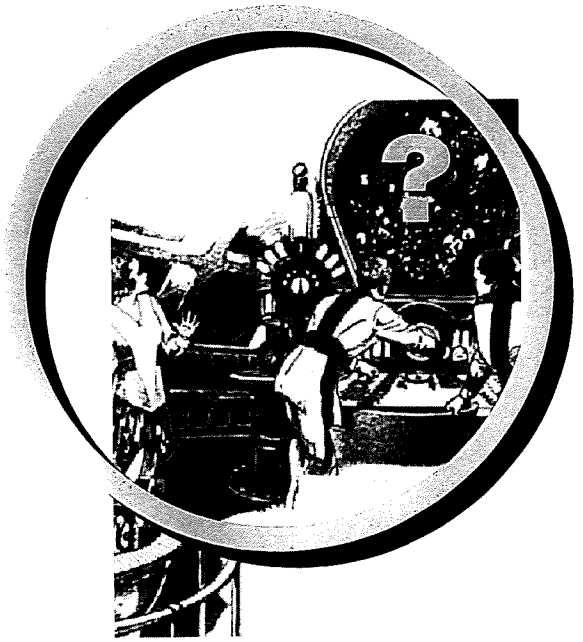
La métaphore de l'autoroute électronique désigne une structure planétaire émergente d'information et de communication. Elle est directement issue du téléphone, de la câblodistribution et de l'Internet. Ce livre veut contribuer à la meilleure compréhension de certains enjeux que soulève l'avènement de ces lieux de communication aux dimensions mondiales. On y traite de l'environnement des autoroutes électroniques et présente un aperçu de l'Internet, et des autres environnements électroniques comme la télévision interactive. On examine les exigences relatives à la sécurité. On expose comment la facilité de communication, la mémoire de masse et les *liens hypertextes* modifient les perspectives de l'enseignement du droit et de la recherche juridique et on pose en des termes inédits la question de la viabilité de l'édition électronique.

Enfin, l'ouvrage traite des principales questions juridiques soulevées par l'émergence de l'autoroute électronique, au fur et à mesure que celle-ci prend forme dans des environnements comme l'Internet. Dans cette optique, le droit ne vise pas à dire aux usagers ce qu'ils peuvent ou ne peuvent faire mais plutôt à cerner ce qu'ils pensent pouvoir légitimement faire ou ne pas faire afin de formuler des règles dont ils peuvent s'accommoder. En somme, cet ouvrage présente l'aménagement de l'autoroute électronique comme un défi que nous pouvons et devons relever.

LES AUTOROUTES ÉLECTRONIQUES
usages, droit et promesses



LES AUTOROUTES ÉLECTRONIQUES

usages, droit et promesses

Sous la direction de
Daniel Poulin, Pierre Trudel et Ejan Mackaay

LES ÉDITIONS YVON BLAIS INC.

Données de catalogage avant publication (Canada)

Vedette principale au titre:

Les autoroutes électroniques: usages, droit et promesses

Textes présentés lors d'un colloque tenu à Montréal le 13 mai 1994.

Comprend des réf. bibliogr.

ISBN 2-89451-022-5

1. Autoroutes électroniques – Droit – Congrès. 2. Autoroutes électroniques – Congrès. 3. Télécommunications – Coopération internationale – Congrès. 4. Information. Réseau d' – Congrès. 5. Internet (Réseau d'ordinateurs) – Congrès. I. Poulin, Daniel, 1954- . II. Trudel, Pierre, 1952- . III. Mackaay, Ejan, 1943- .

K4304.6 1994 343,0994 C95-940675

Graphisme: Tamanoir & Pangolin

Composition: Sylvie Thériault

© Les Éditions Yvon Blais Inc., 1995

Toute reproduction d'une partie quelconque de ce volume par quelque procédé que ce soit est strictement interdite sans l'autorisation écrite de l'éditeur.

Dépôt légal: 2e trimestre 1995
Bibliothèque nationale du Québec
Bibliothèque nationale du Canada

ISBN: 2-89451-022-5

La protection des droits et des valeurs dans la gestion des réseaux ouverts*

Pierre Trudel
et Robert Gérin-Lajoie

INTRODUCTION

Comme toute évocation, l'idée d'autoroute électronique possède une puissante vertu métaphorique. Les milliers d'unités d'information circulant à grande vitesse sur des voies à haute capacité! L'effet mobilisateur de la métaphore compte sans doute pour beaucoup dans le succès qu'elle obtient. Quoi de plus enthousiasmant, en cette époque de stagnation de l'économie que ce projet symbolisant une nouvelle vague industrielle et son cortège de promesses et d'espoirs! Il est toutefois opportun de dégager systématiquement de quelle manière, en contexte canadien, se présente le défi d'assurer le respect des droits des personnes ainsi que les valeurs fondamentales mises en cause par la circulation de l'information dans les réseaux ouverts.

* Cette étude a été réalisée dans le cadre du programme de recherche du CRDP sur le cadre juridique des systèmes d'information électronique. Ce programme a bénéficié d'une aide financière du Conseil de recherches en sciences humaines du Canada. Les auteurs tiennent à remercier Me France Abran, agente de recherche au Centre de recherche en droit public et Daniel Poulin, professeur au même Centre, pour les commentaires qu'ils ont formulés sur une version antérieure du présent texte.

Ce n'est pas parce que l'espace cybernétique transcende les frontières nationales et permet l'existence de lieux virtuels[1] à l'échelle de la planète que disparaissent les inquiétudes découlant de la circulation de matériel pornographique, de la propagande haineuse, du piratage des oeuvres protégées ou de la dissémination d'informations relatives à la vie privée. D'une manière ou d'une autre, il faut identifier les moyens de résoudre les contradictions qui font naître les conflits découlant de la circulation d'information et de comportements manifestés dans les réseaux ouverts.

Le droit encadre les phénomènes nouveaux à partir des analogies que présentent ces derniers avec des situations déjà connues. Le droit actuel possède déjà un ensemble de principes destinés à régir les diffusions et les échanges d'information. L'objet de la recherche juridique est justement d'identifier comment ces principes s'appliquent à des situations nouvelles.

Mais les techniques et approches traditionnellement utilisées pour réguler la circulation des informations dans les espaces publics doivent être revus afin de déterminer la mesure dans laquelle ils sont toujours susceptibles de procurer les équilibres nécessaires entre le besoin de circulation d'information et la protection des droits des personnes ainsi que la préservation des valeurs fondamentales des sociétés démocratiques. L'objet de ce texte est de décrire comment se pose la question de la protection des valeurs chères à nos sociétés pluralistes et démocratiques et des droits des personnes dans le contexte des réseaux ouverts de communication électronique.

La circulation de l'information engendre des interactions entre les sujets. De ce fait, elle peut générer des conflits. Les normes visent le plus souvent à fournir les solutions aux conflits susceptibles de se présenter. Les réseaux sont à la fois des lieux de diffusion, de communication et de transaction. Ils supposent la mise en place, par voie autoritaire ou spontanée, d'une bienséance, de normativités et de règles mutuellement consenties. Ainsi, la question n'est pas tant de savoir s'il y aura des normes qui encadreront le fonctionnement des autoroutes électroniques mais plutôt quelle sorte de normes sont

1. Di Lello explique que : «"virtual" is a term of art in computer technology, signifying the phenomenon of something purely electronic substituting for a physical object or event». Voir : Edward V. DI LELLO, «Functional Equivalency and Its Application to Freedom of Speech on Computer Bulletin Boards», [1993] 26 *Columbia Journal of Law and Social Problems*, 199, p. 216.

susceptibles de se développer pour assurer l'équilibrage entre les différents droits et les valeurs venant en conflit.

