est requise. Dans la pratique, les cinémas semblent considérer que le certificat s'adresse davantage aux parents qu'à eux.

La Recreational Software Advisory Council, organisme qui à l'origine s'intéressait essentiellement aux jeux informatiques et aux jeux video, a mis au point un système de codification destiné expressément à Internet. Le système, appelé RSACi (le "i" désignant Internet), évalue les ressources par rapport à une échelle allant de 0 à 4 pour quatre catégories de contenu : violence, nudité, sexe et langage. Ainsi, un produit ayant une cote 4 3 2 1 contiendra probablement de la violence délibérée et gratuite; de la nudité frontale de caractère non sexuel; des attouchements sexuels entre personnes vêtues; et l'usage d'injures assez modérées. La structure 0 1 2 3, en revanche, indiquera des conflits inoffensifs avec quelques dégâts à des objets; des attitudes suggestives, des attouchements sexuels entre personnes vêtues; et un langage dru et vulgaire, des gestes obscènes et des épithètes raciales.

5.3.2 Auto-évaluation volontaire

Si, comme on l'a indiqué plus haut, il s'avère impossible d'étendre l'évaluation par un tiers au nombre vaste et croissant de ressources Internet, un système d'auto-classement constitue une possibilité plus pratique. Dans un tel système, un site s'évalue volontairement par rapport à une série de critères du type décrit plus haut et indique ensuite la cote qu'il s'est attribuée sur son site. Le logiciel de filtrage utilisé par les particuliers pourrait être ajusté de manière à n'accepter que des sites comportant une cote et, parmi eux, seuls ceux correspondant à un certain niveau de notation. Cela suppose un déploiement d'activités d'une énorme ampleur. En octobre 1997, 45.000 sites sur les millions figurant sur Internet s'étaient auto-classés en fonction de quelques critères tels ceux fournis par RSACi (Arthur, 1997). Les implications de l'auto-évaluation pour la liberté de parole ne laissent pas elles aussi d'être énormes. Les personnes ayant des opinions sujettes à controverse risquent soit de se voir interdire de communiquer avec nombre de personnes si elles s'évaluent honnêtement par rapport aux catégories sommaires offertes par les systèmes de codification (rating), ou d'être dissuadées de s'exprimer librement et sans restriction parce qu'elles se sentent obligées d'afficher un classement neutre (ACLU, 1997).

La possibilité de lois rendant la codification (rating) obligatoire a été étudiée aux Etats-Unis et elle semble une conséquence logique d'un tel système. Il ne fait pas de doute que sans un système de pénalités pour l'étayer, l'auto-évaluation risque d'être détournée à leur profit par certains fournisseurs de services qui, délibérément, attribueront à leurs sites une cote trompeuse. Au sein de la communauté Internet, l'accord ne s'est pas fait sur la manière d'administrer un système d'auto-évaluation pour éviter l'imposition d'un système obligatoire. Elle n'a pas d'idée claire sur les moyens de faire en sorte que tous les créateurs de sites, à quelque pays ou continent qu'ils appartiennent, puissent être amenés à adhérer au système d'auto-évaluation. Or, à ne pas le faire, ils risquent de voir leurs sites exclus par filtrage par de nombreux utilisateurs pour la simple raison qu'ils ne sont pas classés.

5.4 Authentification des utilisateurs

L'ultime composante des systèmes d'évaluation et de codification est en fait un classement des utilisateurs. Le créateur d'un site Web ou le modérateur d'un newsgroup peut en restreindre l'accès à toute personne autre qu'un utilisateur dûment authentifié (ce qui équivaut en fait à faire des utilisateurs des membres d'un club ou des abonnés). Cette solution empêcherait les enfants d'accéder au matériel diffusé sur des sites qui ne sont ouverts qu'aux personnes pouvant prouver qu'elles sont adultes (Cormack, 1997). Le système pourrait être administré de l'une des quatre façons suivantes :

> Vérification de l'identité de l'utilisateur et attribution d'un mot de passe. Cette démarche obligerait les utilisateurs potentiels à fournir une preuve d'identité, de leur âge et peut-être d'autres caractéristiques personnelles avant de se voir accorder le droit d'accéder à une ressource. Les admis seraient identifiés par un mot de passe et seraient seuls à pouvoir visiter un site ou participer à un newsgroup.
>
> Filtrage du destinataire par les fournisseurs d'informations de manière, par exemple, que seuls des universitaires ou des enseignants puissent se voir accorder l'accès à un site.
>
> Validation des utilisateurs par un tiers mandaté à cet effet. Toutes les demandes d'accès feraient l'objet d'un processus de validation par un organisme extérieur avant d'être envoyées à un site.
>
> Certificats de cryptographie. Il s'agirait de preuves d'identité électroniques présentées aux fournisseurs de services à leur demande. Cette solution est considérée comme malcommode parce que les certificats doivent être installés sur un logiciel de navigation (browser) avant d'être utilisés et retirés ensuite.

Bien que la question de l'authentification touche essentiellement au respect du domaine privé, on peut voir de ce qui précède qu'elle a logiquement place dans un débat sur le filtrage de l'accès aux ressources. En faisant peser la responsabilité de l'accès au site sur les fournisseurs d'informations, elle résout certains des problèmes inhérents aux autres approches de la question. Elle revient en fait à confier aux fournisseurs le soin de contrôler l'accès à leurs ressources de manière analogue à celle imposée aux propriétaires des "sex shops" britanniques, qui sont tenus d'en restreindre l'accès aux personnes âgées de plus de 18 ans, et à ceux des bars de nombreux Etats américains qui doivent vérifier les permis de conduire pour s'assurer que leurs clients ont bien plus de 21 ans.

Il existe des sites Web, tels que Adult Check, Adult Pass, Adult Sights, qui offrent des services de vérification de l'identité. Adult Check prétend que près de 3000 sites Web qui ont un contenu "adulte" recourent à ses services. Les personnes qui souhaitent voir confirmer qu'elles sont des adultes aux fins d'accès à un site donnent au site leur nom, adresse et numéro de carte de crédit

et, si elles sont acceptées, se voient attribuer un mot de passe moyennant 12,95 dollars E.U. par an. Même si les procédures utilisées par les responsables du site suffisent à garantir que l'information obtenue avant l'attribution du mot de passe est exacte et consistante, il est facile à un enfant de donner les renseignements exacts correspondant à un adulte et d'utiliser ensuite cette fausse identité. Il existe également des éléments tendant à prouver que l'information détenue par ces services n'est pas sûre et qu'il n'existe pas de moyen, dans le cadre du système, d'empêcher une personne d'utiliser l'identité d'une autre (Markkula Center, 1997).

5.5 Résultats des recherches

Une bonne partie des observations relatives au filtrage sont centrées sur ses imperfections, évidentes ou prétendues. Les adversaires du système avancent régulièrement, comme argument principal à l'encontre de ce procédé, la manière imparfaite dont le filtre opère, en se basant habituellement sur des mises à l'essai assez superficielles. Ainsi, un essai de portée réduite a été fait au Centre Markkula à l'Université de Santa Clara pour voir si les filtres bloqueraient les sites à contenu sexuel explicite, les sites consacrés à l'éducation sexuelle, ceux consacrés aux rapports sexuels sans risque, les sites contenant un matériel factuel sur le lesbianisme, les sites analogues comportant des informations sur les homosexuels. Il a été constaté que tous les filtres essayés bloquaient tous les sites de la première catégorie, permettaient d'accéder aux sites d'éducation sexuelle, produisaient des résultats mitigés pour ce qui est des sites sur les rapports sexuels sans risque, laissaient passer le matériel sur le lesbianisme, mais bloquaient les sites d'homosexuels. Ces résultats intéressants mais peu concluants reflètent assez fidèlement ceux dont il est fait état dans les débats sur le sujet. A ce jour, il n'a été effectué que peu de recherches indépendantes étudiant en profondeur l'efficacité du filtrage d'Internet et ses implications pour l'utilisation d'Internet en tant que ressource d'information.

L'Internet Filter Assessment Project (TIFAP) constitue une exception à cet égard dans la mesure où, malgré des imperfections dûment reconnues sur un certain nombre de points, il fournit maints renseignements intéressants sur les effets des systèmes de filtrage sur la personne cherchant des informations. Au cours de ce petit projet, ont été mis à l'essai 18 exemples de logiciels de filtrage, en étudiant la façon dont ils bloquaient le matériel au moyen de mots-clés identifiés à partir de leur contenu, de noms de sites déterminés (ce que TIFAP appelle une "désélection intellectuelle"), et de protocoles (tous les groupes Usenet, IRC ou Telnet). Le blocage au niveau des sites s'est révélé insatisfaisant parce que de nouveaux sites voient constamment le jour et qu'ils restent à l'entière disposition du public jusqu'à ce qu'il apparaisse que leur contenu est problématique. Le blocage au moyen des protocoles s'est révélé être extrêmement grossier et inclure une quantité exagérée de matériel. Le blocage à l'aide de mots-clés a été testé en essayant d'obtenir d'Internet des réponses à plus de 100 questions du type de celles habituellement posées dans les bibliothèques, tandis que le logiciel fonctionnait. Ces questions visaient à étudier la manière dont le logiciel se comportait à l'égard des 11 domaines suivants :

1. le sexe et la pornographie,
2. l'anatomie,
3. les drogues, l'alcool et le tabac,
4. les questions touchant à l'homosexualité,
5. la délinquance (y compris la pédophilie et la pornographie impliquant des enfants),
6. le langage obscène ou à contenu racial,
7. la culture et la religion,

8. les questions féminines,
9. le jeu,
10. les groupes d'incitation à la haine et l'intolérance,
11. la politique.

Les questions étaient conçues de manière à approcher ces domaines directement (en demandant de la documentation sur des sujets prêtant à controverse) et indirectement (en demandant "par inadvertance" des termes et expressions susceptibles d'être bloqués parce que à double sens (par exemple des recettes de blanc de poulet, l'équivalent anglais "chicken breast" comprenant le mot "breast") ou des instructions sur la culture de graines de colza, le mot "rape" désignant le colza étant le même que celui de viol en anglais). Les chercheurs ont constaté que les filtres bloquaient l'information nécessaire pour répondre aux questions dans plus de 35 pour cent des cas, réagissant aux mots-clés et bloquant des sites contenant la documentation requise sur des sujets tels que la sexualité sans risque, les organisations pour adolescents homosexuels et les arguments pour et contre la légalisation de la drogue. Ces résultats signifient que tous les filtres excèdent, dans une certaine mesure, le rôle pour lequel ils ont été conçus, à savoir empêcher l'accès par inadvertance ou délibéré à un matériel offensant ou indécent. Ils font en fait obstacle à la recherche d'une information parfaitement légitime et utile.

5.6 Le débat

Le débat sur le filtrage s'est poursuivi avec une grande intensité depuis que le rejet de la CDA a semblé probable. Comme en témoigne le nombre des sites Web représentant des organisations intéressées totalement ou partiellement, cette question suscite un vaste intérêt et une nette polarisation d'opinion. Le partage semble se faire entre les tenants d'une totale liberté d'expression d'un côté et, de l'autre, tout un éventail de groupes comprenant aussi bien des partisans de la censure que des opposants favorables à la mise en place de moyens accrus d'éviter la diffusion de matériel offensant. Le débat tourne en bonne partie sur l'utilisation des logiciels de filtrage dans les bibliothèques pour le compte des utilisateurs plutôt que sur leur utilisation par les familles dans les foyers.

L'ACLU et l'American Library Association ne se sont pas bornés à être les instigateurs et les animateurs de la campagne contre la CDA, mais s'opposent tous deux vivement au filtrage. Leur position repose sur le principe du respect du droit des individus et des familles à décider par eux-mêmes ce qu'ils souhaitent voir et sur la conviction que le filtrage porte atteinte à ce droit. On peut également trouver des arguments contre le filtrage sur les sites Web de Censorware Search Engine, Cyber-Rights et Cyber Liberties (RU), Ethical Spectacle, MIT SAFE et Peace Fire (voir la liste des sites Web pour URL). Ont également paru un certain nombre de compte rendus dans la presse et d'articles de revues appelant l'attention sur les incidences possibles du filtrage, dont ceux énumérés ci-après constituent une sélection (Kleiner, 1997; Lasica, 1997; Wallich,1997; Watson, 1997; Winner, 1997). Le rapport de Cyber-Rights et de Cyber-Liberties (RU) intitulé "Who watches the watchmen : Internet content rating systems and privatized censorship" ("Qui garde les gardiens : systèmes d'évaluation des contenus d'Internet et censure privatisée") (Cyber-Rights, 1997) constitue une étude exhaustive des questions qui se posent et de la technologie existante vues sous cet angle.

Ce sont surtout les responsables des sites, notamment Paul Resnick des Laboratoires AT&T, Président du Groupe de travail PICS de W3C, qui se prononcent énergiquement en faveur du filtrage pour des raisons d'ordre essentiellement technique (Resnick et Miller, 1996). Le principe du filtrage est appuyé vivement par Filtering Facts, qui s'intéresse surtout à l'utilisation des filtres dans les bibliothèques. Ses critères pour la sélection des logiciels de filtrage, qui ont été énumérés à la section 6.2.2, ont été élaborés en grande partie à l'intention des bibliothèques. David Burt de

Filtering Facts a répondu à certains arguments avancés contre le filtrage, y compris ceux fondés sur les anomalies dûment reconnues qui résultent du fonctionnement des produits actuellement disponibles (Burt, 1997). Parmi les sites appuyant le filtrage figurent encore Family Friendly Libraries, Enough is Enough, Library Watch, National Coalition for the Protection of Children and Families (voir la liste des sites Web pour URL). La forme que peut revêtir le débat entre bibliothécaires ayant opté pour le filtrage et ceux qui n'en veulent pas est abondamment illustrée par le débat entre les bibliothèques d'Austin (Texas) et de Monroe County (Michigan) qui a été publié par Branch et Conable (1997).

6. Approches Ethiques

La tendance assez répandue que l'on a de décrire Internet comme un organisme anarchique ne tient pas compte de l'immense volonté qu'ont nombre d'utilisateurs de promouvoir une utilisation raisonnable. Elle revient aussi à méconnaître l'effort qu'ont fait les fournisseurs publics d'accès, les prestataires de services et, au moins autant qu'eux, les biliothécaires pour mettre au point des mesures permettant aux communautés et aux familles d'avoir accès au contenu d'Internet à des fins déterminées et dans le respect des utilisateurs. Pour ceux qui rejettent l'idée d'une réglementation en bonne et due forme et le recours à la technologie pour restreindre l'accès au contenu d'Internet, les efforts faits pour étudier des approches éthiques constituent le meilleur moyen de convaincre le public et les dirigeants politiques qu'Internet est en fait une force pour le bien, plutôt qu'une menace pour la structure de la société.

6.1 Netiquette et les formes admissibles d'utilisation

6.1.1 Netiquette

Inonder les newsgroups, les mailing lists ou autres éléments du réseau de messages destinés à faire connaître les vues d'un individu ou à faire de la publicité pour un produit ou un service (spamming) ou pour envoyer des messages injurieux et se livrer à une guerre épistolaire (flaming) sont un aspect seulement de l'utilisation du réseau. Face à cette tendance, le sentiment se fait jour que de bonnes manières sont requises pour rendre l'utilisation du réseau commode et exempte de menaces pour tous. Les codes de conduite destinés aux utilisateurs du réseau sont connus sous le nom de "netiquette" (parfois aussi de "nettiquette"). Leur contenu, pour la plupart, est peu remarquable dans la mesure où il consiste en une réaffirmation des éléments composant un comportement correct et courtois, de rigueur dans toute société. Un des codes de pratique les plus répandus constituant la netiquette (Shea, 1994) est articulé autour des 10 règles suivantes :

1. Ne jamais oublier l'humain en toute chose;
2. Observer les mêmes règles de conduite en ligne que dans la vie réelle;
3. Connaître sa place dans le cyberespace;
4. Respecter le temps et la bande passante d'autrui;
5. Se présenter sous son meilleur jour;
6. Echanger les connaissances spécialisées;
7. Aider à ne pas laisser les guerres d'insultes (flame wars) dégénérer;
8. Respecter l'intimité d'autrui;
9. Ne pas abuser de son pouvoir;

10. Etre indulgent à l'égard des erreurs d'autrui.

Le fait que ces listes sont plus qu'un discours pieux de la part de quelques utilisateurs inquiets est attesté par le nombre de messages indignés qui apparaissent en réaction à ce que l'on considère être des violations flagrantes de la conduite à tenir sur le réseau. Il n'est également pas difficile de trouver des newsgroups où se tiennent des discussions poussées sur le bien ou le mal fondé de quelques prétendues infractions du code. Le souci de l'éthique n'est toutefois pas la note dominante dans les échanges sur Internet. Comme le fait observer un commentateur :

> La nature fragmentée d'Internet a empêché l'élaboration d'une véritable doctrine éthique. Les utilisateurs de longue date observent peut-être des règles tacites, mais ils se trouvent très rapidement dilués par l'énorme afflux d'utilisateurs nouveaux et inexpérimentés (Langford, 1995).