Perritt identifie trois zones de conflits qui se présentent presque toujours à un moment ou un autre dans les environnements de réseaux ouverts. Il écrit que :

> As networks grow, the following kinds of disputes are almost certain to arise : (1) someone not yet on the network wants to get on and on more of the people already on the network want to keep him out; (2) someone wants to stop certain kinds of traffic moving on network (or to recover damages because the traffic in moving) and the person moving the trafic wants to continue moving it; (3) someone on the network believes that someone else on the network has not lived up to his or her commitments.[2]

Pour situer les normes d'origine diverses qui sont susceptibles de jouer un rôle dans la prévention et la résolution de tels conflits, il faut se préoccuper des règles qui concernent l'accès aux réseaux et les conditions de tels accès. Il faut également s'intéresser aux règles portant sur les contenus véhiculés et troisièmement, sur les règles portant sur les transactions qui interviennent entre les usagers. Dans le présent texte, on s'attache principalement aux règles touchant les informations diffusées ou circulant dans les réseaux.

Le nouvel espace cybernétique, le «cyberspace»[3] appelle une révision de la manière d'envisager l'encadrement juridique de la

2. Henry H. PERRITT jr, «Dispute Resolution in Electronic Networks Communities» [1993]38 *Villanova L.R.*, 349-401, p. 353.

3. L'expression est souvent employée dans la littérature américaine sur le sujet. Nous l'utilisons à la suite de Laurence Tribe dans «The Constitution in Cyberspace : Law and Liberty Beyond the Electronic Frontier» où il écrit que : «I'm using the term «cyberspace» much more broadly, as many have lately. I'm using it to encompass the full array of computer-mediated audio and/or video interactions that are already widely dispersed in modern societies -- from things as ubiquitous as the ordinary telephone, to things that are still coming on-line like computer bulletin boards and networks like Prodigy, or like the WELL ("Whole Earth 'Lectronic Link") [...]» Voir : Laurence TRIBE, «The Constitution in Cyberspace : Law and Liberty Beyond the Electronic Frontier», KEYNOTE ADDRESS AT THE FIRST CONFERENCE ON COMPUTERS, FREEDOM & PRIVACY, march 26, 1991, Jim Warren & Computer Professionals for Social Responsibility, affiché sur le Gopher Cyberspace;. voir également,

production, de la diffusion et de la circulation de l'information. Une telle redéfinition n'est pas forcément en rupture avec toutes les façons traditionnelles d'envisager les normes de conduite : elle peut, en bonne part trouver ses racines dans les normativités émergentes et observées dans les environnements actuels de la communication électronique. Cette démarche permet de favoriser les encadrements souples et compatibles avec les acquis des sociétés pluralistes.

L'intégration de composantes informatiques aux médias traditionnels a favorisé la mise en place de nouvelles possibilités et de nouveaux services tels les bases de données en direct ou les transactions commerciales électroniques. Ces services d'information électroniques sont un regroupement de médias, de technologies et de contenus ayant pour effet de générer une multitude de nouveaux environnements virtuels, services et applications. Les divers avancés technologiques permettent de mettre les personnes en relation plus rapidement et plus fréquemment. On peut aussi synergiser les possibilités des médias qui étaient jusque là indépendants les uns des autres : on peut intégrer des documents vidéo dans des banques de données, on peut échanger des textes par courrier électronique, les modifier, les rédiger en commun. On peut y ajouter des sons et des images, des vidéos tirées de serveurs situés aux antipodes.

Au plan de son cadre normatif, la nouveauté de la communication électronique réside dans le fait qu'elle tend à fédérer les différents contextes connus de la diffusion et de l'échange d'information. Il n'y a plus une conversation ou une diffusion de masse, il peut y avoir à la fois l'un et l'autre qui se côtoient de façon à modifier la nature de chacune et la manière dont se pose la question de leur encadrement juridique.

Les types de communication que permet l'émergence des réseaux ouverts ne sont pas vraiment nouveaux en soi. Leur nouveauté réside dans leur pouvoir de transformer des services existants ou de créer des possibilités différentes. Le spectateur-auditeur autrefois captif devient de plus en plus actif : il peut accéder à une multitude

Edward J NAUGHTON, « Is Cyberspace A Public Forum? Computer Bulletin Boards, Free Speech, and state Action», [1992] 81 *Georgetown L. J.*, 409; Dan L. BURK, «Patents in Cyberspace : Territoriality and Infringement on Global Computer Networks», [1993] 68 *Tulane L. R.*, 1.

d'informations écrites ou audiovisuelles, un peu à la manière de celui qui fréquente une bibliothèque[4].

La plupart de ces environnements fonctionnent de manière à constituer à la fois un mode de diffusion, de distribution et d'échange de l'information. c'est ainsi qu'ils offrent la possibilité de communiquer avec un seul correspondant ou une multitude d'entre eux, celle de mettre des informations à la disposition d'un ou d'une multitude d'usagers à tel point que la relation qui existe entre l'usager et les informations disponibles ressemble à la fois à celle d'une bibliothèque électronique et à un réseau de diffusion programmé par l'émetteur. À cela s'ajoute la possibilité de combiner, de recouper de réorganiser et de copier plusieurs types d'informations. De plus, les réseaux eux-mêmes sont interconnectés ce qui confère une portée très étendue à l'ensemble des usagers. Enfin, on peut communiquer avec des personnes sans qu'elles soient à un endroit fixe à un temps déterminé.

La maîtrise des dimensions juridiques d'un phénomène comme la communication par réseaux informatiques ouverts ne saurait découler de la mise en place d'une pléthore de lois et de règlements ou de la mise en place d'un organisme ayant une vocation d'évangélisation juridique! Une telle maîtrise passe par la mise en place d'une capacité d'adapter, le plus rapidement possible, le système juridique dans son ensemble afin de contribuer au développement d'un savoir

4. MINISTÈRE DES COMMUNICATIONS, *Nouveaux médias... Nouveaux choix*, Ministre des approvisionnements et services Canada, 1992, 47 p.; ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUES, *Convergence entre technologies de communications : Études de cas de l'Amérique du Nord et de l'Europe de l'Ouest*, Paris, Politiques d'information, d'informatique et des communications, no 28, 1992, 149 p.; NEUSTADT, Richard M., SKALL, Gregg P. et HAMMER, Michael, «The regulation of electronic publishing», (1981) 33 *Federal Communications Law Journal* 331; SALGRADO, «Regulating a video revolution», (1989) 7 *Yale L. & Pol'y Rev.* 516; SCOTT, Michael D. et TALBOTT, James N., «Interactive media : What is it, why is it important and what do I need to know about it?», (1992) 11 *Computer/Law Journal* 585; STERN, Jill Abeshouse, KRASNOW, Erwin G. et SENKOWSKI, R. Michael, «The new video marketplace and the search for a coherent regulatory philosophy», (1983) 32 *Catholic University Law Review* 529; WACHTEL, Mindy Elisa, «Videotex : A welcome new technology or an orwellian threat to privacy?», (1983) 2 *Cardozo Arts & Entertainment L. R* 287.

juridique dans le domaine de la communication par réseaux informatiques. L'on accroît ainsi les chances d'orienter le développement de ces nouveaux outils dans le respect des droits et intérêts du plus grand nombre. C'est là une composante à part entière du développement véritable des technologies de l'information. De même que la recherche et le développement constituent la clé de voûte de l'innovation et de l'efficacité au plan de la technologie et des contenus, la recherche sur les techniques d'encadrement juridique est le meilleur atout pour assurer l'émergence d'un cadre adapté, réaliste et effectif pour cet environnement global de communication.