Dans ces conditions, il est manifestement besoin de règles élaborées avec plus de soin et largement acceptées, et non pas simplement de la bonne volonté assez vague qui s'exprime dans netiquette.

6.1.2 Formes admissibles d'utilisation

Alors que netiquette est pour l'essentiel un guide de conduite individuelle, on entend par règles acceptables d'utilisation les directives et prescriptions émises par les organisations au sujet de la conduite des usagers au sein de leurs systèmes. L'effort investi dans l'élaboration de ces règles est considérable et, prises ensemble, elles font apparaître un très large consensus en ce qui concerne l'utilisation raisonnable d'Internet. Si tous les utilisateurs se conformaient aux principes inspirant ces règles, les problèmes que présente apparemment le contenu d'Internet disparaîtraient pratiquement d'un jour à l'autre. Il existe de multiples règles de ce genre. On peut en trouver sur Internet de nombreux exemples émanant d'établissements scolaires. Nombre d'entre eux sont affichés sur le site Web de Robbinsdale, Minnesota, School District (voir la liste des URL). Les auteurs de documents de ce genre peuvent obtenir des conseils et un de ces conseillers groupe les problèmes en jeu sous les rubriques suivantes :

1. Liberté intellectuelle;
2. Propriété - intellectuelle et "réelle";
3. Limites des ressources;
4. Dénégation plausible (rubrique aussi intitulée "clauses de sauvegarde", déni de responsabilité) (Wolf, 1994).

D'autres institutions universitaires, serveurs et réseaux ont également une politique propre. Le Joint Academic Network (JANET) du Royaume-Uni a défini en avril 1995 une politique qui vaut pour tous les utilisateurs universitaires britanniques. Dans sa neuvième clause, elle définit clairement ce qui est à son sens une forme d'utilisation inadmissible :

> 9.1 la création ou la transmission (à des fins autres qu'une recherche dûment supervisée et légale) de toute image, donnée ou autre matériel offensant, obscène ou indécent, ou de toute donnée susceptible d'être résolue en image ou matériel obscène ou indécent;
>
> 9.2 la création ou la transmission de matériel conçu pour ennuyer, incommoder ou susciter une inquiétude inutile, ou de nature à produire ces sentiments;
>
> 9.3 la création ou la transmission de matériels diffamatoires;

9.4 la transmission de matériels enfreignant le droit d'auteur d'un tiers;

9.5 la transmission de matériel commercial ou publicitaire non sollicité à d'autres organisations d'utilisateurs ou à des organisations liées à d'autres réseaux;

9.6 l'accès non autorisé délibéré à des équipements ou à des services accessibles par l'intermédiaire de JANET;

9.7 des activités délibérées présentant l'une quelconque des caractéristiques suivantes :

gaspiller les efforts du personnel ou les ressources des réseaux, et notamment du temps sur des systèmes finaux accessibles par l'intermédiaire de JANET et les efforts du personnel affecté à l'appui de ces systèmes;

brouiller ou détruire les données d'autres utilisateurs;

violer l'intimité de tiers;

perturber le travail d'autrui;

utiliser JANET de manière empêchant d'autres utilisateurs d'avoir recours à ses services (par exemple, surcharge délibérée ou imprudente de connections d'accès ou de matériel de commutation;

continuer à utiliser un élément de logiciel ou de matériel du réseau après qu'UKERNA ait demandé qu'on cesse de l'utiliser parce qu'il perturbe le bon fonctionnement de JANET;

tout autre usage impropre de JANET ou des ressources du réseau, tel que l'introduction de virus.

Les fournisseurs de services Internet ont eux aussi défini une politique que l'on peut trouver en ligne (voir la liste des URL du site "Acceptable Use Policies" (Règles acceptables d'utilisation). America Online (AOL) a pour politique de définir les principes qui le régissent en ajoutant d'utiles explications sur les divers éléments composant ses services : messagerie électronique, Usenet et discussions (chat) (voir la liste pour URL). Le problème tient au fait que les fournisseurs d'accès du secteur public (établissements scolaires, universités, bibliothèques, services publics) sont en mesure de faire appliquer les règles qu'ils édictent par leurs membres et employés, tandis qu'il est beaucoup plus difficile aux fournisseurs commerciaux de limiter les activités des clients qui rémunèrent leurs services.

6.1.3 Codes de pratique de l'industrie

L'élaboration de codes pour toute l'industrie est également en cours. Ces codes définiraient de manière plus complète les obligations des divers types de fournisseurs. Une organisation intitulée Internet Content Register (Registre du contenu d'Internet) a, avec la collaboration de l'Association britannique des consommateurs, élaboré un Code de pratique Internet (ICOP) (Internet Code, 1997) qui couvre :

1. La nature du public et les moyens de veiller à ce que l'information qui

lui est transmise soit appropriée;

2. La publicité, et les normes qui devraient être appliquées;
3. Les contrats;
4. Le droit d'auteur et la propriété de l'information;
5. L'information et la qualité de cette information (y compris la décence);
6. Les Applets, les séquences-types de browser et l'utilisation du CGI;
7. Les messageries électroniques et les nouvelles, et notamment les communications non sollicitées.

L'organisation offre de délivrer des certificats aux fournisseurs de services qui s'engagent à opérer conformément au Code de pratique Internet (ICOP). Ce Code sera étayé par un service de suivi et d'investigation des plaintes. Un accord, comportant une claire définition de leurs responsabilités mutuelles, pourra être signé entre l'Internet Content Register et les fournisseurs de services. Que cette initiative vienne à être couronnée de succès ou non, elle offre des idées sur la forme que pourrait revêtir l'auto-réglementation de l'industrie par le biais de codes de pratique.

6.2 Politiques des bibliothèques

Un des thèmes que l'on retrouve constamment dans les documents portant sur l'auto-régulation d'Internet est un hommage à l'utilité des mesures prises par les bibliothèques pour régler le problème. Ainsi, Computers and Academic Freedom publient un article étudiant la manière dont les principes élaborés par les bibliothèques pourraient être appliqués à l'utilisation publique et universitaire des ordinateurs (Kadie, 1994). Les principes analysés sont essentiellement tirés de documents établis par diverses bibliothèques et par l'American Library Association (ALA). D'autres organisations importantes groupant des bibliothèques n'ont pas de position clairement articulée. La Fédération internationale des associations de bibliothèques (IFLA) a adopté une résolution acceptant le rapport d'un Comité sur la liberté d'accès à l'information et la liberté d'expression (CAIFE) à sa réunion de Copenhague de septembre 1997. Les recommandations formulées dans ce document étaient toutefois extrêmement générales et ne disaient rien de précis sur les réseaux. Par la suite cependant, un Comité permanent de l'IFLA a été créé pour traiter de ce problème. La Library Association britannique, dont les membres et le secrétariat suivent et analysent les questions touchant à la liberté d'expression sur les réseaux, n'a elle aussi que des documents de politique générale, tels que la Déclaration relative à la censure (qui a été révisée pour la dernière fois en 1989).

L'ALA, en revanche, a toujours pris fermement position en faveur de la liberté d'expression et admet qu'il lui appartient donc de montrer comment on peut utiliser cette liberté sans danger et de manière responsable. L'essentiel de la position de l'ALA est énoncé dans le "Library Bill of Rights", révisé en 1980, qui a été adopté en même temps que les résolutions relatives à "L'accès à l'information électronique" de 1996 et l'"Utilisation de logiciels de filtrage dans les bibliothèques" de juillet 1997 (voir le site Web ALA, dans la liste URL). Ces documents témoignent d'une position extrêmement ferme en ce qui concerne les libertés constitutionnelles américaines, qui sont considérées comme s'appliquant à tous, indépendamment de leur âge (sous réserve seulement d'autorisations parentales pour ce qui est des enfants). L'Internet est considéré comme assimilable à une bibliothèque et les principes régissant les bibliothèques sont par conséquent réputés s'étendre naturellement à l'accès à Internet dans les locaux occupés par des bibliothèques (Markkula Center, 1997).

Le filtrage est accepté par certains bibliothécaires, qui y voient une analogie de plus avec la sélection des livres et l'accès, normal pour une raison ou une autre, à certaines parties des

collections de bibliothèque, par l'intermédiaire d'un bibliothécaire. La grossièreté des filtres disponibles a toutefois posé de réels problèmes à nombre de bibliothécaires qui cherchaient à concilier leur foi profonde dans la liberté de l'information et le recours à des filtres (Mason, 1997). Lorsqu'elles s'en tiennent à une politique favorable à une liberté d'accès sans entrave, les bibliothèques subissent la pression d'organisations telles que Enough is Enough. Cette organisation fournit un jeu de questions et d'arguments à ceux qui souhaitent encourager les bibliothèques à utiliser des filtres pour protéger les enfants contre un contenu offensif (Safeguards, 1997).

6.3 Responsabilité personnelle et parentale

Il faut enfin compter les organisations qui soulignent qu'en dernière instance les individus doivent assumer personnellement la responsabilité du matériel qu'ils choisissent de consulter sur Internet. Ils doivent en outre accepter qu'ils sont responsables du contenu auxquels leurs enfants sont exposés. Cet argument appelle l'attention sur des règles de responsabilité personnelle et familiale et sur les moyens d'opérer une sélection positive où ne sera retenu que le matériel de haute qualité. C'est là l'argument qui sous-tend l'orientation d'une organisation intitulée "Children's Partnership", qui à son tour collabore avec d'autres organisations américaines, la National PFA (Association nationale de parents d'élèves) et la National Urban League. Children's Partnership met plus l'accent sur la participation des parents, la qualité de l'enseignement des rudiments de l'informatique dans les établissements scolaires et l'égalité d'accès dans la société de l'information, que sur les aspects négatifs de l'utilisation d'Internet (Parents, 1996).

En ce qui concerne la participation des parents, il existe des jeux proposant des règles à l'intention des parents et des enfants. Le National Center for Missing and Exploited Children (voir URL pour la sécurité des enfants sur l'autoroute de l'information) propose aux parents les sept directives suivantes :

> ne jamais donner d'information permettant d'identifier l'Internaute;
>
> apprendre à connaître les services utilisés par l'enfant;
>
> ne jamais permettre à un enfant d'organiser une réunion face à face avec un autre utilisateur;
>
> ne jamais réagir aux articles de nature offensante;
>
> se rappeler que les personnes en ligne peuvent ne pas être ce qu'elles semblent ou prétendent être;
>
> se rappeler que tout ce que l'on lit en ligne n'est pas nécessairement vrai;
>
> fixer des règles et des directives raisonnables aux enfants.

Pippin, une organisation qui cherche à promouvoir une utilisation positive d'Internet, a formulé un jeu analogue de règles que les parents peuvent encourager leurs enfants à suivre :

> ne donnez pas votre nom de famille, votre adresse ou votre numéro de téléphone;
>
> ne dissimulez pas votre âge;
>
> rappelez-vous que les gens ne sont pas nécessairement ce qu'ils prétendent être;
>
> n'ouvrez pas les "annexes" émanant de personnes que vous ne connaissez

pas;

si vous avez peur, dites-le à vos parents;

si vous vous sentez mal à l'aise, sauvegardez le message et quittez;

n'allez pas rencontrer seul une personne dont vous avez fait la connaissance en ligne.

L'ALA, de même, dit aux parents que la meilleure manière d'assurer la sécurité de leurs enfants sur Internet est d'y être présents avec eux et de convenir avec eux de règles (Librarian's Guide, 1997). A l'instar de plusieurs autres organisations, elle ajoute à ce conseil une active recommandation indiquant les sites qui devraient, à son avis, amuser et informer les enfants. Une première liste de 50 sites a été élargie et on en compte actuellement plus de 700, choisis suivant les critères affichés sur le site (Great Sites, 1997).

7. Conclusions de la Premiere Partie

On est à bon droit fondé à se préoccuper de la nature de certains des matériels disponibles sur Internet. Ces préoccupations ne diffèrent toutefois de celles que peuvent susciter les matériels imprimés, radiodiffusés ou télévisés que par l'absence relative de réglementation de l'information qui pénètre dans les foyers, les bibliothèques et les milieux scolaires ou universitaires par le biais des réseaux. L'inquiétude des pouvoirs publics et des organismes officiels s'est exprimée sous la forme de trois approches au problème : les solutions législatives, le filtrage et le blocage du contenu et l'auto-réglementation d'Internet et de son utilisation.

Les solutions reposant sur une nouvelle législation sont généralement inadéquates pour diverses raisons :

elles tendent à enfreindre le principe fondamental de la liberté d'expression;

elles sont difficiles à appliquer parce qu'Internet opère dans trop de juridictions différentes;

la nature du réseau est telle qu'elle fournit des moyens techniques d'éviter les contrôles, tels que les sites-miroirs;

l'environnement des réseaux change trop rapidement pour que la législation puisse suivre.

Le filtrage et le blocage ne sont pas des solutions qui recueillent une adhésion totale pour des raisons à la fois de principe et de pratique. Les objections de principe sont plus ou moins insurmontables. Des éléments mineurs de filtrage devraient toutefois être utilisés par les parents, et par ceux ayant des responsabilités parentales, sans s'écarter des normes sociales qui limitent l'accès des enfants à d'autres formes de matériels. L'utilisation du filtrage et du blocage doit être l'effet d'un libre choix et être opérée, si possible, avec le consentement des intéressés. Leur imposition sans ce consentement ou sans qu'une objection puisse être exprimée est, à n'en pas douter, aussi inadmissible que toute autre forme de censure. C'est certes là un compromis, mais les compromis font normalement partie du tissu de toute vie.

Il est actuellement difficile d'arriver à des compromis en matière de filtrage et de blocage, parce que les effets du processus de filtrage sont assez grossiers et que le matériel bloqué et les raisons du blocage ne sont pas transparents. Pour que le filtrage et le blocage puissent être acceptés par tous les partisans de la liberté d'expression, il faudra beaucoup améliorer la technologie et disposer de systèmes de haute qualité pour l'évaluation et l'étiquetage du contenu. PICS constitue déjà une plate-forme acceptable d'évaluation des métadonnées qui, en dépit de l'hostilité

manifestée à son égard par les partisans d'une totale liberté d'expression, n'agit pas automatiquement comme un instrument de censure.

C'est plutôt le système d'évaluation auquel PICS devrait servir de support qui pourrait constituer un moyen de censure. Les systèmes de codification supposent une série valable de normes et les normes existantes d'évaluation qui, pour l'essentiel, ont été conçues pour du matériel à contenu récréatif ne sont pas adéquates. Idéalement, c'est aux fournisseurs de contenu qu'il incombe de joindre des métadonnées d'évaluation au contenu, mais des systèmes efficaces d'évaluation par des tiers sont également acceptables. Il convient de créer des organismes d'évaluation et de codification convenablement financés bénéficiant de la confiance de l'industrie et des utilisateurs d'Internet, si l'on entend poursuivre sérieusement cette approche.

L'auto-réglementation des réseaux et de leur contenu au moyen de codes de pratique du contenu et de codes à l'usage des fournisseurs de services et des utilisateurs est, en principe et pour des raisons techniques, le moyen le meilleur de donner confiance au public dans la valeur des réseaux en tant que moyen de communication. Ces codes devront être améliorés et encouragés si l'on veut qu'ils puissent être efficacement appliqués par les groupes auxquels s'adressent leurs dispositions. Auto-réglementation ne devant pas nécessairement dire auto-contrôle, il faut définir clairement les champs de compétence respectifs des organismes d'application des lois et des organismes réglementaires. L'auto-réglementation doit enfin être étayée par des programmes propres à encourager une utilisation responsable et informée des réseaux, du type de ceux fournis par l'ALA et d'autres organisations.

Deuxieme Partie:
Application de la liberté d’expression dans les points d’accès publics

1. Introduction

L’accès aux réseaux de communication, en particulier à l’Internet, constitue un sujet de préoccupation pour le simple citoyen et pour les gouvernements, mais aussi pour les personnes responsables de la gestion d’un point d’accès public à ces réseaux. De toute évidence, il appartient à chaque individu de décider lui-même de ce qu’il souhaite consulter et lire. Par ailleurs, les gouvernements démocratiques ont la responsabilité de veiller à ce que l’information soit conforme aux exigences de la loi, en particulier sur des questions telles que la sécurité nationale, l’ordre public, la prévention de la criminalité et la protection de la santé et de la morale. Mais s’agissant des points d’accès publics, les responsables ont pour mission essentielle de donner à leurs " clients " le plus de liberté possible dans la recherche de connaissances. Ce rôle est difficile à remplir pour deux raisons. La première tient à la présence sur les réseaux de contenus illégaux dans le pays à partir desquels on y accède (mais pas nécessairement dans leurs pays d’origine) ou à des contenus qui, s’ils ne sont pas illégaux, sont généralement réputés préjudiciables. La seconde est liée au fait que ces mêmes réseaux sont très souvent utilisés par des jeunes encore sous la tutelle légale de leurs parents. De l’avis de beaucoup, certaines catégories de contenus représentent un danger potentiel pour ces jeunes internautes. Le responsable d’un point d’accès public doit trouver les moyens d’affronter ce dilemme entre le principe fondamental en vertu duquel il est donné au public un accès aux réseaux, et les inquiétudes que font naître dans l’esprit du public la nature de certains des contenus mis à la disposition de ce dernier par l’intermédiaire desdits réseaux.

Il suffit, pour se convaincre qu’il s’agit-là d’un souci bien réel, et non d’un phénomène créé par les médias pour attirer lecteurs, auditeurs et téléspectateurs, de se pencher sur les résultats de quelques sondages d’opinion menés récemment en Grande-Bretagne. Dans le cadre de la

première de ces enquêtes, intitulée *Which? Online* et réalisée par le cabinet d'études de marché MORI (*Annual Internet Survey*, 1998), cinquante-huit pour cent des personnes interrogées se ont déclaré estimer que l'Internet menaçait la moralité nationale en donnant à tout au chacun la possibilité d'accéder à des contenus à caractère pornographique et autres sites illégaux, treize pour cent seulement ayant indiqué n'avoir aucune hésitation à laisser leurs enfants " surfer " sur l'Internet sans aucune surveillance. Par ailleurs, un autre sondage, mené également par MORI sur l'attitude des enfants, a montré que les parents ont peut-être raison d'avoir parfois le sentiment de ne pas être entièrement maîtres de la situation dans ce domaine, puisque 30 % des enfants interrogé ont affirmé en savoir davantage sur l'Internet que leurs professeurs et instituteurs (*Children's attitudes*, 1998). Enfin, un sondage réalisé peu de temps auparavant pour connaître le sentiment des enseignants sur les " nouvelles technologies de divertissement " a révélé que ces derniers étaient remplis d'inquiétude. Les trois quarts des personnes interrogées environ se sont déclarées convaincues qu'il existait une relation de cause à effet entre l'usage fréquent de l'ordinateur à des fins de divertissement et diverses formes de problèmes d'apprentissage (Miller, 1994). Ces préoccupations sont peut-être plus ou moins fondées, mais il n'en reste pas moins qu'elles contribuent à créer un climat général dont les responsables doivent tenir compte dans leur gestion des points d'accès publics aux réseaux.

Le présent rapport reprend les méthodes du premier volume. Il porte plus particulièrement sur la question des points d'accès publics aux réseaux, à partir de l'étude du premier volume, mais aussi d'un échantillon récent d'informations et d'opinions recueillies au cours des six premiers mois de l'année 1998. Le but visé consiste ici à contribuer à la préparation, par le Conseil de l'Europe, de Recommandations qui aideront les gouvernements à envisager une action législative ou autre susceptible de retentir sur l'administration des points d'accès publics et d'avoir des conséquences également pour ceux qui sont directement responsables de la gestion au quotidien de ces endroits.

2. Les Points d'Accès Publics aux Reseaux

Bien que les foyers européens soient nombreux à posséder un ordinateur à la maison (38 % en Grande-Bretagne, un peu plus encore pour les ménages ayant des enfants scolarisés) ("*Nation Divided*", 1997), une grande majorité de la population reste tributaire des points d'accès publics pour accéder aux réseaux de communications et à l'information qu'ils véhiculent. Cet accès public est inégal selon les pays, et même au sein d'une même nation. Ce sont les établissements d'enseignement qui offrent le plus grand nombre de points d'accès aux réseaux. Viennent ensuite les bibliothèques et autres centres d'information, les institutions culturelles et les bornes d'information. Le nombre de points d'accès publics en dehors du secteur de l'éducation varie considérablement d'un organisme à l'autre et selon les catégories d'établissements. L'importance de la notion d'accès public tient au fait qu'elle est à l'origine de toute affirmation selon laquelle les réseaux seraient universellement disponibles. Par conséquent, les politiques et l'administration des établissements offrant cet accès public aux réseaux jouent un rôle essentiel lorsqu'il s'agit de faire de la liberté d'expression et de la liberté d'accès aux contenus disponibles sur les réseaux une réalité, et pas seulement des principes.

2.1 Etablissements d'enseignement

Dans les pays européens, la quasi-totalité des universités et autres établissements d'enseignement supérieur offrent un accès aux réseaux, de même que les écoles sont de plus en plus nombreuses à le proposer au personnel et aux élèves. Ainsi, plus de 85 % des écoles secondaires britanniques offrent un accès à l'Internet, contre 5 % seulement des écoles primaires (Blamire, 1998). Etant donné la multiplicité des initiatives gouvernementales destinées à faciliter l'accès à l'Internet dans les écoles britanniques, on peut penser que celles-ci y auront toutes accès au début du prochain millénaire ; en outre, les autres pays européens vont eux aussi de rapides progrès en ce sens. Les universités visent généralement l'objectif d'un ordinateur raccordé au

réseau par bureau, et nombre d'entre elles commencent également à proposer la possibilité d'un raccordement dans chacune des chambres des résidences destinées aux étudiants. Toutefois, l'accès aux réseaux se fait encore le plus souvent dans une salle informatique, un laboratoire ou une bibliothèque. Le taux d'équipement est très variable puisque certaines écoles ne possèdent qu'un seul ordinateur branché au réseau, tandis que quelques universités disposent littéralement de centaines d'appareils connectés dans leurs centres d'apprentissage. C'est ainsi que l'essentiel des contenus véhiculés sur le réseau et mis à la disposition des enseignants dans les écoles et des étudiants ou élèves à tous les niveaux de l'enseignement sont consultés à partir de points d'accès public.

2.2 Bibliothèques et autres centres d'information

Les bibliothèques et centres d'information sont de plus en plus nombreuses à proposer au public un accès aux réseaux de l'information. Aux fins du présent rapport, nous nous proposons d'assimiler l'accès dans les bibliothèques scolaires et universitaires et scolaires à une forme d'accès public offert par les établissements d'enseignement en général, et non à l'accès proposé par les bibliothèques. Nous n'en ferons pas de même, toutefois, pour les bibliothèques de recherche et autres bibliothèques spécialisées qui, de par leur clientèle étroitement définie et limitée, diffèrent des bibliothèques publiques pour ce qui est de l'accès public aux réseaux. Au même titre que ceux des centres d'information spécialisés dans le domaine du tourisme, de l'éducation, de l'emploi et autres thèmes importants pour le citoyen, les points d'accès mis à la disposition du " public " dans ces établissements répondent à un objectif clair et bien défini. Le cas des bibliothèques publiques est manifestement différent, elles qui commencent à proposer un accès aux réseaux dont on peut véritablement dire qu'il est public. Un grand nombre de bibliothèques publiques en Grande-Bretagne et au Danemark sont assez largement équipées en ordinateurs, et beaucoup proposent un accès à l'Internet. Les autorités britanniques ont promis que toutes les bibliothèques publiques de Grande-Bretagne seraient prochainement raccordées au réseau (*New Library*, 1997). En 1996 cependant, on considérait que 20 % seulement des bibliothèques publiques d'Allemagne et du Portugal étaient équipées d'ordinateurs (Thorhauge, 1997). En 1997, on ne dénombrait en Allemagne que 20 bibliothèques publiques ayant leur propre site Web, mais la situation a rapidement évolué depuis, puisque des bibliothèques publiques aussi modestes que celle de Zadar, en Croatie, se sont dotées en 1998 d'un site présenté de manière professionnelle.

Les centres d'archives disposent également de stations de travail en libre accès, en premier lieu pour la consultation de leur propre réseau de recherche et de récupération de documents. Un raccordement à l'Internet permet alors l'accès aux réseaux électroniques et aux pages Web d'autres centres d'archives. Dans ce contexte, certaines catégories de restrictions sont d'ores et déjà imposées dans le cadre normal du fonctionnement d'un service d'archives, restrictions qui relèvent généralement de la protection de la confidentialité de l'information et de la vie privée (Conseil de l'Europe, 1998). Toutefois, un autre principe important de la pratique archivistique consistant à assurer le meilleur accès possible aux documents anciens quel que soit leur support, le fait pour les archives de proposer des points d'accès public s'inscrit tout naturellement dans leur philosophie.

2.3 Institutions culturelles

Il est désormais pratique courante pour les musées de proposer à leurs visiteurs une forme quelconque de présentation multimédia consacrée à leurs collections et à leurs expositions, mais nombre d'entre eux leur offrent également la possibilité d'accéder à des ressources culturelles extérieures, mises à disposition du public sur les réseaux informatiques. Nombreux sont aussi les institutions à vocation culturelle telles que les médiathèques, les centres d'action sociale et artistique et diverses petites entreprises artistiques de toutes sortes qui offrent un accès aux réseaux. L'ampleur et la nature de l'accès proposé par ces institutions sont très variables selon les cas, mais d'une manière générale, possibilité est donnée au public, non seulement de consulter le

travail d'autrui, mais aussi de fabriquer lui-même ses propres contenus culturels ou éducatifs. Pour ne citer que quelques-uns de ces établissements déjà nombreux et dont le nombre est en constante augmentation, mentionnons Artec, à Londres, la *Society for Old et New Media*, à Amsterdam, *Public Netbase*, à Vienne, Terravista, à Lisbonne et Mikro, à Berlin (exemples tirés d'une contribution inédite de Marleen Stikker, de la *Society for Old et New Media*). L'imposition d'une restriction d'accès aux réseaux, quelle qu'elle soit, serait totalement contraire à la philosophie de ces centres et constituerait une sérieuse entrave à la liberté d'innover grâce aux nouveaux médias, qui est leur véritable raison d'être.

2.4 Bornes d'information et cafés Internet

Enfin, il est une autre forme d'accès dont on peut dire qu'elle est publique, dans la mesure où elle est disponible à moindre coût pour quiconque souhaite y recourir. Mais cet accès est en même temps souvent privé, en ce sens qu'il est assuré par des entités privées ou dans une enceinte privée. Les cafés Internet ou cybercafés sont de plus en plus nombreux dans les grandes villes ou dans les villes moyennes. Il s'agit de cafés où l'on peut, moyennant consommation et pour un coût modique, se servir d'un ordinateur raccordé au réseau, un peu à l'instar de la lecture (gratuite) de journaux et de magazines que les cafés continuent de proposer à leurs consommateurs dans certains pays européens. On trouve aussi des terminaux (ou bornes) publics d'information dans l'entrée d'édifices publics, les galeries marchandes, les infrastructures de transport, ainsi que dans la rue. Il s'agit dans la plupart des cas pour le public d'accéder à un réseau unique et dédié d'informations en matière d'administration locale, de consommation, de voyages ou autres renseignements divers. Touchpoint constitue un exemple de ce type de services au Royaume-Uni. Aux Pays-Bas, KPN Telecom, l'opérateur national de télécommunications, a installé dans les rues des bornes à partir desquelles on peut accéder à l'Internet avec une simple carte téléphonique nationale. D'abord expérimenté dans 25 sites pilotes à Amsterdam, ce système est en cours de généralisation, et intéresse d'autres régions du monde. A de nombreux égards, il s'agit de points d'accès au réseau dont on peut véritablement dire qu'ils sont publics et libres du type de contraintes stratégiques et administratives qui se posent aux autres établissements proposant un tel service à l'intérieur de leurs murs.

3. Aspects du Probleme

Bien que nombre des problèmes se posant aux responsables de points d'accès publics aient été abordés dans le Vol. I de ce rapport, il convient à ce stade de faire la synthèse des principaux thèmes de préoccupation. Il y a d'abord les aspects relatifs à la responsabilité des points d'accès au réseau eu égard aux contenus mis à la disposition du public par leur intermédiaire et aux contenus effectivement consultés par les usagers. Se posent notamment les questions suivantes :

- la responsabilité relative aux contenus illégaux;
- la responsabilité relative aux contenus préjudiciables;
- la protection des mineurs;
- la lutte contre les attentats à la pudeur.

Se posent ensuite les problèmes inhérents à l'adoption éventuelle de systèmes de filtrage des contenus et de blocage d'accès à certains sites, notamment :

- la justification morale du filtrage des contenus
- coûts et conséquences du filtrage.

3.1 La responsabilité relative aux contenus illégaux

Les personnes ou institutions offrant des points d'accès publics au réseau redoutent de voir leur responsabilité engagée pour l'usage susceptible d'être fait de leurs installations. Toutefois, il s'agit d'une responsabilité que la loi tend à faire porter très clairement aux fournisseurs desdits contenus. Ainsi, les fournisseurs d'accès à l'information sont eux aussi largement dégagés de cette responsabilité à l'égard des contenus qu'ils mettent à disposition des usagers, à moins d'être intervenus, à un titre ou à un autre, dans leur édition, leur rédaction ou leur conception. Mais en mai 1998, les tribunaux bavarois n'en ont pas moins déclaré Felix Somm, ancien directeur de CompuServe en Allemagne, coupable d'avoir favorisé et encouragé la pornographie impliquant des enfants. Ce verdict semble aller à l'encontre de la récente législation allemande en matière de multimédia, qui dégage les fournisseurs d'accès à l'information de toute responsabilité eu égard aux contenus mis en réseau par leurs clients, à moins qu'ils n'aient eu connaissance de la nature desdits contenus et aient manqué de prendre des mesures pour les retirer (*Child porn*, 1998). Il ressort donc clairement que les gérants de points d'accès publics ne courent aucun véritable risque légal du fait des contenus auxquels leurs " clients " sont susceptibles d'accéder à partir des stations de travail mises à leur disposition. En fait, c'est essentiellement l'utilisateur lui-même qui doit assumer la responsabilité des contenus qu'il choisit de consulter sur le réseau. C'est ainsi que des enseignants ont été suspendus ou congédiés pour avoir téléchargé des contenus à caractère pornographique sur des écrans susceptibles d'être vus par des jeunes dont ils avaient la garde.

3.2 La responsabilité relative aux contenus préjudiciables

La question des contenus dits préjudiciables, mais pas nécessairement illicites, pose un problème plus délicat. Suite aux protestations véhémentes de certains groupements bien organisés suscitées par certains contenus de l'Internet liés au sexe, à la drogue, à la politique et autres thèmes controversés, mais bénéficiant à l'évidence de la protection de la loi dans la plupart des pays démocratiques, le débat relatif à cette catégorie de contenus est désormais assimilé à celui dont font l'objet les contenus illégaux. Il s'agit-là d'un dangereux amalgame, qui menace de saper l'objectif central des points d'accès publics, ainsi que les institutions qui les hébergent. Lorsque des contenus ne sont pas illégaux, chacun a clairement le droit d'opter pour leur consultation. Si le gérant d'un point d'accès public n'est pas fondamentalement responsable des contenus mêmes, il l'est par contre de veiller à garantir le libre accès à ces contenus.