1. LES RATIONALITÉS AU SOUTIEN DES RÈGLES DE CONDUITE

Les règles de conduite limitant l'accès aux réseaux ou limitant la circulation des messages affectent l'exercice de la liberté d'expression. Ils doivent donc reposer sur des justifications suffisantes. La plus souvent, on juge à propos de limiter l'exercice de la liberté d'expression parce que le respect d'autres droits et valeurs paraît le nécessiter. À l'égard de la liberté d'expression, ces motifs invoqués pour en limiter l'exercice constituent les rationalités au soutien des règles imposant des contrôles ou des sanctions à la suite de la diffusion d'informations.

L'encadrement juridique est tributaire des valeurs, souvent contradictoires, qu'on essaie d'y refléter. Il ne peut donc s'analyser en faisant abstraction de ces valeurs. Ces valeurs sont captées par le droit qui en fait parfois des notions chargées de signification et de conséquences juridiques. Au nom de ces valeurs naissent des droits et des obligations à la charge de ceux qui sont considérés comme ayant la responsabilité des informations mises en circulation.

L'appréhension des règles encadrant un phénomène comme la communication dans des réseaux ouverts suppose une connaissance des rationalités sous-tendant les règles envisagées ou envisageables. Il s'agit en quelque sorte de connaître les raisons qui poussent à l'adoption des règles, les rendent «rationnelles».

Les représentations de la réalité que se font les acteurs et les décideurs, les impératifs dictés par les inquiétudes se développant à diverses époques au sein de ce qu'il est convenu d'appeler «l'opinion publique» jouent assurément un rôle majeur dans l'émergence et la cristallisation de rationalités perçues comme autant de motifs légitimes pour intervenir à l'égard d'une question. Par exemple, nos

sociétés contemporaines attachent beaucoup d'importance à la protection de la dignité des personnes, à l'égalité, au bon fonctionnement du système judiciaire, à la protection de la vie privée.

Les rationalités peuvent se fonder sur les missions assignées à un réseau, par exemple, un réseau informatique dévolu prioritairement à l'enseignement et à la recherche sera réglementé de manière à favoriser son utilisation en conformité avec sa mission. Ces rationalités peuvent aussi refléter les valeurs qu'il paraît nécessaire de protéger. Ces rationalités ne sont pas identiques dans les différents sites qui existent sur la planète. Il y a des différences de valeurs, de sensibilités et de culture.

Se pose alors la question de la légitimité de l'intervention au niveau des réseaux locaux. Cette légitimité doit-elle s'appuyer sur les motifs traditionnellement admis comme raisonnables pour restreindre l'expression ou doit-elle trouver appui dans un nouvel ensemble de motifs particuliers à l'environnement ouvert et planétaire des réseaux ouverts.

2. LES TECHNIQUES DE RÉGLEMENTATION

Nous appelons «techniques de réglementation» les divers moyens utilisés par ceux qui veulent imposer des normes de conduite à ceux qui prennent part à une activité. C'est en adoptant l'un ou l'autre ou une combinaison de techniques de réglementation que les instances chargées de mettre au point les politiques parviennent à définir et à prévoir les modes d'articulation entre les droits, les obligations et les intérêts des diverses parties impliquées dans la circulation de l'information.

En général, il n'y a pas une façon unique de s'y prendre pour énoncer les droits et les obligations des personnes ou pour énoncer des préceptes qui guideront les comportements de ceux qui participent à une activité. L'analyse des techniques de réglementation vise à identifier les diverses possibilités qui s'offrent afin de mettre en oeuvre les politiques plutôt que de faire seulement jouer les réflexes de l'habitude et avoir recours à des règlements ou d'autres outils familiers dans des situations qui ne s'y prêtent pas.

La connaissance des pratiques réglementaires, para-réglementaires et professionnelles est nécessaire à la compréhension du droit et du fonctionnement d'un environnement comme les autoroutes

électroniques. Les normes auxquelles on s'intéresse ici concernent des activités se déroulant dans un contexte qui dicte certaines règles du jeu. La réglementation et surtout l'autoréglementation constituent donc des dimensions marquantes d'un cadre juridique qui n'est souvent formulé dans les textes de loi sous la forme d'une esquisse. Le plus souvent, il faut déduire à partir des principes généraux du droit commun.

Pour faire l'étude des techniques de réglementation envisageables à l'égard d'un phénomène, il faut donc posséder des informations suffisantes sur les traits fondamentaux et le fonctionnement des techniques de réglementation disponibles afin de tenter de faire passer dans les comportements des objectifs conformes aux rationalités sous-tendant les règles de droit. Deux grands traits marquent les normes encadrant les échanges d'information et les diverses activités prenant place dans les réseaux ouverts. Un premier trait de ces normes est qu'elles sont énoncées au moyen de principes généraux et de notions floues. Un second trait tient au lieu d'énonciation de ces normes : on les retrouve très souvent dans les politiques des gestionnaires de réseaux.

2.1 Le recours aux principes généraux et aux standards

L'énonciation des droits et obligations des acteurs à l'égard de réalités immatérielles demeure un défi pour le droit. Il est malaisé de prescrire des normes à partir des modèles développés pour l'appréhension de phénomènes matériels. D'ailleurs, ce qui est recherché dans la régulation de l'univers des réseaux ouverts d'information, c'est bien plus un résultat global qu'une application mécanique des règles de droit. Les mécanismes de réglementation et de surveillance doivent donc viser à procurer les ajustements et mises à niveau que requiert le respect des valeurs essentielles[5].

Cela explique sans doute, en partie, le recours aux formules larges, aux préceptes généraux et aux jugements après-coup qui parait constituer la technique privilégiée de réglementation dans ces univers cybernétiques. Lorsqu'il y a des lois qui s'appliquent à de tels environnements, elles sont généralement énoncées en termes larges et

5. Bernard GUILLOU et Jean-Gustave PADIOLEAU, *La régulation de la télévision*, Paris, CNCL, La documentation Française, 1988 p. 44.

réservent une grande place aux évaluations concrètes des acteurs sur le terrain[6].

Dans un environnement ouvert, transcendant les frontières nationales, et dans lequel les notions de temps et de lieu sont redéfinies, il est malaisé de déterminer *a priori* de quelle façon les divers principes, valeurs et objectifs énoncés dans les politiques ou les lois générales pourront être atteints dans le concret. Daniel Gifford écrit à ce propos que : «These value-referents reflect [...] the inability of the legislature to speak more precisely.»[7] C'est comme si les réalités auxquelles la loi entend faire face étaient si multiples, si complexes et si volatiles qu'il est impossible de les encadrer de façon plus précise. Ce genre de formulation au moyen de notions floues répond à un impératif d'adaptabilité : l'un des plus difficiles à réaliser pour le droit.