Si le débat sur ce point a essentiellement porté jusqu'à présent sur les bibliothèques, il concerne en fait toutes les catégories de centres d'information. Les services d'archives, par exemple, ont pour mission de garantir la liberté d'accès à l'information, au même titre que les bibliothèques. L'archivage des contenus de l'Internet est une question importante qui n'a encore été qu'effleurée par les professionnels. On pourrait, grâce à un service de numérisation des contenus de l'Internet, s'efforcer de les archiver dans l'intérêt de la postérité, en se concentrant se faisant sur les contenus dépourvus de support papier. En poussant au maximum la logique de ce raisonnement, les types de contenus controversés qui posent problème en d'autres points d'accès publics présenteront les mêmes difficultés aux archives.

Il est important que le principe de la liberté d'accès soit clairement compris à l'échelle de tous les métiers de l'information. Lors de la conférence consacrée à la Société de l'information du vingt-et-unième siècle et au rôle des associations de bibliothèques, qui s'est tenue à Budapest du 11 au 13 mai 1998, le caractère central de cette liberté a été fortement réitéré, ainsi par Barbara Ford, Présidente de la *American Library Association*: " La liberté intellectuelle est la valeur clé de la bibliothéconomie " ou par Bendik Rugaas, de la Bibliothèque nationale de Norvège: " La liberté est la seule raison d'être de la bibliothéconomie ". De tels principes peuvent aussi s'appliquer tout aussi bien à d'autres activités professionnelles en matière d'information dans les domaines de l'éducation et de la culture.

Ce principe de la liberté est particulièrement important pour des établissements tels que less bibliothèques publiques, qui ont les attributions les plus larges qui soient en matière de contenus et de disciplines. Leur vaste fonction culturelle permet tout naturellement à leurs utilisateurs de suivre

des pistes de recherche susceptibles de le mener à des contenus faisant l'objet de controverses intellectuelles, politiques et artistiques. Si d'aucuns prétendent que les établissements financés par l'Etat devraient empêcher l'accès aux contenus réputés préjudiciables, une telle interdiction constituerait une violation flagrante de la liberté d'accès à l'information.

3.3 La protection des mineurs

Dans tout ce débat, la question la plus délicate concerne les jeunes toujours sous la tutelle légale de leurs parents. L'école et autres institutions assumant une partie de cette responsabilité *in loco parentis* doivent s'efforcer d'agir dans le même esprit que le feraient les parents. Toutefois, même si les parents et leurs substituts sont légalement habilités à imposer des restrictions d'accès aux jeunes dont ils ont la garde, on peut se poser la question de savoir s'ils ont entièrement le droit moral de le faire. On pourrait faire valoir qu'un point d'accès public à partir duquel les jeunes peuvent obtenir des informations sur la manière dont il convient de se protéger lors des relations sexuelles ou se renseigner sur les problèmes de drogues est plus bénéfique qu'un parent ayant tout fait pour tenter d'interdire aux jeunes l'accès aux informations en question.

Quoi qu'il en soit, on constate que les enfants n'ont qu'un accès restreint à l'information, parfois en raison du fait que de nombreuses écoles, par exemple, s'en remettent entièrement à l'information fournie par l'enseignant et issue des manuels. En fait, les bibliothèques scolaires offrant véritablement un vaste choix de matières et de contenus constituent l'exception plutôt que la règle dans la plus grande partie de l'Europe. Même aux Etats-Unis, où les bibliothèques ont le plus souvent de grandes dimensions et bien fournies, on constate une tendance à garder un contrôle assez strict sur les ouvrages disponibles (Doyle, 1997). Pour reprendre les propos d'un auteur récent :

> Les précédents juridiques et historiques ne manquent pas, qui témoignent de l'imposition de la censure sur tout support utilisé dans les écoles financées grâce aux deniers publics (Lamont Johnson, 1996).

En conséquence, si la restriction de l'accès des jeunes aux réseaux de l'information porte certes atteinte à cette précieuse liberté d'explorer et d'apprendre par l'exploration qu'offre ce moyen de communication, il faut admettre que la pratique n'est pas inhabituelle dans les systèmes scolaires.

3.4 La lutte contre les attentats à la pudeur

Dans un certain sens, on peut dire que l'usage, à des fins de divertissement, des contenus mis en réseaux consultés dans les lieux publics peut contribuer à distraire les " vrais " internautes. Ainsi, on peut citer l'exemple des jeux vidéo ou informatiques bruyants ou remplis de couleurs et de gadgets clignotants. Dans certaines catégories de centres d'information (les bibliothèques spécialisées, etc.), l'accès aux réseaux est offert grâce à des financements publics ou privés à des fins qui, bien que pouvant à l'occasion comporter des éléments ludiques ou récréatifs, visent une finalité informative, éducative ou culturelle spécifiquement définie. On peut faire valoir que l'internaute qui se connecte au réseau à partir de ces points d'accès n'a aucun droit particulier d'accéder aux contenus autres que ceux se rapportant aux objectifs définis par les institutions qui les hébergent. Le fait pour ces dernières d'interdire l'accès à de tels contenus non pertinents ne constituerait donc pas une violation notable des droits fondamentaux.

Par ailleurs, si le point d'accès est utilisé par l'usager pour consulter des contenus illégaux ou préjudiciables (c'est le plus souvent de pornographie qu'il s'agit dans ce contexte, on peut parfois parler d'attentats à la pudeur, de troubles de l'ordre moral, voire de harcèlement aux dires de certains. Nombreux sont ceux qui prétendent que celui qui récupère sur l'ordinateur des textes, des images, voire des sons, inconvenants à partir d'un terminal public ne doit pas ce faisant attenter à la pudeur d'autrui. Ainsi, il est arrivé que des individus soient surpris en train de se masturber en public devant des écrans à caractère pornographique, de même que des femmes

ont gagné le procès pour harcèlement sexuel qu'elles avaient intenté à leur patron ou collègues ayant téléchargé des contenus à caractère pornographique dans des fichiers qu'elles avaient par la suite été appelées à consulter. Toutefois, des arguments du même ordre ont toujours été invoqués et le sont encore (sans grand succès d'ailleurs) à l'encontre des personnes qui consultent des ouvrages ou des magazines à caractère pornographique dans un lieu public quelconque comme une bibliothèque. Il existe une différence entre le fait de consulter discrètement ce genre de littérature, et ce pour quelque raison que ce soit, et le fait de le faire ostensiblement ou par négligence d'une manière susceptible d'offusquer autrui. Dans ce dernier cas de figure, le gérant du point d'accès peut intervenir sans nécessairement empêcher l'accès aux sites en question ; par contre, dans le premier cas de figure, accepter son intervention revient à reconnaître que les préférences morales ou personnelles d'un individu peuvent l'emporter sur celles d'un autre.

3.5 La justification morale du filtrage des contenus

La question qui se pose consiste à savoir si le responsable d'un point d'accès public au réseau qui filtre certains contenus et bloque l'accès à d'autres catégories de contenus pratique en fait une forme de censure. Le filtrage a été qualifié par certains de " privatisation de la censure " (Lasica, 1997) et par d'autres comme une " véritable solution de rechange à la censure de l'Internet " (*Internet censorship*, 1997). Ces affirmations recèlent toutes deux une part de vérité, variable selon les circonstances. Pour l'individu ou la famille déterminés à limiter leur propre degré d'exposition à certains types de contenus, le filtrage peut effectivement apparaître comme une solution de rechange acceptable par rapport à la censure. Il faut noter ici la formulation retenue dans la Déclaration de Bonn sur le filtrage et l'évaluation, aux termes de laquelle l'important consiste à :

> Donner aux usagers la possibilité de sélectionner les catégories de contenus qu'ils souhaitent ou, au contraire, ne souhaitent pas récupérer, compte tenu de la surcharge d'information et de la présence sur le réseau de contenus indésirables ou préjudiciables (Conférence ministérielle,1997).

Ce texte fait référence aux utilisateurs des réseaux informatiques, plutôt qu'à ceux qui agissent en leur nom. Il mentionne le recours au filtrage pour aider les usagers à déterminer eux-mêmes ce qu'ils souhaitent consulter, avant même de parler de ce qu'ils *ne veulent pas* récupérer à l'écran. Il évoque le problème de la localisation des ressources en situation de surcharge d'information, avant de faire allusion à la question des contenus indésirables. Dans tous les cas, il s'agit de l'individu et de sa capacité à opérer un choix.

Mais aux yeux du particulier faisant usage d'un point d'accès public aux réseaux, l'utilisation par l'institution d'accueil d'un logiciel de filtrage s'apparenterait incontestablement à une forme de censure. Par ailleurs, dans la plupart des pays, elle serait considérée comme un abus législatif. Etant donné que l'objet du présent rapport concerne les points d'accès publics aux réseaux de l'information, il convient ici de se pencher plus particulièrement sur leur cas. Comme nous l'avons laissé entendre au point 3.3, la mise en place d'un système de filtrage dans un établissement scolaire ne serait pas incompatible avec la tradition dans un type d'institution où l'application du concept *in loco parentis* est très importante. Elle peut également se justifier dans les institutions où l'accès du public à l'information doit nécessairement rester dans les limites des buts et objectifs de ces dernières (voir le point 3.4), et ce pour des raisons n'ayant rien à voir avec un quelconque jugement moral porté sur les contenus susceptibles d'être consultés.

Une chose est certaine, le filtrage n'a pas sa place dans les institutions ayant en matière d'information un mandat très large, notamment les bibliothèques publiques. Comme nous l'avons indiqué dans le Vol. I, le plus ardent défenseur de ce point de vue est la *American Library Association* (ALA), invoquant le premier amendement de la Constitution américaine, texte qui a inspiré par la suite la *Library Bill of Rights*. Ce dernier texte a été adopté par l'ALA le 16 juin 1948 et cité à plusieurs reprises depuis, la dernière fois remontant au 23 janvier 1996 (*Library Bill*,

1996). Cette " charte " énonce sans la moindre ambiguïté possible :

> Les bibliothèques doivent mettre à la disposition des lecteurs un éventail d'ouvrages, de documents et d'informations présentant l'ensemble des points de vue exprimés sur les questions d'actualité et historiques. Aucun contenu ne doit faire l'objet d'une interdiction ou d'un retrait pour des raisons partisanes ou doctrinales.

On fait parfois valoir, qu'étant donné que les bibliothécaires ont toujours exercé une certaine sélection dans les ouvrages qu'ils achètent et mettent à la disposition du public, le recours au filtrage constitue le prolongement logique d'une telle pratique. S'il est probablement vrai que certains bibliothécaires ont invoqué le commode argument de la nécessaire sélection pour justifier leur non-acquisition d'ouvrages controversés, le *Bill of Rights* fait clairement état de la nécessité de prendre en compte la totalité des points de vue exprimés. Avec l'Internet, aucune sélection motivée par des raisons de manque d'espace ou d'argent n'étant justifiée, tous les points de vue peuvent désormais être pris en compte. D'ailleurs, le juge d'une cour américaine fédérale de grande instance a directement rejeté l'analogie entre sélection et filtrage, faisant remarquer que, puisque les contenus stockés sur l'Internet ne nécessitent pas d'étagères ou d'entretien, il est en réalité plus coûteux à une bibliothèque de restreindre l'accès à certains d'entre eux que de laisser carte blanche aux utilisateurs (*Censorship ruling*, 1998). En dépit des arguments passionnés invoqués pour la justifier (Burt, 1997), l'installation d'un système de filtrage n'est pas une pratique acceptable dans les points d'accès aux réseaux véritablement publics.

3.6 Coûts et conséquences du filtrage

Le filtrage des contenus comporte des coûts directs presque tout au long de la chaîne de l'information. Le coût de l'achat et de l'installation de logiciels de filtrage et de blocage d'accès, probablement le poste le moins important, est une dépense qui incombe directement au propriétaire du point d'accès, même si le logiciel est fourni avec le reste du système. A Boston, au Massachusetts, où des systèmes de filtrage ont été installés sur 200 bornes en accès public, on a estimé le coût de l'opération à 10 dollars par ordinateur raccordé au réseau et à 40 dollars par ordinateur avec accès direct au cadran. La plupart des autres coûts, presque impossibles à quantifier, sont répartis entre les divers intervenants. On ne peut donner à leur sujet qu'un ordre de grandeur.

La création d'une plate-forme de métadonnées telle que PICS suppose des coûts à l'échelle du système tout entier. De même, la mise au point de dispositifs d'évaluation n'est pas sans comporter de frais, bien que les frais directs de tels systèmes puissent être supportés par un organisme intéressé tel qu'une association professionnelle (la *Recreational Software Association*, par exemple), un groupe de lobbying ou une entité religieuse. Le coût inhérent à l'installation effective par un tiers tel une agence spécialement créée à cette fin de systèmes d'évaluation sur certains sites Web ou contenus serait exorbitant, ne serait-ce qu'en raison du nombre de contenus à évaluer. Même l'auto-évaluation comporte un coût, lequel peut être modeste lorsqu'il s'agit pour le fournisseur de contenus de consacrer temps et efforts à s'acquitter de cette mission, mais nettement plus important quand on confie à un organisme public ou non gouvernemental (comme la *Internet Watch Foundation* en Grande-Bretagne) le soin d'assurer la surveillance et de veiller à l'application du système. Interdire aux mineurs l'accès aux sites " réservés aux adultes " grâce à des systèmes d'authentification de l'utilisateur comporte également un coût, visible dans la mesure où, pour l'instant, les entreprises offrant ce service récupèrent leur mise grâce aux redevances qu'elles facturent à leurs clients. Même tous les ordinateurs du monde étaient équipés de mécanismes de filtrage et de blocage, il resterait les coûts afférents à la surveillance du système et les frais des poursuites judiciaires. Ces derniers ne seraient pas nécessairement réduits étant donné qu'une réglementation plus stricte des contenus pourrait en réalité se traduire par une augmentation du nombre de cas litigieux signalés à l'attention des autorités chargées de faire appliquer la loi et de la justice.

La question des coûts ne se pose pas simplement en termes monétaires. Il y a également ce que l'économiste appelle les *coûts d'opportunité*. En imposant des restrictions sur l'Internet, on peut priver certains usagers des avantages qui résultent d'une " navigation " relativement plus libre sur le réseau utilisé pour développer leurs compétences et leur expérience en matière d'information. Par ailleurs, on risque également d'entraver les possibilités de création découlant pour l'usager de découvertes fortuites et de la juxtaposition inattendue d'images et d'idées. L'Internet représente actuellement un univers trop chaotique pour que son utilisation puisse être facilement canalisée dans des directions totalement prévisibles, et toute tentative en ce sens risquerait de se traduire par des pertes pour l'individu ou l'organisation en question.

Inversement, on peut faire valoir que le fait de ne pas filtrer comporte également certains coûts. Ainsi, l'une des raisons qu'une institution peut avoir d'imposer des restrictions d'accès aux réseaux tient au fait qu'une bonne partie des utilisateurs se servent de l'Internet à des fins de divertissement. Il faut simplement reconnaître que de telles pratiques ont non seulement pour résultat d'occuper l'employé ou l'étudiant pendant un temps qu'il est censé consacrer à d'autres fins directement liées aux objectifs de l'établissement, mais elles peuvent aisément faire peser une charge trop lourde sur la largeur de bande et la mémoire des systèmes d'information de ce dernier, au détriment d'usages plus pertinents. Les gestionnaires n'ont guère de difficulté à se laisser convaincre qu'il est nécessaire, dans l'intérêt de leur entreprise, d'imposer des mesures de restriction d'accès pour éviter les utilisations non pertinentes de leurs systèmes d'information, et que le meilleur moyen de parvenir à cet objectif consiste à bloquer l'accès à certains contenus disponibles sur le réseau.

Il faut également mentionner le coût des préjudices réputés subis par ceux ou celles qui ont été exposés à des contenus préjudiciables. Ceux qui souhaitant restreindre ou barrer l'accès à certaines catégories de contenus font valoir que ces dernières encouragent des comportements non dépourvus de coûts sociaux, dont certains sont quantifiables. Ainsi, en supposant que l'Internet incite à la consommation de drogues, cette situation pourrait avoir des conséquences sur le taux de délinquance et sur la nécessité de fournir certains services d'aide psychologique et médicale. Dans certaines affaires de harcèlement sexuel, les victimes ont prétendu avoir subi un traumatisme du fait de leur exposition accidentelle à des contenus inconvenants, et obtenu e ce fait des dommages et intérêts importants, de même que la condamnation des coupables à de lourdes sanctions.