Pour garantir un équilibre entre les impératifs contradictoires qui se manifestent dans les environnements de réseaux ouverts, on ne peut se fonder sur des démarches fondées sur la quête de «règles» de droit précises. Ce genre de démarche est d'ailleurs difficile car on fait face à un univers en mutation constante. Comment alors énoncer, de façon claire, précise et définitive ce qui est permis et ce qui est interdit alors que l'environnement des réseaux est appelé à des mutations continues.

Il faut souvent se résoudre une démarche moins sécurisante, plus complexe mais infiniment plus susceptible de procurer effectivement cet équilibre entre les valeurs contradictoires qu'il faut tenter de réconcilier. Les notions floues et les notions à contenu variable sont essentielles pour permettre au droit de se maintenir en contact avec les pratiques et les évolutions. Comme les droits et les libertés ne sauraient se définir en vase clos, il est essentiel de rédiger les règles ayant trait aux droits fondamentaux en préservant cette ouverture sur tous les milieux qui réfléchissent et exercent leur activité autour de ces droits.

6. Voir pour ce qui a trait aux lois reslatives à la protection de la vie privée : Karim,BENYEKHLEF *La protection de la vie privée dans les échanges internationaux d'information*, Montréal, Éditions Thémis, pp. 65 et ss; Ruel Torres,HERNANDEZ,, «ECPA and online computer privacy», 41 *Federal Communications Law Journal* 17.

7. Daniel J. GIFFORD, «Communication of Legal Standards, Policy Development, and effective conduct Regulation» [1971] 56 *Cornell L.R.* 409. p. 419

C'est ainsi que l'on trouvera souvent des normes énoncées au moyen de notions floues, des standards On entend par standard une norme souple fondée sur un critère intentionnellement indéterminé. Cette technique convient aux situations pour lesquelles il est malaisé de formuler des règles *a priori* sur les comportements que doivent avoir les sujets de droit[8]. La transmission de l'information, caractérisée par son évolution rapide et la place importante qu'elle laisse à l'activité créatrice s'accommode mal de règles détaillées. Les standards se présentent selon la formule de Rials comme «des instruments de mesure en termes de normalité»[9] c'est ce qui fait leur spécificité; c'est aussi de là qu'ils tiennent leur ambiguïté. La normalité, dans les sociétés pluralistes, est ambiguë[10].

En somme, dans des environnements volatils comme les espaces cybernétiques, il est peu réaliste de s'attendre à ce que des textes de lois ou des règlements viennent définir une fois pour toutes ce qu'il est permis et interdit de faire. La régulation énonce plutôt des principes larges et laisse leur actualisation à un processus continu de dialogue, de découverte et d'expérimentation. Un tel processus de régulation est d'ailleurs caractéristique des réseaux ouverts. Le dialogue et la controverse contribuent à réguler le discours qui circule en flot continu et multidirectionnel.

Le sens des droits fondamentaux et autres notions utilisées pour départager les droits et les obligations des participants à un environnement aussi volatil que les réseaux ouverts se définit dans

8. Al Sanhoury écrit : qu'«À la fixité et la rigidité de la règle, s'oppose avantageusement la souplesse et l'adaptabilité du standard.» A.-A. AL-SANHOURY, «Le standard juridique» dans *Recueil d'études sur les sources du droit en l'honneur de François Gény*, Tome II, Paris, Librairie du Recueil Sirey, 1935, p. 144; Pierre TRUDEL, «Le standard de programmation de haute qualité dans la législation sur la radio et la télévision», [1989] 34 *R. D. Mc Gill* 203-233.

9. RIALS, Stéphane, «Les standards, notions critiques du droit», dans Chaim PERELMAN et Raymond VANDER ELST (dir.), *Les notions à contenus variables en droit*, Bruxelles, Travaux du Centre national de recherches en logique, 1984., p. 43

10. Pierre TRUDEL, «Le rôle de la loi, de la déontologie, et des décisions judiciaires dans l'articulation du droit à la vie privée et de la liberté de presse» dans Pierre TRUDEL et France ABRAN (éds), *Droit du public à l'information et vie privée : deux droits irréconciliables?*, Montréal, Éditions Thémis, 181-202, p. 195.

les systèmes diffus[11] comme la morale, l'idéologie, les croyances communes ou communément admises. Aucune source du droit, et la législation pas plus que les autres, ne saurait agir de façon définitive sur l'émergence des conceptions et des façons de voir qui se combinent et se recombinent de façon spontanée. C'est pourquoi le raffinement des raisonnements et des concepts passe par le maintien d'un milieu vivace au sein duquel peuvent se confronter les diverses conceptions et systèmes de valeurs.

Les arbitrages et les articulations entre les droits fondamentaux se manifestent aussi bien au niveau des systèmes diffus que dans les systèmes denses que sont le système politique, les institutions proprement juridiques et surtout, les moeurs qui s'élaborent dans les environnements que constituent ces réseaux. Ils se manifestent dans la déontologie et se cristallisent parfois dans le droit étatique par le truchement des décisions des juges ou des autres instances éventuellement appelées à résoudre les conflits. Tous ces systèmes contribuent, à leur façon, à la détermination du sens des droits et des libertés dans un contexte donné et au raffinement des règles qui y sont suivies.

Les réseaux ouverts mettent en présence une multitude d'utilisateurs. Ces utilisateurs sont regroupés en différentes communautés. C'est au niveau de ces communautés que s'expérimente, s'énonce, s'applique et se discute la régulation. Dans un tel contexte, il est difficile de s'attendre à ce que la régulation s'exprime par le véhicule de la loi étatique. Les systèmes de droit des différents états vont plutôt se borner à énoncer les valeurs fondamentales et devront tenir compte que ces valeurs seront défendues et promues dans des communautés d'utilisateurs qui sont virtuelles.

Dans les réseaux ouverts, il n'y a plus de lien obligé entre les lois nationales et les utilisateurs. Il n'est en effet impossible de poser que chacun des utilisateurs est lié par les dispositions de la loi nationale du lieu ou il se trouve. Il peut en effet se trouver à Québec et prendre part à un groupe de discussion qui est dirigé depuis Amsterdam.

11. Voir Philippe JESTAZ, *Le droit*, 2e édition, Paris Dalloz, 1992, p 26 et ss. : «Le droit, avec son réseau serré de règles et d'institutions, est un système compact, de surcroît imbriqué avec d'autres systèmes sociaux. Certains sont aussi denses que lui [...] le système politique et les moeurs, [...] d'autres paraissent plus diffus. [...] la morale et l'idéologie [...].»

À l'inverse, une communauté d'utilisateurs peut *de facto* ou par choix se retrouver liée par une loi étrangère. Par réverbération, les lois qui apparaissent les plus adaptées aux communautés d'utilisateurs seront plus spontanément suivies et choisies par ces dernières. D'où la tendance à une plus ou moins marquée à l'uniformisation du droit.

Devant les défis découlant de la nécessité de protéger les droits des personnes et les valeurs fondamentales dans les environnements réseaux, l'on peut envisager deux grandes approches juridiques. Une première approche consiste en la mise au point d'une réglementation spécifique déterminant les obligations des usagers des réseaux, notamment à l'égard des données personnelles.