La plupart de ces questions ont donné lieu à un débat passionné dans les métiers de l'information aux Etats-Unis. La polémique s'est à tel point dégradée dans le cadre du gestionnaire de messagerie électronique Listserv tenu par le *Office for Intellectual Freedom* de l'ALA qu'il a fallu lancer quelques appels à la modération (Berry, 1998). David Burt, peut-être le plus ardent défenseur du filtrage dans les bibliothèques et dans le monde de la bibliothéconomie, s'est retiré de la liste à la suite de ces évènements, et refusé de contribuer au débat à moins que l'on n'introduise une certaine forme de modération. Bien que le point de vue de Burt semble ne concerner qu'une minorité de personnes au sein de l'ALA, il est très largement partagé par l'opinion publique (voir le Vol. I , point 5.6). L'ALA publie un certain nombre de documents pour aider les bibliothécaires à répondre à ceux de leurs usagers qui contestent la nature des ouvrages mis à leur disposition (*Coping with challenges*, 1996; *Questions and answers*, 1997). Si ce débat existe également en Europe, il est loin d'avoir atteint le même degré d'intensité qu'outre-atlantique.

4. Filtrage: Legislation et Application

Le débat sur les points d'accès publics aux réseaux porte essentiellement sur des questions de filtrage et de blocage de l'accès à certains contenus. Il concerne en substance la totalité ou la plupart des aspects abordés dans la section précédente. Il tend à être axé en priorité sur deux grands domaines : les tentatives de législation et les polémiques auxquelles donnent lieu les efforts déployés par certains pour introduire le filtrage dans leurs bibliothèques et écoles.

4.1 Le droit européen

Depuis la rédaction du premier volume de ce rapport (décembre 1997), la principale nouveauté survenue en Europe dans le débat politique sur le filtrage concerne la Recommandation sur la protection des mineurs et de la dignité humaine dans les services audiovisuels et d'information (Commission européenne, 1998). Ce texte a été promulgué par le Parlement européen le 14 mai 1998, à une majorité de 513 voix contre 1, et adopté le 28 mai par le Conseil. Il y est précisé que contenus illégaux et contenus préjudiciables constituent deux problèmes différents, qui nécessitent des démarches et des solutions différentes. Le document met l'accent sur l'auto-réglementation et la responsabilité et, en particulier, au point 5 de la Recommandation, appelle à des mesures susceptibles de "faciliter la recherche et la consultation de contenus et de services de qualité pour les mineurs, notamment dans les établissements d'enseignement et les lieux d'accès publics". Cette insistance sur la nécessité de faciliter l'accès à des contenus de qualité, et non d'empêcher celui aux contenus préjudiciables constitue une affirmation importante de la notion selon laquelle l'action doit être guidée par des principes positifs, et non dictée par la crainte.

Le texte poursuit en indiquant que l'auto-réglementation doit passer par un ou plusieurs codes de conduite. Si l'on veut qu'un tel code puisse effectivement assurer la protection des mineurs, il faudrait que les fournisseurs de services d'information signalent les contenus potentiellement préjudiciables au moyen d'une page d'avertissement, d'un étiquetage descriptif et de systèmes permettant de vérifier l'âge des usagers. Il est également mentionné que les parents devraient être aidés dans leur mission de surveillance par un logiciel de filtrage configuré à l'avance (certaines options pouvant être choisies par l'utilisateur final). Mais à aucun moment dans le texte on ne fait référence à la question du filtrage sur les points d'accès publics, ce qui est important dans la mesure si des dispositions devaient effectivement être prises en ce sens, en particulier dans les endroits fréquentés par des jeunes de tous âges, elles auraient des répercussions sur lesquelles il serait important de se pencher.

S'agissant des points d'accès aux réseaux exclusivement destinés à des jeunes (écoles ou bibliothèques pour la jeunesse), la recommandation européenne autoriserait le recours à un système de filtrage qui permette un accès aussi large que possible tout en donnant aux parents des garanties de sécurité quant aux conditions de la consultation. Les fournisseurs veilleraient à ce que les jeunes ne puissent pas tomber aisément sur des contenus réputés ne pas leur convenir. Une page d'avertissement donnerait à l'usager la possibilité de ne pas récupérer certains contenus s'il ne le souhaite pas les consulter. En outre, l'adjonction d'un dispositif d'étiquetage descriptif permettrait un filtrage encore plus précis, fondé sur des évaluations de contenus soigneusement pesées à l'avance. Quant aux mécanismes de vérification de l'âge de l'usager, ils interdiraient aux jeunes l'accès à certains sites bloqués par les fournisseurs de contenus (ou laisseraient aux jeunes en question la possibilité d'endosser eux-mêmes la responsabilité d'une consultation rendue possible par un contournement quelconque du dispositif de protection). Le responsable d'un point d'accès public aux réseaux destiné à des jeunes serait alors en mesure de conseiller et d'aider les usagers à partir des informations fournies par ces différents avertissements et mécanismes de blocage. A ce stade, il serait possible à ceux qui estiment que certains contenus sont inutilement bloqués de désactiver ou d'adapter le filtrage au terme d'une négociation.

La situation serait autre dans un point d'accès public destiné à des personnes de tous âges (dans une bibliothèque publique, par exemple). Un adulte peut tout à fait souhaiter tirer parti des avertissements pour s'éviter des contenus susceptibles de lui déplaire. Par ailleurs, ce même adulte peut désirer accéder à des contenus licites, mais inconvenants, et ce pour toute une série de raisons parfaitement légitimes. Il se peut que les avertissements soient plus ou moins opportuns et que le dispositif de vérification de l'âge de l'usager ne pose aucun problème, mais la mise en place d'un mécanisme de filtrage des contenus, fondé sur les désirs des parents quant aux sites auxquels ils souhaitent autoriser l'accès à leurs enfants, constituerait une atteinte manifeste du droit de l'adulte à la liberté d'accès à l'information. Ainsi, aussi louable que soit la

Recommandation à bien des égards, tout code de conduite relatif aux points d'accès publics susceptible d'en être inspiré devra veiller à ce que le souci de protection des mineurs ne porte pas atteinte aux libertés fondamentales.

A l'échelon national, l'Allemagne a adopté assez récemment une nouvelle législation en la matière. Un amendement à la loi sur la diffusion de publications moralement nocives pour la jeunesse est entré en vigueur en août 1997, dans le cadre d'un train de mesures de transposition de directives communautaires (République fédérale d'Allemagne, 1997). Cet amendement fait référence à un ensemble de mesure techniques …. destinées à faire en sorte que l'offre ou la diffusion en Allemagne [de publications moralement nocives par le biais de services d'information et de communication électroniques] soient réservées aux usagers d'âge légal." Cette disposition a généralement été interprétée de manière telle qu'elle oblige les points d'accès publics aux réseaux à équiper de logiciels de filtrage celles de leurs stations de travail qui sont mises à la disposition des moins de 18 ans, bien que la formulation (du moins dans sa version traduite) semble sur ce point obscure. Il semblerait que cette loi soit le texte le plus ferme qui soit en matière de filtrage en Europe.

4.2 La loi aux Etats-Unis après la CDA

Depuis 1997, année au cours de laquelle la *Communications Decency Act* (CDA, Loi sur la moralité des communications) a été rejetée par les tribunaux pour cause d'inconstitutionnalité, le débat politique aux Etats-Unis a évolué. Le sommet consacré au thème de l'Internet, qui s'est tenu à Washington du 1 au 3 décembre 1997, n'a pas vraiment permis de dégager un consensus. Dans une contribution peut-être plus éloquente par ce qu'il n'y était pas dit, le vice-président Al Al Gore s'est déclaré très favorable à l'utilisation par les parents de mécanismes de filtrage, mais à l'instar des autres participants à ce sommet, il n'a guère abordé la question des points d'accès publics. Cette manifestation n'ayant pas réussi, pas plus d'ailleurs que d'autres initiatives, à calmer l'indignation et l'inquiétude populaires au sujet des contenus de l'Internet, de nouveaux projets de loi ont été présentés depuis au corps législatif américain

Le plus important d'entre eux a été celui du sénateur John McCain sur le filtrage de l'Internet dans les écoles (St. Lifer, 1998), visant à réserver les remises sur les services de télécommunications aux écoles et bibliothèques ayant accepté d'introduire des mécanismes de filtrage sur leur accès à l'Internet. Ce projet de loi a franchi avec succès les premières étapes de la procédure habituelle, même si l'on soupçonne le président Clinton et le vice-président Al Gore de préférer un amendement réservant les subsides aux seuls points d'accès ayant adopté une stratégie de protection des mineurs. Le texte a été rejeté par l'ALA pour des raisons de principe, l'association estimant que ce projet de loi empêcherait les bibliothèques de répondre aux besoins d'information de la collectivité dans son ensemble. Il a également été fait remarquer que de nombreuses bibliothèques refuseraient toute subvention liée à l'introduction obligatoire d'un dispositif de filtrage. McCain a lui-même défendu son projet de loi :

> " La prévention ne consiste pas à censurer les contenus placés sur l'Internet, mais plutôt à filtrer ce qui peut être récupéré sur les ordinateurs que nos enfants utilisent en dehors de chez eux " (Flagg, 1998).

Dans ce cas, la prévention s'exercerait en réalité à l'encontre des adultes comme des enfants, sans faire non plus de distinction entre jeunes d'âges différents. Or, un site relatif, par exemple, aux pratiques sexuelles sans risque, susceptible de ne pas convenir à un enfant de 6 ans, peut être tout à fait indiqué pour un adolescent de 16 ans.

On assiste par ailleurs à une activité législative considérable au niveau des différents Etats américains. Si l'intention de ces projets de loi est variable d'un cas à l'autre, tous les textes visent généralement la protection des mineurs contre les contenus préjudiciables (Oder, 1998). Dans divers Etats comme le Nouveau-Mexique et l'Ohio, quelques projets de loi ont été déposés qui

cherchent à réglementer les contenus mis en réseau par les fournisseurs d'accès à l'Internet. Ces différentes initiatives n'ont pas pour l'instant fait énormément de progrès et semblent promises au même sort qu'une loi de l'Etat de New York State rejetée en 1996 par les tribunaux. Les efforts législatifs ont remporté davantage de succès en ce qui concerne l'imposition, sur les points d'accès publics fréquentés par des mineurs, de mécanismes de filtrage des contenus à caractère explicitement sexuel. En 1998, divers projets de loi ont été introduits dans les Etats de l'Arizona, de Californie, de l'Indiana, du Kansas, du Missouri, de l'Oklahoma, du Tennessee, de Virginie et de Washington qui, malgré des différences en ce qui concerne les détails de la démarche adoptée dans chaque cas, ont tous en commun de concerner, partiellement du moins, les points d'accès publics. Plusieurs de ces projets de loi s'apparentent au texte de McCain en ceci qu'ils tentent, d'une manière ou d'une autre, de lier l'attribution d'un financement quelconque à la mise en place d'un mécanisme de filtrage. Dans la plupart des cas, la *American Library Association* a monté des campagnes efficaces d'information et de lobbying pour modifier les mesures proposées ou leur faire échec. De toute évidence, le combat est loin d'être terminé et devrait se poursuivre un certain temps encore.

4.3 La mise en œuvre du filtrage

Un certain nombre de municipalités, dont les exemples les plus fameux concernent les Etats-Unis d'Amérique, ont cherché à imposer le filtrage sur leurs points d'accès publics aux réseaux. Et c'est précisément au sein de ces municipalités que les divergences d'opinion au sujet du filtrage se sont le plus clairement exprimées. Le cas de certaines d'entre elles fait d'ailleurs figure de mini-causes célèbres. Nous nous proposons de développer ci-après deux affaires importantes, celle de Austin, au Texas et celle de Loudoun, en Virginie.

4.3.1 Austin (Texas)

Dans la ville d'Austin, au Texas, les bibliothèques publiques pratiquent le filtrage depuis 1997 (Branch et Conable, 1997), une décision précipitée par deux incidents ayant troublé le personnel. D'abord, un usager a été surpris en train d'imprimer des écrans récupérés sur des sites à caractère pédophile, un autre adulte ayant par la suite été pris en flagrant délit au moment où il montrait à de jeunes enfants comment accéder à des sites pornographiques. Dans un premier temps, il a donc été décidé d'installer le logiciel de filtrage *Cyber Patrol*, la ville d'Austin n'ayant pas cessé depuis de revoir sa position sur la question. Trois raisons ont été invoquées pour justifier la décision d'introduire le filtrage : la nécessité de mettre les enfants à l'abri de contenus susceptibles de leur être préjudiciables; la nécessité de protéger le personnel contre ce que certains considéraient relever du harcèlement sexuel; et celle la nécessité d'éviter aux usagers récupérant des contenus illégaux tout risque de voir leur responsabilité engagée devant la loi. Les bibliothécaires de la ville de Austin reconnaissent que le système bloque certes l'accès à certains contenus légaux et utiles, mais ils ont accepté de redonner l'accès à environ 300 sites suite aux réclamations du public. Afin d'éviter d'être accusés de porter atteinte aux droits des usagers en vertu du premier amendement de la Constitution, les bibliothécaires affichent un avertissement indiquant que les contenus sont filtrés sur toutes les stations de travail raccordées à l'Internet. Ils n'utilisent pas pour l'instant toute la gamme des possibilités offertes par le logiciel, puisqu'ils ont choisi au départ de ne bloquer l'accès qu'aux seuls sites contenant des images "de nudité partielle et totale", "des scènes choquantes" et "d'actes sexuels".

L'intérêt du cas de la ville d'Austin tient au fait que le filtrage n'y a été adopté qu'à titre provisoire et qu'il a fait l'objet depuis d'une étroite surveillance (Cyber Patrol, 1998). Le responsable de la programmation des systèmes de données a configuré Cyber Patrol en fonction des besoins locaux tels qu'ils les percevait à l'époque, et les catégories de contenus auxquels il est désormais impossible d'accéder ont été réduites pour ne concerner désormais que les seuls actes sexuels. On a envisagé la possibilité de séparer les ordinateurs (filtrés) réservés aux enfants des autres (non équipés de mécanismes de filtrage) destinés aux adultes. A l'origine, on a pensé qu'une telle solution ne serait pas pratique dans les établissements ne disposant que de deux ordinateurs,

utilisés de surcroît par une majorité d'adultes. La gêne occasionnée aux usagers dans les bibliothèques où ce système a été introduit posait un réel problème. Des expériences ont été menées, qui ont consisté à filtrer certains terminaux par souci de protection de la vie privée et de l'intimité de l'usager, mais cette solution ne s'est pas avérée entièrement satisfaisante (Schuyler, 1997). Pour toutes ces raisons, on peut dire de la ville d'Austin qu'elle a fait office de laboratoire d'expérimentation du filtrage dans les bibliothèques publiques. Les résultats de l'expérience ont livré quelques enseignements utiles quant à la gestion pratique du filtrage. Il est intéressant de remarquer que, depuis son adoption à Austin, le filtrage est de moins en moins fréquent et intensif, et grâce à l'expérience au quotidien que bibliothécaires et usagers ont pu vivre des effets du filtrage. Il s'agit désormais de tenter de concilier les préoccupations ayant mené à l'adoption du filtrage et la nécessité d'offrir un service d'information qui réponde aux exigences des usagers.

4.3.2 Loudoun (Virginie)

Le cas de Loudoun est important de par l'intérêt dont il a fait l'objet de la part du public et de la manière dont il a été jugé devant les tribunaux. En intentant des poursuites judiciaires contre la bibliothèque de Loudoun en décembre 1997, l'association locale baptisée " Mainstream Loudoun " a contesté l'installation de filtres sur tous les terminaux de la bibliothèque (St. Lifer et Rogers, 1998a). Cette politique de filtrage avait été adoptée pour les mêmes raisons qu'à Austin, à savoir la nécessité de protéger les mineurs, mais aussi pour empêcher les adultes de récupérer des contenus choquants, de nature à favoriser "un climat d'hostilité" propice à d'éventuelles accusations de harcèlement sexuel. Il s'agissait également d'éviter que la bibliothèque ou ses employés ne soient tenus responsables des contenus illégaux consultés par les usagers. La bibliothèque de Loudoun a opté pour le logiciel de filtrage X-Stop auquel l'on a reproché, comme à de nombreux autres produits de filtrage, de bloquer l'accès à un nombre de sites bien plus important qu'on ne l'aurait voulu à l'origine, notamment un certain nombre de sites tout à fait respectables comme Zero Population Growth, Safer Sex Education et le Women's site de la *American Association of University Women*. La bibliothèque de Loudoun a répondu à ces critiques en indiquant que les usagers pouvaient demander le déblocage de certains sites, la décision finale étant soumise à l'appréciation des bibliothécaires.

En assimilant pour sa défense le filtrage aux diverses pratiques acceptées en matière de bibliothéconomie, Loudoun a poussé un peu plus loin que d'habitude l'analogie habituelle avec la sélection de livres et de documents opérée par les bibliothèques. Il a été fait valoir que les ces dernières étaient libres de retenir certains ouvrages et d'en rejeter d'autres, et qu'elles n'avaient aucune obligation de se conformer aux préférences des lecteurs, pas plus qu'elles n'étaient contraintes de recourir au prêt inter-bibliothèques pour emprunter les livres qu'elles avaient choisi de ne pas acheter. Mainstream Loudoun a réfuté l'argument en faisant valoir que l'Internet constituait en fait une seule et même acquisition, et que le fait de refuser à un usager le droit de récupérer un contenu sur le réseau mondial équivalait à retirer un ouvrage des étagères de la bibliothèque ou de découper les articles d'une encyclopédie. Comme nous l'avons indiqué au point 3.5, le juge a finalement rejeté l'argument de Loudoun (St. Lifer et Rogers, 1998b) le 7 avril 1998, au motif que la politique de la bibliothèque n'était pas comparable à une décision de sélection, mais équivalait en fait à interdire à l'usager l'accès à des contenus déjà présents dans une collection de bibliothèque.

Le cas de Loudoun montre à quel point le filtrage peut faire l'objet d'une énergique défense, mais il est intéressant de l'opposer à celui du comté voisin de Prince William, en Virginie toujours, qui a opté pour une politique assez différente. Le Conseil de la bibliothèque y a voté contre l'installation d'un logiciel de filtrage, préférant laisser libre accès à l'Internet sur la plupart des ordinateurs. L'exception à cette règle devait concerner les terminaux de la section jeunesse, où les enfants étaient orientés en direction de des sites présélectionnés pour leur qualité, grâce au logiciel *Library Channel*. On a reproché à ce dernier de ne pas présenter un échantillon représentatif des contenus de l'Internet et de bloquer l'accès à certains sites exactement comme les filtres utilisés

ailleurs. Toutefois, dans la mesure où la bibliothèque de Prince William n'a pas l'intention de leur interdire l'accès aux stations de travail situées en dehors de la salle qui leur est réservée, les jeunes pourront continuer de faire sur l'Internet toutes les recherches qu'ils souhaitent effectuer. D'après les sondages menés localement, l'opinion publique semble, dans l'ensemble, favorable à une telle démarche, Prince William ayant pour l'instant réussi à éviter les controverses que l'on a connues dans la ville voisine de Loudoun.

4. La Gestion de la Liberté d'Expression

Bien que l'Internet appartienne à une nouvelle génération de médias qui est en train de bouleverser la communication dans le monde entier, il ne faut pas oublier qu'il ne nous est pas entièrement étranger. En effet, l'Internet a beaucoup en commun avec d'autres moyens de communication. Il lui faut des expéditeurs, tels que les créateurs de sites Web et autres fournisseurs de contenus, ou des correspondants de courrier électronique et des participants aux discussions de groupe. Les échanges se font par l'intermédiaire des ordinateurs et des liaisons de télécommunication. Il lui faut en fait des destinataires, autres usagers de l'Internet qui, avec une agréable circularité, sont également expéditeurs quand ils fournissent eux-mêmes des contenus, aussi fragmentaires soient-ils. Les messages véhiculés par l'Internet ne sont pas fondamentalement différents de ceux des autres formes de communication humaines, mais tout simplement plus riches, plus variés et plus aisément accessibles. Ce sont précisément la richesse et l'apparente étrangeté de l'Internet qui sont sources d'inquiétudes, voire de peurs. Et cette appréhension explique les appels lancés à une gestion de l'Internet dans l'intérêt de la protection des usagers, en particulier les jeunes.

Ces exhortations ont une incidence considérable sur les responsables de points d'accès publics, qui se sentent obligés de mettre au point des stratégies susceptibles d'apaiser les inquiétudes et les craintes du public, de ses représentants et des médias qui commentent la situation. Ils font appel ce faisant à des principes et à des interprétations élaborés pour traiter de formes passées et présentes de médias et de contenus. La validité de ces principes n'est pas fondamentalement remise en cause dans les circonstances actuelles, mais il faut décider de l'interprétation à leur donner par rapport aux nouvelles technologies. A notre avis, trois démarches principales s'offrent aux responsables de points d'accès publics aux réseaux, à savoir :

- la démarche réglementaire, le responsable se bornant alors à appliquer des lois et des règlements strictement interprétés;
- la gestion automatique, le responsable confiant alors le soin de décider à un système qui va se charger de filtrer et de bloquer l'accès à l'information selon des critères pré-établis;
- l'autogestion, démarche dans le cadre de laquelle le gérant va devoir élaborer des stratégies fondées sur des principes et assumer la responsabilité de ses décisions au cas par cas.

5.1 La démarche réglementaire

Cette stratégie équivaut à accepter que le rôle du gérant consiste, ni plus ni moins, à comprendre la loi et à en appliquer les exigences strictement et à la lettre. Une telle position est généralement adoptée par le gérant pour s'éviter toute marge de manœuvre sur les points au sujet desquels la loi ne dit rien ou est trop vague. Les conséquences d'une telle stratégie varient selon la nature des lois en vigueur en un lieu donné. Ainsi, aux Etats-Unis et dans certaines autres démocraties, la Constitution et la loi qui en découle prévoyant d'importantes libertés, c'est alors tout naturellement au gérant qu'il incombe de les protéger et de les défendre. La lutte de principe engagée par la *American Library Association* contre la CDA et la campagne qu'elle continue de mener contre le filtrage sont des exemples concrets d'actions pour la protection des libertés constitutionnelles, cet

organisme ayant choisi de prendre les devants plutôt que d'attendre passivement les orientations législatives. Dans des systèmes plus restrictifs comme celui de l'ex-Union soviétique ou les régimes autoritaires en place dans bien d'autres régions du monde, le rôle du gérant d'un point d'accès public aux réseaux peut fondamentalement se dégrader pour n'être plus que celui d'un administrateur de restrictions d'accès à l'information et de la liberté d'expression venues d'en haut.

Si une telle stratégie peut porter à croire à la supériorité d'une éthique fondée sur les libertés constitutionnelles, les solutions qu'elle apporte aux problèmes ne sont pas toujours simples. Ainsi, la position morale de la bibliothéconomie moderne n'est pas aussi claire qu'on le dit généralement. Dans la première moitié de ce siècle, elle a été dominée par un certain activisme incitant le bibliothécaire "à orienter la lecture et, par ce biais, à façonner la pensée de la collectivité tout entière" (Harris, 1976). Ce n'est que depuis une cinquante d'années que l'on assiste à l'apparition d'une philosophie axée plutôt sur la liberté d'expression et d'accès à l'information. Le premier principe directeur de la bibliothéconomie est aujourd'hui la lutte contre la censure, et non plus le souci de la qualité et de l'opportunité de l'information. L'un des grands facteurs ayant conduit à une telle évolution semble avoir été l'engagement des bibliothécaires américains dans la lutte contre les injustices de l'époque McCarthy. Parallèlement, on assistait en Grande-Bretagne à l'émergence d'une neutralité qui s'est exprimée au travers du "credo" du bibliothécaire : "pas de politique, pas de religion, pas de morale" (Foskett, 1962). Mais poussé à l'extrême, ce raisonnement revient à exonérer le bibliothécaire de toute décision d'ordre moral.

Les effets pratiques d'une foi aveugle en la liberté d'accès à l'information sont faciles à illustrer. En 1976, dans le cadre d'une expérience simple (Hauptman, 1976), Hauptman s'est rendu dans 13 bibliothèques pour se renseigner sur les propriétés chimiques de la cordite, en laissant fortement sous-entendre qu'il avait l'intention d'utiliser cette substance pour faire exploser une maison de banlieue. Chacun des bibliothécaires consultés s'étant plié à sa demande sans poser de questions, il en a conclu que ces derniers ne semblaient pas, ce faisant, avoir l'impression de faire un choix éthique. Les conclusions de Hauptman ont été contestées par certains, qui ont fait valoir, notamment, que les bibliothécaires " prenaient en fait un engagement éthique en choisissant de ne pas se renier " (Swan, 1982). Toutefois, il va sans dire qu'en choisissant de s'en remettre trop littéralement à des orientations extérieures, le gérant d'un point d'accès public à l'information peut en arriver à ne plus jouer d'autre rôle que celui qui consiste à appliquer passivement les décisions des autres. Il est important de ne pas oublier que, en fonction de la nature des influences externes subies, une telle position peut exposer les gérants aux ambiguïtés morales de la liberté, tout aussi bien qu'elle peut faire d'eux les agents d'un système de censure.

Dans un ou deux pays, dont la Grande-Bretagne et les Pays-Bas, par exemple, certaines instances ont été instituées pour servir d'intermédiaires entre les autorités chargées de faire appliquer la loi et les fournisseurs d'information. Ces entités peuvent aussi permettre au gérant de points d'accès publics de se défausser sur un organisme externe précis de toute responsabilité en matière de stratégie et de décision. Ainsi, la *Internet Watch Foundation* (IWF) en Grande-Bretagne gère un service téléphonique auquel le public peut s'adresser pour signaler les contenus de l'Internet qu'il estime contestables. En une année de fonctionnement de ce service, la IWF a reçu 781 signalements, concernant au total plus de 4300 cas, généralement liés à des sites de pornographie impliquant des enfants (Internet Watch Foundation, 1998a). Dans la moitié environ de ces cas, la Fondation a pu contacter le fournisseur de services Internet concerné, l'invitant à retirer les contenus jugés choquants. La IWF s' étant également intéressée aux questions d'accès, elle recommande l'utilisation du filtrage et de l'évaluation pour favoriser "la liberté d'expression sur le Net et la liberté de choix des consommateurs" (Internet Watch Foundation, 1998b). Comme nous le verrons au point suivant, le filtrage peut effectivement être bénéfique pour le consommateur, mais pas nécessairement pour l'usager d'un point d'accès public aux réseaux de l'information.

5.2 La gestion automatique

Le filtrage et le blocage automatiques de certains contenus de l'Internet constituent des moyens en apparence séduisants de résoudre les problèmes d'accès. Comme nous l'avons indiqué à plusieurs reprises dans le Vol. I, le principe des filtres n'est pas nécessairement contestable. L'idée de filtrer l'amas chaotique de ressources que contient l'Internet, que ce soit pour sélectionner les contenus que l'on souhaite réellement récupérer ou pour éliminer ceux que l'on souhaite éviter, est une réponse tout à fait valable au problème de la surcharge de l'information. Le fait d'installer des systèmes de filtrage au nom d'autrui, ce qu'un bibliothécaire par exemple peut être amené à faire, est également tout à fait raisonnable, pour autant que les desiderata d'autrui soient pleinement connus et aient fait l'objet d'un commun accord. Par contre l'installation de systèmes de filtrage au nom d'une collectivité tout entière, faite comme il se soit d'une multitude d'individus aux intérêts, aux goûts et aux sensibilités divers, comporte à l'évidence un risque d'atteinte à la liberté de tout ou partie des membres de cette collectivité.

Il va sans dire que le gérant d'un point d'accès public a besoin de pouvoir bénéficier d'orientations judicieuses sur la question du filtrage. Les cas évoqués au point 4.3 illustrent les problèmes que ce dernier peut poser, de même qu'ils montrent à quel point il est difficile de rechercher dans l'expérience de médias plus connus comme la presse des interprétations utilisables. L'exemple concret le plus intéressant est peut-être celui de la ville d'Austin, au Texas, suffisamment ancien désormais pour illustrer abondamment le " dialogue " entre principe et pratique. Ce cas montre également à quel point il y a beaucoup à faire si le gérant veut faire du filtrage plus qu'un simple moyen de tenir à distance le problème des contenus de l'Internet. Si l'on veut sérieusement faire en sorte que les adultes et les enfants aient légalement un accès aussi large que possible aux réseaux de l'information, alors il faut avoir une compréhension approfondie des systèmes de filtrage disponibles et apprendre à s'en servir correctement. Celui qui achète un logiciel de filtrage n'est pas toujours entièrement au fait des modalités de son fonctionnement, et éprouve parfois quelques difficultés à s'habituer à son mode d'emploi.

Dans son guide complet des filtres disponibles et de leurs conditions d'utilisation, Schneider (1997) précise qu'un filtre ne doit pas constituer la seule solution au problème et que son adoption suppose énormément de travail. Il s'agit tout d'abord de tester tout produit de filtrage dont on envisage l'acquisition. Ces essais doivent se dérouler dans le contexte où l'on prévoit d'utiliser le futur filtre et permettre d'en évaluer les performances en situation réelle. Comme pour la plupart des produits logiciels, Schneider a montré lors de ses travaux de recherche que les filtres disponibles sur le marché ont des performances parfois meilleures, parfois plus mauvaises que prévu, mais de toute façon, différentes par rapport aux attentes. Il ressort de ses études de cas sur l'usage des filtres dans un certain nombre de bibliothèques que, dans la mesure où ces dernières se dotent d'une stratégie d'ensemble en matière d'Internet, elles peuvent y intégrer le filtrage au niveau souhaité. Ainsi, elles peuvent décider d'installer un filtrage sur tous leurs ordinateurs, sur quelques-uns d'entre eux seulement, d'introduire certains éléments de filtrage dans un programme destiné, par exemple, à promouvoir l'usage de l'Internet par les enfants ou de préférer au filtrage d'autres dispositifs tels que les écrans privés sur certaines de leurs stations de travail. Les conseils et les détails que donne Schneider montrent bien que les filtres sont loin de constituer pour le gérant un moyen facile d'échapper à l'obligation pour lui d'assumer pleinement la responsabilité de ses choix en matière d'accès.

5.3 L'auto-administration

Il s'agit ici pour le gérant d'assumer la pleine et entière responsabilité de son administration de l'accès du public aux réseaux de l'information. Il n'est plus question alors de s'en remettre à une interprétation rigide des textes de loi et de réglementations imposées de l'extérieur, ni de dépendre de dispositifs qui exonèrent le gérant de la nécessité de prendre des décisions au cas par cas. Certes, c'est la stratégie la plus exigeante qui soit, supposant à la fois une certaine préparation et une vigilance de tous les instants. Pour ce qui est du premier point, il suffit pour le gérant d'élaborer des politiques en matière d'accès aux réseaux. Il doit par ailleurs faire preuve de

vigilance afin de pouvoir proposer en permanence une interprétation de la politique en vigueur en fonction des cas qui se présentent à lui. On retrouve les principes inhérents à cette démarche dans la philosophie des métiers de l'information et de la bibliothéconomie modernes, de même que, de manière implicite, dans la philosophie contemporaine de l'éducation.

S'agissant tout d'abord de ce dernier aspect, les préceptes ayant guidé la réforme et l'évolution de l'éducation tout au long de la seconde moitié de ce siècle placent l'enfant au cœur du processus d'apprentissage. Dans le cadre de cette démarche centrée sur l'enfant, on considère que le développement de l'écolier commence à des niveaux d'expérience très différents selon les cas, qui donnent lieu à des besoins uniques et particuliers en matière d'apprentissage. Puisque c'est finalement à l'enfant lui-même qu'il appartient de satisfaire ces besoins, l'enseignant doit s'abstenir de jouer les arbitres du processus d'apprentissage. Son rôle devient alors celui de conseiller et de soutien. Bien que cette philosophie soit régulièrement attaquée par les tenants d'une pédagogie plus traditionnelle, on retrouve ce respect du jeune apprenant dans tous les systèmes scolaires d'Europe et d'Amérique du Nord. Voici en quels termes une association d'enseignants, aussi traditionnelle soit-elle, formule son code déontologique par rapport à l'individualité de l'enfant :

> L'enseignant professionnel reconnaît l'individualité de chaque élève, respecte sa personnalité, favorise un environnement propice à l'éducation et à l'apprentissage, exerce son autorité avec compassion, veille à ce que ses actions disciplinaires ou autres mesures punitives soient constructives, s'abstient de prononcer des mots (ou de commettre des gestes) destructeurs ou négatifs et respecte la dignité de tous les intéressés (*Professional Association of Teachers*, 1988).