Au niveau macro-juridique, il s'agit d'examiner les stratégies d'intervention étatique pour donner suite à un ensemble donné de rationalités. Au premier chef, on ne peut ignorer l'importance croissante des organismes nationaux et internationaux de standardisation qui parfois à partir de normes techniques énoncent un ensemble des préceptes qui finissent par s'imposer, peu importe leur caractère contraignant. Ce processus de «sur-normalisation» joue un rôle majeur dans l'émergence des normativités dans les environnements techniques.

Dans la définition d'une politique nationale relativement à un phénomène identifié et pour lequel on aura pris la peine d'identifier les rationalités sous tendant l'intervention de l'État, on aura à décider s'il convient de :

- s'en tenir aux principes du droit commun;
- d'intervenir par le truchement du droit pénal;
- de créer un organisme de réglementation et de surveillance;
- d'énoncer de grands principes en laissant aux instances le soin de les mettre en oeuvre ou énoncer avec précision les droits et obligations des acteurs;
- de s'en remettre à l'autoréglementation;
- de mettre sur pied des campagnes de «sensibilisation».

Les mécanismes fiscaux et financiers sont une autre façon de mettre en oeuvre les politiques publiques. En ce sens, on n'hésite pas à les considérer comme une technique de réglementation.

En somme, l'analyse macro-juridique des techniques de réglementation doit évaluer les stratégies d'énonciation des normes et évaluer les approches pour en assurer le décodage et l'application.

Au niveau micro-juridique, c'est-à-dire de la mise en oeuvre par chacun des intervenants exerçant un certain pouvoir de décision, l'analyse des techniques de réglementation est aussi nécessaire. Elle doit identifier les moyens compatibles avec le contexte, susceptibles de contribuer à mettre en oeuvre les rationalités. Il faut aussi identifier les micro-rationalités qui se manifestent au niveau de la mise en oeuvre des grandes politiques qui peuvent être esquissées dans les textes généraux.

Là encore, il est sans doute opportun de prendre la peine d'énoncer les principes qui doivent être suivis par ceux qui participent aux activités du réseau. En plus, on peut avoir recours à des techniques préventives, programmes d'éducation, énoncés de principe, normes d'éthique.

La surveillance est un autre moyen par lequel on peut s'assurer du respect des normes. La surveillance peut être continue ou par «spot-check», elle peut s'exercer à la suite de plaintes expressément signalées, à la suite d'un constat lors de démarches de routine ou selon un programme sophistiqué de monitoring général ou ciblé. La surveillance pose d'importants problèmes de départage entre les valeurs liées à la protection de la confidentialité et la protection des autres valeurs qui peuvent êtres affectées par certaines activités des protagonistes dans un réseau. Pour cette raison, on trouve souvent nécessaire de l'encadrer dans un processus offrant des garanties contre l'arbitraire.

Les avertissements servis à ceux qui ne respectent pas les normes sont sans doute, en eux-mêmes, une partie de l'activité régulatrice. Bien sûr, les sanctions proprement dites, la fermeture des comptes etc. constituent les ultimes mesures de sanction.

En adoptant une politique d'encouragement à des réflexions déontologiques dynamiques dans les milieux de la communication dans les réseaux ouverts, on multiplie les chances de favoriser le développement, au sein des communautés d'utilisateurs, de

comportements, voire de réflexes d'analyse et de prise en compte des valeurs et intérêt en présence. Une telle approche suppose d'accroître la formation de tous ceux qui ont à prendre des décisions relatives à la diffusion et à la régulation de l'information dans ces environnements.

2.2 Les politiques des gestionnaires de réseaux («Sites policies»)

Ceux qui ont la maîtrise d'un lieu (un site) dans le réseau ont la possibilité d'adopter des politiques relativement à l'accès au site, aux comportements acceptés et aux actes prohibés. La plupart des institutions universitaires se sont dotées de politiques ou de règles délimitant les droits et prérogatives de ceux qui font usage des capacités informatiques des institutions.

Les rationalités sur lesquelles s'appuient ces politiques découlent souvent d'un souci de favoriser l'usage rationnel des ressources de l'institution, le respect des droits fondamentaux et de la dignité des personnes. Par exemple, l'Université Mc Gill a édicté un règlement à l'intention des usagers de ses services informatiques. Ce texte dispose que :

> McGill Computing Facilities (MCF) are defined as any computer, computer-based network, computer peripheral, operating system, software or any combination thereof, owned by McGill of under the custody or control of McGill University. Equipment and Software purchased from research funds administered by McGill are owned by McGill University unless otherwise specified in the research grant or contract.
>
> All McGill staff, students and other users of the MCF shall :
>
> 1- Recognize that MCF are strictly intended to support the academic mission and the administrative functions of the University and assume full responsibility for using these facilities in an effectiveefficient ethical, lawful and polite manner.
>
> 2- Use only those facilities which are in the public domain or for which they have obtained explicit authorization, at McGill or at any other location accessible through a network.

> 3- Take all necessary steps to protect the integrity of MCF. In particular, the users shall not share with others the access codes, account numbers, passwords or other authorization which have been assigned them.
>
> 4- Respect the copyrights of owners of all software and data they use.
>
> 5- Respect the policies established by the administrators of external networks such as RISQ, CA*net, NSFNET when using such networks. They shall also respect the policies established by the administrators of local computing facilities at McGill.
>
> 6- Respect the privacy of E-mail and other user files carried and stored in MCF or at any other location accessible through a network.
>
> 7- Not use the MCF for conductin private business or for personal financial gain, unless specifically authorized.
>
> 8- Not use the MCF for any unauthorized or illegal purpose, such as destruction or alteration of data owned by others, interference with legitimate access to computing facilities or harassment of users of such facilities at McGill or elsewhere, unauthorized disruption of MCF, attempts to discover or alter passwords or to subvert security systems in MCF or in any other computing facility.
>
> 9- Properly sign or make traceable any remote access to MCF, any E-mail, message or file transfer initiated on MCF.
>
> 10- Take all reasonable steps to protect the integrity and privacy of the software and data made available to them.
>
> Users should recognize that authorized McGill personnel may have access to data and software stored in MCF while performing routine operations or pursuing systems problems. Users should further recognize that, as specified in the relevant administrative policies at McGill, authorized personnel have the obligation to take appropriate steps to ensure the integrity of MCF and to ensure that the present regulations are observed.

Any violation of these regulations will be prosecuted in conformity with the relevant University policy (Code of Student Conduct, Personnel policies, etc.) and the principle of due process.[12]

Les politiques de certaines institutions prévoient le cas particulier du harcèlement résultant de l'usage des réseaux informatiques. Récemment, le gouvernement d'Ontario a émis une directive à l'endroit des universités. On peut y lire que :

In developing their local policy and procedures, institutions are encouraged to review best practices already present in the post secondary system and material in the Council of Regents Harassment Task Force Report. This information will be provided to any interested stake holder group by the Ministry. In writing their policies and procedures, institutions will have to balance legal soundness and accessibility for users. The product should be easy to read, easy to understand, and easy to use. Those developing policies and procedures should write simply, clearly, and use plain language.

The government will provide $1.5M to the post secondary sector to support the development and production of training packages, data collection models, ongoing evaluation models, an external audit model and process, the development and production of educational materials for all constituent groups and regional training and information sharing workshops.[13]

Rosenberg préconise des politiques marquées au coin de la souplesse. Il s'appuie sur la nécessité de préserver la liberté d'expression et de chercher à éduquer les gens plutôt que de réprimer. Il met de l'avant six principes à l'intention des gestionnaires de réseaux :

12. «Regulations for Users of McGill Computing Facilities», tiré de *Computer and Academic Freedom*, gopher EFF.