La reconnaissance de l'autonomie de l'apprenant individuel comporte un certain nombre de conséquences évidentes pour les enfants ayant des besoins particuliers en matière d'apprentissage, pour les minorités et pour les enfants en marge des centres d'éducation. De même, elle débouche tout naturellement sur le concept d'apprentissage tout au long de la vie, ou d'éducation permanente, sans parler de ses répercussions manifestes pour ce qui est de l'accès à une source d'autodidactisme telle que l'Internet. Cette philosophie se situe à l'opposé de la perception générale de l'apprenant défendue par ceux qui souhaitent une réglementation de l'accès à l'Internet. Dans ce derniers cas, les enfants sont considérés comme constituant l'objet (et le non le sujet) d'un processus d'apprentissage dirigé par les enseignants, avec le soutien et l'orientation des parents, où la connaissance est transmise à une cadence et à des niveaux déterminés au nom de l'enfant par le système. Les systèmes éducatifs actuels reconnaissent généralement que chaque individu apprend à sa manière, a des besoins différents en fonction des disciplines étudiées, progresse à son rythme et possède son propre degré de maturité affective. Il s'ensuit que les personnes chargées de gérer un outil d'apprentissage individuel tel que l'Internet doivent s'efforcer de laisser à l'apprenant la plus grande liberté possible, lui donnant les moyens d'utiliser le réseau en fonction de ses propres besoins.

Les bibliothécaires et autres professionnels de l'information reconnaissent également la place centrale de l'utilisateur de l'information, et ce parfois de manières totalement nouvelles. La politique de neutralité évoquée au point 5.1, si elle peut être synonyme d'acceptation passive d'un contrôle extérieur, a également pour objectif de donner aux individus le plus de liberté possible dans leur entreprise d'exploration. Les bibliothèques et les centres d'information progressistes reconnaissent qu'ils se doivent, non seulement de comprendre les besoins et les préférences changeants de leur public par la recherche, l'analyse et le suivi des résultats de leurs efforts, mais aussi d'utiliser ce savoir pour mettre en place des systèmes qui facilitent l'autonomie de "l'utilisateur final". Une telle position peut s'avérer inconfortable pour un professionnel dont le rôle a toujours été celui d'un intermédiaire, formé à trouver et à sélectionner des contenus pour autrui, mais elle ne diminue nullement l'importance du professionnel de l'information, dont l'usager a toujours besoin pour mener efficacement ses recherches et tirer le meilleur parti possible des

contenus qu'il aura trouvés.

Qu'il s'agisse de la vision de l'éducation centrée sur l'enfant ou de celle de la bibliothéconomie centrée sur l'utilisateur, ces deux perceptions évoquent la position traditionnellement adoptée par certaines professions, à savoir que le premier devoir du professionnel est celui qu'il a envers le client. Comme Hill (1997) le souligne, dans le cadre du travail de celui qu'il qualifie de professionnel moderne de l'information, il est parfois difficile de savoir qui de l'écolier, du parent ou du conseil scolaire, de l'usager de la bibliothèque ou de l'employeur du bibliothécaire, est en réalité le client. Cependant, la position de principe consiste à dire que le client est celui dont on cherche à satisfaire les besoins spécifiques. Il est courant pour les professionnels dans tous les domaines (médecine, droit, finances, etc.) de considérer que leur client a droit à un certain degré de confidentialité et à un traitement à l'égal des autres clients. Une telle position n'est pas sans comporter de répercussions si le professionnel de l'information considère un jeune comme un client. En effet, il se pose alors la question de savoir à quel moment les opinions du parent priment sur celle de leur enfant, et vice-versa. Il semblerait que, dans bien des cas, le professionnel de l'information privilégie les préférences exprimées par l'enfant, avec toutes les conséquences qu'un tel choix pourrait avoir en ce qui concerne l'usage de l'Internet.

Dans son exposé sur l'éthique de l'information, Hill fait notamment allusion à deux principes essentiels au débat sur les points d'accès publics à l'Internet :

- un professionnel moderne de l'information doit en tout temps défendre et promouvoir le droit à la liberté de l'information lorsqu'il s'agit d'accès à l'information et de communication d'informations à des tiers;

- un professionnel moderne de l'information ne doit pas tenter de censurer ou de dissimuler d'information, à moins qu'il n'y soit contraint par la loi ; même dans ce cas, il doit s'en abstenir si un tel choix est contraire aux droits de l'homme universellement acceptés.

Bien que la formulation des ces propositions de principes ne soit pas des plus claires, leur intention générale est évidente et susceptible d'être largement acceptée par les professionnels de l'information. Ils obligent notamment le gérant à assumer l'entière responsabilité de son point d'accès public sans s'en remettre, pour la définition de sa stratégie, à une forme quelconque de réglementation extérieure ou, pour la gestion au quotidien, à une forme quelconque de dispositif électronique.

6. Conclusion de la Deuxieme Partie

Dans le présent Volume, nous avons cherché à savoir comment il convient de gérer les points d'accès aux réseaux de manière à offrir au public un accès vraiment aussi large et complet que possible à l'information mise à sa disposition sur les réseaux électroniques. Le problème que nous avons évoqué ici concerne les contenus illégaux ou préjudiciables dont le prétexte est invoqué pour justifier la mise en place de restrictions d'accès. Certains aspect importants, tels que la question de savoir comment les gouvernements peuvent assumer les coûts d'une démocratisation de l'accès aux réseaux ou celle qui consiste à déterminer comment on peut mettre à la disposition du public des contenus qui répondent aux besoins de toutes sortes d'individus, quel que soit leur sexe, de leur situation sociale, de leur langue et de leur culture, n'ont pas été abordés ici. Nous mentionnerons simplement que le dossier des contenus illégaux et préjudiciables est indissociable de celle de l'accès des jeunes à l'Internet.

Compte tenu des problèmes développés dans les quelques sections précédentes de ce Volume et dans une grande partie du Vol. I, on peut tirer plusieurs conclusions :

1. le gérant doit accepter la responsabilité de la manière dont il donne

accès aux réseaux électroniques de l'information;

2. les lois et les réglementations nationales et internationales offrent un certain nombre de cadres de travail, mais elles ne dégagent en rien le responsable de son obligation de prendre des décisions en matière de gestion;

3. le filtrage ne remplacera jamais une gestion éclairée et suivie des installations et des équipements ;

4. les principes professionnels donnent au gérant des orientations générales quant la manière dont il doit se comporter, mais ils doivent être faire l'objet d'interprétations au cas par cas;

5. il faut une politique en matière d'accès à l'Internet, qui guide le gérant et signale aux usagers les paramètres à l'intérieur duquel l'accès aux réseaux leur est offert.

Si la nécessité d'une politique figure ici en dernière position sur la liste, elle constitue pourtant l'élément le plus important d'une bonne gestion des points d'accès publics. Armé d'une politique pleinement acceptée par toutes les parties en présence et clairement affichée, le gérant peut aborder les différents problèmes susceptibles de se poser, avec la certitude que ses décisions seront fondées. Pour ce qui est de l'élaboration de cette politique en matière d'accès à l'Internet, il lui est possible de se tourner dans un certain nombre de directions, notamment la législation national, les buts et les objectifs de l'institution à laquelle il appartient et les codes de déontologie. Il est également essentiel d'avoir pour commencer par une parfaite connaissance des normes, des besoins et des préférences de la collectivité, autant d'informations qu'il est possible de recueillir à l'occasion d'enquêtes spéciales et de trouver en consultant des sources déjà publiées ou par ailleurs disponibles.

Cet exercice de formulation d'une politique ne doit pas se faire de manière isolée. Il existe de nombreuses sources d'information que l'on pourra utilement consulter pour connaître les éléments que d'autres institutions ont choisi d'inclure dans leurs propres politiques (voir à la fin de ce Volume la liste des sites d'information sur les politiques relatives à l'Internet). Il existe également un certain nombre de publications sur le processus même d'élaboration d'une politique (Fishman et Pea, 1994; Campbell, 1998). Les partenariats avec les associations de parents, avec les organisations professionnelles, avec les organisations non gouvernementales œuvrant dans le domaine de l'éducation et de la protection de l'enfance et avec d'autres instances compétentes, jouent un rôle important lorsqu'il s'agit de rédiger une politique qui soit acceptable pour le plus grand nombre. Certaines de ces organisations sont mentionnées dans le Volume I, Section 6.3, tandis que les sites Web pertinents sont indiqués dans la liste figurant à la fin du Volume I.

Les principaux éléments à prendre en compte dans la formulation d'une politique sont les suivants : la définition de la collectivité à desservir, ses caractéristiques et ses besoins, les facteurs qui influent sur ses attitudes à l'égard de l'accès à l'information et l'incidence des lois et des réglementations. Il est important de bien comprendre quels sont les organismes ou individus réputés responsables des contenus consultés : les fournisseurs de contenus, les fournisseurs de services d'information, les usagers eux-mêmes ou les gérants de points d'accès publics. La politique élaborée doit évoquer la mesure dans laquelle le point d'accès public fera état de sa propre responsabilité par des mesures telles que l'inscription et la formation des usagers, l'affichage d'avertissements ou d'écrans de mise en garde, l'obligation pour les usagers de signer des déclarations indiquant qu'ils assument l'entière responsabilité de leur utilisation du système, l'aménagement des stations de travail, la surveillance des zones en accès public ou le recours au filtrage. Cette politique devra également aborder des points tels que les actions à mener en cas d'atteintes aux règlements et la conduite à tenir en cas de protestations relatives aux contenus

récupérés par les usagers. Toute institution ayant des jeunes dans sa clientèle doit veiller à ce que les questions pertinentes tels que la mesure dans laquelle elle agit *in loco parentis* soient pleinement prises en compte.

La politique de l'établissement peut être considérée comme un document public à part entière, ou alors, elle peut servir de guide pour l'élaboration de lignes directrices à l'intention du public. Etant donné que l'on s'adresse à deux publics différents (bailleurs de fonds, collègues, organismes chargés de faire appliquer la loi, groupes de pression, etc. d'un côté, et usagers de l'autre), il est probablement préférable de disposer de deux textes différents. Le document interne pourra donner le contexte et l'argumentation, tandis que celui destiné à l'usage du public sera fait de déclarations brèves et claires faisant état de ce que propose le point d'accès public et de la conduite attendue de l'usager. La compilation des principaux éléments contenus dans un total de 72 documents de politique en matière d'accès à l'Internet destinés au public montre que l'on retrouve dans la plupart d'entre eux, sinon la majorité, certaines déclarations types (Lake Oswego Public Library, 1996). Il ne s'agit pas nécessairement des éléments les plus pertinents à mettre en relief, mais la compilation fournit au moins une indication des tendances qui se dégagent de la manière dont les politiques sont présentées à l'usager.

Il s'agit le plus souvent de décharges et d'avertissements; ainsi, on met en garde l'usager contre le fait qu'il est susceptible de trouver sur l'Internet des contenus inconvenants ou choquants (57%); des clauses d'exonération de responsabilité pour les contenus que l'usager est susceptible de trouver (79%); et des déclarations de responsabilité parentale pour ce que les enfants sont susceptibles de trouver (58%). Dans un grand nombre de documents, on trouve aussi des avertissements généraux quant aux sanctions que l'usager encourt en cas d'atteinte au règlement (43%), de même que l'on attire l'attention de l'usager sur certains comportements précis faisant l'objet d'une interdiction, au nombre desquels les atteintes aux droits de propriété intellectuelle (32%) ou à la sécurité du système (35%) et autres types d'actes illicites (35%). Une série d'autres thèmes sont également mentionnés, mais moins fréquemment. Il s'agit notamment des durées maximales d'utilisation des stations de travail, de l'obligation faite à l'usager de signer une sorte de règlement sur les pratiques acceptables, de l'interdiction d'amener ses propres logiciels ou de harceler les autres, etc.

En dépit du volume de travail d'ores et déjà accompli en matière d'élaboration de politiques par les institutions offrant des points d'accès publics aux réseaux et du nombre de documents de politique générale publiés à l'usage du public, il reste beaucoup à faire dans ce domaine. Il est indispensable de disposer de politiques très solides si l'on veut pouvoir assurer la défense de la liberté d'expression et d'accès à l'information contre la censure ou contre les débordements des systèmes de filtrage. Il s'agit d'adopter une démarche positive à l'égard de la fourniture d'un accès public aux réseaux, sans borner à vouloir le défendre contre les pressions extérieures. Il convient en premier lieu de bien comprendre les raisons pour lesquelles on choisit d'offrir cet accès et de faire état de cette compréhension dans un document étayé par de solides arguments. Telle est la meilleure défense qui soit.

La formulation des politiques est le domaine dans lequel le Conseil de l'Europe peut intervenir le plus utilement, par le biais de l'élaboration de lignes directrices fondées sur les principes qu'il a vocation à défendre. Ces lignes directrices seront utiles aux gouvernements qui envisagent une législation ou une réglementation de l'accès public à l'Internet. Elles aideront également les responsables de points d'accès publics à formuler des politiques adaptées à leurs propres circonstances.

Bibliographie de la Premiere Partie

ACLU (1997) Fahrenheit 451.2: Is cyberspace burning? www.aclu.org/issues/cyber/burning.html

ALA (1986) Intellectual Freedom Committee. *Books/materials challenge terminology*. Chicago: ALA.

Ang, P.H. and Nadarajan, B. (1996) Censorship and the Internet: a Singapore perspective. *Communications of the ACM* 39, 6. pp.72-78.

Arthur, C. (1997) Ratings plan for Internet sparks censorship fears. *Independent* (UK) Oct. 6th.

Atton, C. (1996) Anarchy on the Internet. *Anarchist Studies* 4. pp.115-132.

Barme, G. and Ye, S. (1997) The great firewall of China. *Wired* 5.06 www.wired.com/wired/5.06/china.html

Bennahum, D.S. (1997) The Internet revolution. *Wired* 5.04

http://www.wired.com/wired/5.04/internet.revolution.html

Borger, J. (1997) Hamas accused of using Internet as terror tool. *Guardian* (UK) Sept. 27th.

Branch, B. and Conable, G. (1997) To filter or not to filter. *American Libraries* Aug. pp.100-102.

Burt, D. (1997) In defense of filtering. *American Libraries* Aug. pp.46-48.

Capitanchik, D. and Whine, M. (1996) *The governance of cyberspace: racism on the Internet*. London: Institute for Jewish Policy Research.

Carol, A, (1996) A feminist argument against censorship. www.fiawol.demon.co.uk/FAC

Cavazos, E.A. and Morin, G. (1994) *Cyberspace and the law*. Cambridge, Mass: MIT Press.

Censorware Search Engine (1997) *Netly News*. http://cgi.pathfinder.com

Cormack, A. (1997) Web security. www.niss.ac.uk/education/jisc/acn/authent/cormack.html

Cyber-Rights (1997) and Cyber-Liberties (UK) Who watches the watchmen: Internet content rating systems and privatized censorship. www.leeds.ac.uk/law/pgs/yaman/watchmen.html

Dempsey, L. and Heery, R. (1998) Metadata: a current review of practice and issues. *Journal of Documentation* forthcoming.

Diamond, E. and Bates, S. (1995) Law and order comes to cyberspace. *MIT Technology Review* 98. Oct. pp.22-33.

Dority, B. (1997) Ratings and the V-chip. *The Humanist* May/June pp.16-19.

Elliott, C. (1995) Paedophiles on the Internet use codes to avoid detection. *Guardian* (UK) Nov. 21st.

Elmer-DeWitt, P. (1995) On a screen near you. Its popular, pervasive and surprisingly perverse. *Time International* July 3rd. p.38.