13. ONTARIO, FRAMEWORK REGARDING PREVENTION OF HARASSMENT AND DISCRIMINATION IN ONTARIO UNIVERSITIES, dans Gopher, Computer and academic freedom archives and info.

A. Administrative principles

1. Do not treat electronic media differently than print media, or traditional bulletin board, merely because they can be more easily controlled.

2. Do not censor potientially offensive material on networks : Encourage the use of sexual harassment procedures, if appropriate.

3. Be awara of your responsibility with respect to the uses and misuses of your facilities. However, do not use cost of services as an excuse to censor and limit access.

4. Trust and educate people to be responsible.

B. Social principles

1. Issues will proliferate beyond the ability of organizations to control them by rigid policies.

2. Occasional offensive postings do not detract from the benefits of electronic networks.[14]

Il ajoute que le réflexe de censure peut être celui qui se manifeste le premier. Il est souvent en effet plus facile de recourir aux solutions autoritaires pour répondre aux plaintes de ceux qui peuvent se sentir embarrassés par certains comportements ou certaines diffusions. Il explique en effet que :

Experience indicates that under pressure, administrators at public institutions may be willing to sacrifice free speech over networks to appease loudly expressed concerns about pornography corrupting the morals of otherwise innocent students. On the opposite side it might be argued, unsuccessfully I would maintain, that networks are a special case with respect to free speech because tey are so pervasive

14. Richard S. ROSENBERG, «Free Speech, Porrnography, Sexual Harassment, and Electronic Networks», *The Information Society*, Oct.-dec. 1993, 9(4), 285-331.

and so difficut to monitor for material that might beruled illegal because of a violation of community standards.[15]

L'ampleur du travail nécessaire pour assurer la surveillance par les gestionnaires de sites peut s'avérer considérable. Comme l'explique Rosenberg :

> Posting to given newsgroups can be cross-posted to other, less threatening, ones. So for example an item in alt.sex might also appear in alt. censorship. The job of making sure that no ofensive postings appear anywere on the network would be formidable, far beyond the capability of any site. But suppose that the nimber of these cross-postings is limited and not a real concern. Is everything safe for the university and its students and staff? Probably not. The more entreprising people will do a remote login (i.e. connect from the home site to another site), even in a different countrym, that carries the desired newsgroup, having firts acquired a c9omputer ID (identification codeword) and password at that site. Once downloaded, postings from this newsgroup are then available for distribution at the home site.[16]

Un site peut décider de supprimer un accès à un groupe, ou une liste etc. mais cet accès peut être obtenu par le truchement de la fréquentation d'un autre site, lui-même disponible et procurant les relais pour le site interdit. En somme, il y a des limites pratiques considérables à la possibilité de supprimer les messages dans un environnement de réseaux ouverts et interconnectés. Un rapport de l'Université de Western Ontario relève ainsi l'ampleur des problèmes auxquels on fait face lorsqu'on souhaite limiter l'accès aux informations disponibles dans certains babillards de l'Internet :

> A partial filtering of postings to the system based on presumed content (eg. based on the title of the newsgroup to which a posting is made) would not significantly impair access, and might generate additional network traffic. Moreover, there is the matter of the legitimacy of censorship (however ineffective) based on presumed or possible content rather than actual content. The CUC judges that, in general, the campus

15. *Id.*

16. *Id.*

> community would be against such arbitrary censorship. This course of action is, therefore, not acceptable either.
>
> [...]
>
> Given the volume of daily postings to the entire News system, it is not feasible for anyone to read all postings before they are placed on the system. However, should a specific posting be received by a user of the system and its content judged to be possibly illegal, the CUC agrees that it is reasonable to expect that there be a procedure for that individual to follow that could lead to the posting in question being removed from the University's local feed (even though that would not prevent users from gaining access through remote feeds). Even if this is granted, however, questions remain, including : How do we determine whether a posting is or might be judged to be illegal? and How can timely decisions regarding this matter be made, given that all postings are automatically removed from the local feed after a few days in any event?[17]

Étant donné l'ampleur des ressources qu'il serait nécessaire de consacrer à la suppression d'informations dans un tel contexte, il faut que les rationalités au soutien des règles que l'on chercherait par ce moyen à faire appliquer soient très sérieuses. Or, il faut bien constater que dans la tradition canadienne, on a souvent recours à la censure comme moyen-réflexe pour résoudre des difficultés. Les environnements de réseaux ouverts supposent de développer des méthodes moins rudimentaires pour faire face aux conflits résultant de la circulation de l'information.

Plusieurs conflits peuvent être prévenus en énonçant les politiques suivies en cas de conflit par le gestionnaire du site. En attendant une revue de la teneur de ces politiques, on peut citer celle de l'Université Western Ontario qui prévoit ce qui suit :.

1. The Computer Users' Committee (CUC) is responsible for reviewing and approving all Usenet-related policy proposals from Computing and Communications Services

17. University of Western Ontario, Department of Computing and Communications Services, Computer Users' Committee, *Report on Usenet Policy*, May 12, 1993, alt.comp.acad-freedom.talk, Message-ID : <2drlpc$qk0@eff.org> aussi affiché au Gopher EFF.

(CCS), including those relating to the newsgroups to be carried in the University's local feed.

2. In its publications regarding Usenet, CCS should make it clear that the individual user bears the primary responsibility for the material that he or she chooses to send or display on the network or on the University's computer systems.

3. Anyone who wishes to lodge a complaint regarding the content of a particular newsgroup posting should file a complaint with CUC in accord with the following procedure :

   (i) A complainant should register his or her complaint with the News Manager in CCS. The complaint should be in writing, preferably via e-mail, and should define the newsgroup and the posting of concern and specify how the material was obtained by the complainant.

   (ii) The News Manager will immediately forward this material to the CUC, through the Director of CCS, and the Chair of the CUC will call a meeting within two days of its receipt. The CUC will solicit a legal opinion if necessary. The Committee might take the following actions : reducing the time that the posting of concern remains on the local feed; reducing the time that the newsgroup in question remains on the local feed; asking CCS to assist the complainant to contact the individual who posted the material in order to register a complaint. Copies of the decision, including reasons, will be sent to the Director of CCS and to the complainant, and relevant action will be taken by CCS through the Director.

   (iii) Appeals of CUC decisions may be made to the Director of CCS in writing, who will forward it to the University Computer Council (UCC), along with copies of the original complaint, as well as the CUC decision. UCC will review this material and make its decision on the appeal through a simple majority vote. This decision will be forwarded to the Director of CCS and the appellant, and the original complainant if this is not the same individual.

4. All administrators of CCS and other campus computing systems should continue to be responsible for following up on reported abuses of the information technology resources under their control by the faculty, staff and students of the University who are users of their system(s), including abuses of the Usenet system such as the posting of possibly offensive or illegal material.

5. Anyone wishing to lodge a complaint regarding suspected abuse of the information technology resources of the University by a member of the University community, should contact the administrator responsible for the system on which the abuse took place or, if it is unclear or unknown who that person is, or if the abuse is of a more general nature, the Director of CCS.[18]

Il n'y a pas encore de typologie systématique des politiques suivies dans les différents milieux donnant accès à des réseaux ouverts. Il est toutefois possible de voir certaines tendances. Mais pour préparer la mise en place d'une telle typologie et apprécier la portée réelle de telles politiques, il faut surtout identifier comment se pose la question de la défense des droits et des valeurs dans ces environnements ouverts. Pour y parvenir, il faut tenir compte des contextes diversifiés et des rôles assumés par les différents intervenants dans un tel univers.

3. LES CONTEXTES

La communication électronique se déroule dans différents contextes. Certains de ces contextes mettent en évidence les rôles et responsabilités des fournisseurs de réseaux et des transporteurs de communications tandis que d'autres mettent plus directement en relief les relations qui se nouent entre les participants à cet espace virtuel.

Pour mieux comprendre les normes émergentes dans ces environnements électroniques virtuels, il faut identifier les principaux cas de figure des contextes qu'ils présentent aujourd'hui et les possibilités qui se dessinent. On peut identifier quatre principaux cas de figure à partir des situations souvent évoquées comme

18. *Id.*

constituant la préfiguration de la communication par les autoroutes électroniques.

Quatre contextes paraissent ensemble couvrir la gamme des situations dans lesquelles les droits des personnes sont mis en cause et pour lesquels on ressent le besoin d'avoir recours à des normes pour prévenir ou résoudre les conflits. Il s'agit premièrement des réseaux à contrôle centralisés destinés au public comme les réseaux câblés et les divers perfectionnements susceptibles de les rendre interactifs, en second lieu, les réseaux complètement ouverts comme l'Internet. D'autre part, en troisième lieu, les relations entre les gestionnaires de réseaux et, en quatrième lieu, entre les usagers engendrent des contextes et situations dans lesquelles l'intervention de règles de conduite est nécessaire.

3.1 Les réseaux à contrôle centralisés

Un premier contexte est celui des réseaux à contrôle relativement identifiable tels que les réseaux câblés ou les services télématiques offerts au grand public ou aux groupes professionnels. Ces réseaux sont sous la maîtrise d'une entité unique, bien identifiée[19]. Les lieux d'émission et les lieux de réception y sont relativement bien identifiables et la répartition de rôles y est assez bien caractérisée. La diffusion est sous l'entière maîtrise de l'entreprise qui offre les contenus. Ces contenus sont livrés aux abonnés à la suite de choix effectués par ces derniers ou leur sont disponibles d'office. Par exemple, dans le projet UBI ou son actuel ancêtre, le Vidéoway, le point focal, celui par lequel transitent les communications, est le serveur à la tête de ligne du réseau câblé[20].

19. Pierre TRUDEL et France ABRAN, *Droit de la radio et de la télévision*, Montréal, Éditions Thémis, 1991, 1180 p., aux pages 325 et 764 à 771.

20. Il est, dans l'état actuel du droit canadien difficile d'imaginer que les services offerts par le truchement des entreprises de câble échappent complètement au contrôle de ces dernières. L'entreprise de câblodistribution doit, sauf autorisation contraire du CRTC, être exploitée de façon effective par la titulaire de sa licence ou, réellement, par ses employés. Elle droit de plus détenir la propriété et exploiter elle-même ses équipements et ses installations. L'article 4 du *Règlement de 1986 sur la télédistribution* exige que la titulaire possède et exploite sa tête de ligne locale, ses amplificateurs et ses prises de service d'abonné. Lorsque l'entreprise est autorisée à offrir des services de télévision payante ou spécialisés, elle doit aussi posséder les décodeurs ou autres dispositifs de brouillage et, dans le cas d'un système de sécurité adressable, l'ordinateur contrôlant ce système. Ces obligations, visant l'exploitation effective de l'entreprise et la possession au minimum de certaines installations, traduisent l'attitude du Conseil quant à la nécessité pour les titulaires d'exercer un contrôle déterminant sur leurs entreprises afin de remplir leurs obligations réglementaires. Le Conseil veut s'assurer que les titulaires soient comptables, envers le public et le Conseil, de la prestation des services et des tarifs imposés. Voir : Pierre TRUDEL et France ABRAN, *Droit de la radio et de la télévision*, Montréal, Éditions Thémis, 1991, p. 713; CRTC, Avis public 1983-82, 22 avril 1983, *Propriété du matériel de prestation de services de télévision payante par les entreprises autorisées de télévision par câble*.

C'est un système centralisé : l'abonné obtient son accès au réseau d'un câblodistributeur qui assure la fourniture du réseau et donne l'accès aux différents contenus et services.

Ces environnements permettent l'accès à des services d'information, des services de communication, des services de transaction, des services de prestation et des services de contrôle et de surveillance. L'on inclut dans les services d'information des services accessibles au public comme l'accès à des serveurs d'informations et de vidéos; de tels services présentent beaucoup d'analogies avec les situations de diffusion d'informations déjà connues. Par exemple, la radio et la télévision sont présentement envisagées comme des entités diffusant des informations vers le public et sont dotées d'un régime juridique reflétant ce rôle[21].

Les services de communication regroupent la messagerie, le courrier et les boîtes postales électroniques. Dans les services de transaction, on trouve le télé-achat et le transfert électronique de fonds. Les services de prestation regroupent les jeux et les services dits «intelligents» de type transactionnel comme les services de télé médecine et de télé éducation. Enfin, il y a les services dits de contrôle et de surveillance tels que la lecture à distance de la consommation d'électricité et la surveillance à distance des domiciles[22].

21. TRUDEL et ABRAN, *op. cit.*, pp. 292 et ss.

22. André MARTIN, *Portrait d'ensemble de l'industrie de la télématique*, Québec, Ministère des communications, Direction de l'information électronique et de la télématique, février 1989, p. 2.; Yves POULLET et Claire MONVILLE. *La demande finale en télématique- aspects juridiques*, Paris, La documentation française, 1988, p. 27; BAUM, Michael S. et PERRITT Jr, Henry H., *Electronic*

Le modèle d'autoroute électronique proposé par les entreprises de câblodistribution se présente actuellement avec des fonctions de diffusion et de réception relativement bien définies. Cependant, plusieurs facteurs contribuent à favoriser la mutation de ce modèle vers une plus grande ouverture à mesure que se multiplient les possibilités d'interconnexions. Alors, les fonctions d'émission et de réception deviennent plus difficiles à situer. Il est en effet de moins en moins possible d'identifier le lieu et les traits caractéristiques des fonctions d'émission et des fonctions de réception. Plus cette tendance s'accentue, plus on migre vers le contexte des réseaux complètement ouverts dont l'Internet semble, pour l'heure, constituer le prototype le plus achevé.

3.2 Les réseaux ouverts et décentralisés

Le modèle du réseau complètement ouvert est le second cas de figure envisagé. Ce contexte se caractérise par l'absence d'un lieu centralisé susceptible d'exercer un contrôle sur les contenus véhiculés dans le réseau ou plus exactement dans les réseaux interconnectés. L'environnement technologique permet d'être à la fois, en concomitance ou successivement producteur, consommateur, émetteur et récepteur, lieu d'émission et lieu de réception.

La conjonction de l'ensemble des fonctionnalités de réseaux interconnectés comme l'Internet a amené plusieurs auteurs à le considérer comme un espace cybernétique aux dimensions mondiales. Le «Cyberspace» apparaît beaucoup plus décentralisé que les services envisagés par les entreprises de câblodistribution. En soi, l'Internet est un réseau ouvert : on y entre, on en sort, on y émet et on reçoit des informations sans qu'il y ait un contrôle centralisé. On y accède souvent à partir d'un réseau local. Il est possible d'y trouver une multitude de lieux d'émission d'information, de serveurs tandis que les modèles dérivés de la télévision par câble reposent présentement sur l'hypothèse d'un contrôle en un lieu clairement identifiable à la tête de ligne de chaque réseau câblé.