European Commission (1996). Illegal and harmful content on the Internet. www2.echo.lu/legal/en/internet/wp2en.html

European Commission (1997) Action plan on promoting safe use of the Internet. www2,echo.lu/legal/en/internet/actpl-cp.html

Family Research Council (1997). Press release. June 26th. www.ciec.org/SC-appeal/970626-FRC.html

Faucette, J.E. (1995) The freedom of speech at risk in cyberspace. *Duke Law Journal* 44. pp.1155-1182.

First Report (1997) on UK Encryption Policy. Cyber-Rights and Cyber-Liberties (UK). www.leeds.ac.uk/law/pgs/yaman /ukdtirep/htm

Great Sites (1997). www.ala.org/parentspage/greatsites/amazing.html

Hoffman, D.L. and Novak, T.P. (1995) A detailed critique of the Time article 'On a screen near you'. www.hotwired.com/special/pornscare/hoffman.html

Internet censorship (1997) and freedom of expression. www.surfwatch.com/surfwatch/censorship.html

Jeffreys, D. (1997) Do we want our schools linked to a world that obeys no law? *Daily Mail* (UK) Oct 6th.

Jellinek, D. (1997) Beyond the bamboo cybercurtain. *Guardian* (UK) Nov. 27th.

Kadie, C.M. (1994) Applying library intellectual freedom principles to public and academic computers. www.eff.org/CAF

/cfp94.kadie.html

Katz, I. (1997) Internet escapes censor's web. *Guardian* (UK) Nov. 7th.

Kleiner, K. But who guards the guards? *New Scientist* Mar. 29th. p.50.

Kuner, C, (1996) Federal law to regulate the conditions for information and communication services.

http://ourworld.compuserve.com/homepages/cjuner/multimed1.htm

Langford, D. (1995) Law and disorder in Netville. *New Scientist* June 17th. pp.52-53

Lappin, T. (1996) Cyber rights now. *Wired* 4.05 www.wired.com/wired/4.05/cyber.rights.html

Lasica, J.D. (1997) Censorship devices on the Internet. *American Journalism Review* July 19th. p.56.

Lessig, L. (1997) Tyranny in the infrastructure: the CDA was bad, but PICS may be worse. *Wired* 5.07. www.wired.com/5.07/cyber-rights.html

Librarians' Guide (1997) to cyberspace for parents and kids. www.ala.org/parentspage/greatsites/safe.html

McMurdo, G. (1997) Cyberporn and communication decency. *Journal of Information Science* 23, 1. pp.81-90.

Makkula Center (1997) for Applied Ethics. Access, Internet and public libraries. www.scu.edu/ethics/practicing/focusareas /technology/libraryaccess/

Marshall, J.M. (1997) Internet ratings bureaus: how many will there be? *Internet Legal Practice Newsletter* 2. www.collegehill.com/ilp-news/

Mason, M.G. (1997) Sex, kids and the public library. *American Libraries* June/July. pp.104-106.

New FBI Draft (1997) encryption legislation. www.cdt.org/crypto/fbi_draft_text.html

Newey, A. Networking for God. *Index on Censorship* 4. pp.132-137.

Parents (1996) and the Information Superhighway: an action sheet for getting involved. www.childrenspartnership.org/bbar/pbpg.html

Pedlars (1996) of child abuse: we know who they are. *Observer* (UK) Aug. 25th.

Perkins, M. (1997) Barriers to technical solutions. *IFLA Journal* 23. pp.23-29.

Policing the Internet: (1997) *Conference Report*. London: Association of London Government.

Recommender systems. (1997) Special section. ed. Resnick, P. and Varian, H.R. *Communications of the ACM* 40. Mar. pp.56-89.

Resnick, P. and Miller, J. (1996) PICS: Internet access controls without censorship. *Communications of the ACM* 39. Oct. pp.87-93.

Resnick, P. (1997) Filtering information on the Internet. *Scientific American* Mar. pp.54-56.

Right turn (1995) in cyberspace. *Economist* Aug. 26th. pp.77-78.

Robot as censor (1997). *IBM Networked World*. www.ibm.park.org/censor2.html

Rodriguez, F. (1997) Bad thing: Policing the Internet. www.teleport.com/room101/badthing/police.htm

Safeguards (1997) library alert. www.enough.org/safeguards_lib.htm

Shea, V. (1994) *Netiquette*. San Francisco: Albion Books.

Smith, G. (1996) *Internet law and regulation*. London: FT Law and Tax.

Sterling, B. (1992) *The hacker crackdown*. New York: Bantam.

Usdin, S. (1997) The great firewall of China. *Computer Life* 23. Mar. pp.44-47.

UK JET Report Controversy. (1997) Cyber-Rights and Cyber-Liberties (UK). www.leeds.ac.uk/law/pgs/yaman/htm

Vitiello, G. (1997) Freedom of expression online. *Focus* 28.

Wallace, J. and Mangan, M. (1996) *Sex, laws and cyberspace*. New York: Henry Holt and Co.

Wallich, P. (1997) Parental discretion advised. *Scientific American* Aug. p.21.

Watson, D. (1997) Internet censorship: demands for content controls. *Library Association Record* 99, 12. p.638.

Winner, L. Electronically implanted values. *MIT Technology Review* 100. p.69.

Wolf, C.J. (1994) Developing a school or district 'Acceptable Use Policy' for student and staff access to the Internet. gopher://inspire.ospi.wednet.edu:70/00/accept_use_policies/IN_policies.txt

---

Bibliographie de la Deuxieme Partie

Annual Internet Survey (1998). *Which? Online*. www.which.net/nonsub/special/ispsurvey/foreword.html

Berry, J.N. (1998) Practising free expression. *Library Journal* 123, 7. p.6.

Blamire, R. (1998) The information rich and the information poor: avoiding a new divide in Britain. In: Carr, J. and Mullins, A. (eds.) *Children on the Internet: opportunities and hazards*. London: NCH Action for Children. pp.7-11.

Branch, B. and Conable, G. (1997) To filter or not to filter. *American Libraries* 28, 8. pp.100-102.

Burt, D. (1997) In defense of filtering. *American Libraries* 28, 8. pp.46-48.

Campbell, S. (1998) Guidelines for writing children's Internet policies. *American Libraries* 29, 1. pp.91-92.

Censorship ruling (1998). *Library Association Record* 100, 5. p.238.

Child porn (1998) verdict stuns Net lawyers. *Guardian* (UK) 29th May.

Children's attitudes (1998) *towards teachers and school environment: a research study among 11-16 year olds*. London: Association of Teachers and Lecturers.

Coping with challenges (1996). Chicago: American Library Association.

Council of Europe (1998) *Draft recommendation No. R (97) on a European policy on access to archives*. Strasbourg: Council of Europe.

Cyber Patrol (1998) in Austin Public Library. www.realtime.net/~bladex/apl/apl.htm

Federal Republic of Germany (1997). *Information and Communication Services Act*. Bonn: Federal Parliament. www.iid.de/rahmen/iukdgebt.html

Doyle, R.P. (1997) *Books challenged or banned 1997*. Chicago: American Library Association.

European Commission (1998). Recommendation on the Protection of Minors and Human Dignity in the Audiovisual and Information Services. http://europa.eu.int/en/comm/dg10/avpolicy/new_srv/comlv-en.htm

Fishman, B.J. and Pea, R.D. (1994) The Internetworked school: a policy for the future. *Technos: Quarterly for Education and Technology* 3, 1. pp.22-26.

Flagg, G. (1998) Senate Committee approves Filtering Bill. *American Libraries* 29, 4. p.13.

Foskett, D.J. (1962) *The creed of a librarian*. London: Library Association.

Harris, M. (1976) Portrait in paradox: commitment and ambivalence. *Libri* 26, 4. pp.281-301.

Hauptman, R. (1976) Professionalism or culpability? An experiment in ethics. *Wilson Library Bulletin* 50, 8. pp.626-627.

Hill, M. (1997) Facing up to dilemmas: conflicting ethics and the modern information professional. *FID News Bulletin* 47, 4. pp.107-117.

Internet censorship (1997) and freedom of expression. www.surfwatch.com/surfwatch/censorship.html

Internet Watch Foundation (1998a) *First annual report December 1996-November 1997*. www.iwf.org.uk/about /annual97.htm

Internet Watch Foundation (1998b) *Rating and filtering Internet content: a United Kingdom perspective*. www.iwf.org.uk/label/index.htm

Lake Oswego Public Library (1996) *Internet policies: tables*. www.ci.oswego.or.us/library/politab.htm

Lamont Johnson, D. (1996) Finding the middle ground in the debate of Internet censorship in the public schools. *Computers in Schools* 12, pp.1-5.

Lasica, J.D. (1997) Censorship devices on the Internet. *American Journalism Review* 19th July. p.56.

Library Bill (1996) *of Rights*. www.ala.org

Miller, J. (1994) *The street of the pied piper*. Derby: Professional Association of Teachers.

Ministerial Conference (1997) on Global Information Networks. 6-7 July 1997. *The Bonn Declaration*.

Nation divided (1997) into IT haves and have-nots. *Guardian* (UK) 22nd October.

New Library: (1997) *the people's network*. London: Library and Information Commission.

Oder, N. (1998) Intellectual freedom legislation: the state of the States. *Library Journal* 123, 6. pp.54-57.

Professional Association of Teachers (1988) *Code of professional conduct*. Derby: Professional Association of Teachers.

Questions and answers (1997) *Access to electronic information, services and networks: an interpretation of the Library Bill of Rights*. Chicago: American Library Association.

St. Lifer, E. (1998) McCain Filtering Bill draws support despite misperceptions. *Library Journal* 123, 5. p.14.

St. Lifer, E. and Rogers, M. (1998a) Despite Federal filtering fight, PLs are handling it locally. *Library Journal* 123, 4. pp.12-13.

St. Lifer, E. and Rogers, M. (1998b) Judge: Loudoun challenge to filtering policy can proceed. *Library Journal* 123, 8. p.12.

Schuyler, M. (1997) When does filtering turn into censorship? *Computers in Libraries* 17, 5. pp.34-38.

Schneider, K.G. (1997) *A practical guide to Internet filters*. New York: Neal-Schuman.

Swan, J.C. (1982) Ethics at the reference desk: comfortable theories and tricky practices. *Reference Librarian* 4. pp.99-116.

Thorhauge, J. et al. (1997) *Public libraries and the information society*. Luxembourg: European Commission DGXIII.

Quelques Sites Web

Acceptable Use Policies of Selected Internet Service Providers: http://www.jmls.edu/cyber/statutes

> Very full list of the policies of the main ISPs.

American Civil Liberties Union: http://www.aclu.org

> Led campaign against CDA. Site has documents.

American Library Association: http://www.ala.org

> The best site for documents on library-related aspects.

America Online (AOL): http://www.aol.com/nethelp/news/newsnetiquette.html

> Sets out AOL's policy on acceptable use.

Bluehighways: http://www.bluehighways.com

> Has The Internet Filter Assessment Project (TIFAP) and other documents.

Campaign for Internet Freedom (UK): http://www.netfreedom.org

> The site that was closed down for carrying 'dangerous' material.

Censorship and Intellectual Freedom Page: http://php.indiana.edu/~quinnjf/censor.html

Provides links to many other relevant sites and Usenet groups.

Censorware Search Engine: http://cgi.pathfinder.com

Reports on filtering products, but some doubts about reiability.

Center for Democracy and Technology: http://www.cdt.org

Advocates public policies advancing civil liberties in the networked environment.

Child Safety on the Information Highway: http://www.4j.lane.edu/safety/childtoc.html

The National Center for Missing and Exploited Children's brochure, on the site of Eugene, Oregon, School District.

Citizens Internet Empowerment Coalition: http://www.ciec.org

Organization formed to campaign against the CDA.

Computer & Information Ethics Resources on WWW: http://www.ethics.ubc.ca/papers/computer.html

Canadian site with many links.

Computer Professionals for Social Responsibility: http://cpsr.org/dox/cpsr/about-cpsr.html

Presents the computer professional's approach.

Computers and Academic Freedom; http://www.eff.org/CAF

Has extensive archive relating to the academic community and the Internet.

CyberPatrol: http://www,microsys.com

Site for a leading filtering product.

Cyber-Rights & Cyber-Liberties (UK): http://www.leeds.ac.uk/law/pgs/yaman/yaman.htm

Many links and documents, and a regular Cyber-Rights & Cyber-Liberties Newsletter.

CyberSpace Law Center: http://www.cybersquirrel.com/clc/expression.html

Has many links to other sites and documents on this and other law-related topics.

Electronic Frontier Foundation: http://www.eff.org

Many links and extensive archives on the site of the major libertarian campaigning body.

Electronic Privacy Information Center: http://epic.org

Site has many basic legislative documents.

Electronic Rights and Ethics: http://www.zip.com.au/~pete/ere.html

Developing an ethical standard for the Internet.

Enough is Enough: http://www.enough.org

Has materials for campaign to promote filtering in libraries.

Ethical Spectacle: http://www.spectacle.org

Online magazine covering ethical issues generally, and Internet censorship particularly.

Families Against Internet Censorship: http://shell.rmi.net/~fagin/faic

Accepts filtering as part of an anti-censorship programme.

Family Friendly Libraries http://www.fflibraries.org

Opposes social involvement of ALA (particularly on gay issues).

Filtering and Censorware in Libraries: http://www.geocities.com/Athens/Delphi/7382

Anti filtering site.

Filtering: http://www.filteringfacts.org

Site supporting filtering in libraries. Has links to other similar sites, articles and details of filtering products.

First Amendment Cyber-Tribune: http://w3.trib.com/FACT/

Monitors freedom of expression issues worldwide.

Global Internet Liberties Campaign: http://www.gilc.org

International campaigning organization for human rights on the Internet.

Internet Content Register: http://www.internet.org.uk/icop.html

Promoters of the Internet Code of Practice (ICOP).

Internet Content Coalition: http://www.netcontent.org

Represents major media companies providing Internet content.

Internet Watch Foundation: http://www.iwf.org.uk

UK industry self-regulatory body.

Library Watch: http://netwinds.com/library

An online magazine opposing the ALA stand on censorship.

Markkula Center for Applied Ethics: http://www.scu.edu/ethics

Has the report on Access, Internet, and Public Libraries.

MIT SAFE: http://www.mit.edu/activities/safe

MIT student organization against censorship which links to sample newsgroups.

National Campaign to Combat Internet Pornography: http://www.nccip.org

Mostly about pornography, but discusses attitude to the Internet.

Netparents: http://www.netparents.org

Much information on filtering and rating.

Peacefire: http://www.peacefire.org

Student group's site, with links and documents.

People Against Pornography: http://earth.vol.com/~shark//pap.html

Christian site, mainly concerned with pornography as such.

PICS: http://www.w3.org/PICS

The official site describing and promoting PICS.

Pippin Central: http://www.pippin.com/indexen.html

Offers guidance on safe Internet use for children.

Recreational Software Advisory Council: http://www.rsac.org

Responsible for RSACi rating system.

Robbinsdale, Minnesota, School District: http://www.eta.K12.mn.us/~WMrdale/281.html

Very full list of school acceptable use policies, plus related documentation.

SurfWatch: www.surfwatch.com

(*Editorial note: January 2001: SurfWatch has recently been acquired by SurfControl and they have merged their Web sites: www.surfcontrol.com)*

Promotes the product as a means to fight Internet censorship.

VF-INFOethics: http://www.de3.emb.net/infoethics/start.html

Site based at the University of Constance, Germany, with links to many other sites.

WEBHITZ: http://web.sbtcorp.com/infostar/wd34.htm

Links to sites related to parental control of Internet use.

Wired: http://www.wired.com

Journal with many relevant articles.

Politiques Relatives a l'Internet

Public Library Internet Access Policies: http://www.ci.oswego.or.us/pol-ci.htm

Lake Oswego Public Library collection of policies from 126 libraries.

Rice University Collection of K-12 Policies: Gopher://riceinfo.rice.edu:1170/11/More/Acceptable

Contains policies and documents relating to creating policies.

Robinsdale, Minnesota, School District: http://www.eta.K12.mn.us/~WMrdale/281.html

Very full list of school acceptable use policies, plus related documentation.

Technology and WWW Policies: http://www.cc.colorado.edu/Library/Current/wwwpol.html

Collection of academic policies and links to other collections.

World-Wide Web Guidelines: http://cspmserver.gold.ac.uk/guidance.html

Mainly British academic policies.