L'Internet est un réseau de réseaux : tout utilisateur raccordé peut, moyennant les équipements informatiques appropriés, offrir des services et des contenus[23]. Il ne peut y avoir de contrôle centralisé

contracting, publishing and EDI Law, New York, John Wiley & Sons Inc, 1991, 871 p.

23. KROL, Ed, *The whole INTERNET-User's guide & catalog*, Sebastopol CA, O'Reilly & Associates Inc., 1992, 376 p.; KEHOE, Brendan P., *Zen and the art of the INTERNET-A beginner's guide to the INTERNET*, Chester PA, 1992, 96 p. et annexes.

sur ce qui circule dans le réseau. Chacune des composantes de l'Internet est à la fois un lieu de réception et un lieu potentiel de diffusion. Mais pour entrer dans l'Internet, il faut, d'une façon ou d'une autre se raccorder à l'un des multiples réseaux qui en font partie. Le réseau est en quelque sorte la porte d'accès à cet environnement global.

Dans l'Internet, le contrôle s'effectue au niveau des composantes, c'est à dire les réseaux locaux, les pourvoyeurs de passerelles, bref, ceux qui ont une certaine possibilité de regard sur ce qui transite vers et en provenance du réseau dont ils ont la maîtrise ou sur lequel ils exercent une certaine prise. À ce niveau peuvent s'exercer différentes formes de surveillance et de vérification de la conformité des usages et des messages avec les normes qui ont cours dans le milieu où le réseau est localisé.

Dans le contexte des réseaux ouverts, les possibilités effectives de contrôle sont aux mains de ceux qui administrent les différents sites entre lesquels des interconnexions existent ou sont possibles. Les administrateurs de réseaux ont la possibilité de déterminer s'ils doivent permettre les connexions avec les sites qui ne semblent pas respecter certaines règles.

3.3 Les relations entre les usagers et les gestionnaires de réseaux

Un troisième cas de figure concerne les relations entre les usagers des réseaux locaux et les gestionnaires de ces réseaux. Puisque les gestionnaires des réseaux sont les portiers donnant accès aux environnements électroniques ouverts, c'est autour des relations qu'ils entretiennent avec leurs usagers qu'émergent certaines normes et processus de régulation susceptible de procurer un équilibre entre la liberté d'expression et la protection des droits des personnes et des autres valeurs fondamentales.

Dans un tel contexte, les administrateurs de réseaux apparaissent comme les portiers à qui on demande parfois de devenir gendarmes afin de protéger les droits de propriété intellectuelle ou les valeurs morales. Leur intervention peut se fonder sur les politiques explicitement formulées ou sur des plaintes qui sont jugées légitimes. Se pose alors la question du cadre de leur intervention et

des limites qu'il conviendrait de fixer à leurs pouvoirs et prérogatives.

Les régulations qui s'observent dans ce genre de contextes sont souvent liées aux missions assignées aux réseaux. Soit qu'ils sont conçus pour les fins d'une entreprise ou d'une institution de recherche ou d'enseignement ou qu'ils sont dévolus aux fins d'une entreprise. C'est au nom de la protection de cette mission du réseau et aussi de la garantie de son intégrité que les administrateurs de réseaux justifient leur intervention.

3.4 Les rapports entre les usagers

Enfin, un quatrième contexte est celui qui a trait aux rapports entre les usagers. La fréquentation de l'Internet laisse voir qu'il se constitue des communautés d'utilisateurs qui ont leurs usages, leurs règles de bienséance, leur compréhension de ce qui est admis et accepté et ce qui est tenu pour inadmissible[24].

On peut supposer que des règles de bienséance et de bon usage émergent afin de faciliter les rapports harmonieux entre les usagers. Les communautés informelles peuvent développer des règles de conduite généralement acceptées sans vraiment qu'il y ait une intervention de la loi ou de la réglementation étatique mais ce phénomène d'émergence spontanée de normes se produit moyennant certaines conditions. Au nombre des plus importantes, il y a l'existence d'une perspective de continuité des relations[25]. Or, les relations sont peut-être suivies dans certains contextes comme les réseaux de chercheurs universitaires; elles le sont beaucoup moins dans le cas de réseaux constitués autour d'intérêts plus évanescents ou plus ponctuels.

Les réseaux ouverts mettent en présence des individus isolés ou se rattachant à différentes communautés. Entre eux se nouent des relations régies par des cadres contractuels explicites comme pour les transactions électroniques à caractère commercial (EDI) ou les transactions occasionnelles. Perritt relève aussi un autre obstacle au développement de règles spontanées parmi les utilisateurs. Il écrit en effet que :

24. Henry H. PERRITT jr, «Dispute Resolution in Electronic Networks Communities» [1993]38 *Villanova L.R.*, 349-401.

25. Henry H. PERRITT jr. *op. cit.*

> Participants in electronic network communities may have continuing relationships, but their relationships are unidimensional; they involve only a particular type of communication and no other important human activities. This unidimensionnality greatly weakens the force of informal community. If a violator of network community norms gest expelled, he simply can connect to another network.
>
> [...]
>
> As the scope of networking increases, the likelihood that users will shares values and feel membership to be essential decreases. This weakens the power of the social group to enforce its norms.[26]

Cet auteur constate qu'un réseau s'étendant à une municipalité éprouve plus de difficultés à développer et à imposer un ensemble de normes tandis qu'un réseau réunissant des usagers faisant partie d'un groupe social homogène comme le groupe des chercheurs universitaires va facilement générer des règles qui seront plus spontanément observées par les participants sans qu'il faille s'en remettre à des forces externes[27].

Ainsi, il est nécessaire de prévoir l'adaptation des règles relatives aux rapports entre les membres des communautés afin de prévenir ou de régler les conflits susceptibles de survenir entre les usagers des réseaux ouverts. À cet égard, il convient de situer les rôles et responsabilités de ceux qui prennent part à la communication dans les réseaux ouverts.

4. LES RÔLES ET LES RESPONSABILITÉS

L'identification des rôles assumés par les entités impliquées dans la communication en réseaux ouverts permet une qualification pratique des situations juridiques mises en cause. En identifiant les rôles joués par l'un et l'autre des différents acteurs, il est possible de mieux cerner comment se pose la question de leurs droits et de leurs responsabilités. Du même coup, il devient plus aisé de déterminer ou de comprendre comment se détermine ce qu'ils ont la possibilité de faire et ce qui leur est interdit.

26. *Id.*, p. 360.

27. *id.*

Différents types de décideurs interviennent dans la production, le traitement et l'acheminement de l'information. Selon les contextes diversifiés de la communication dans les réseaux électroniques, ces acteurs jouent différents rôles; ils assument même parfois une pluralité de rôles. Ainsi, un usager peut devenir un fournisseur d'information ou opérer un lieu de discussion public ou semi-public. De tels rôles peuvent parfois être assumés par l'opérateur de système ou même par le transporteur.

Par rapport au régime juridique actuel des médias électroniques, comme la télévision et la radio, l'environnement des réseaux ouverts montre une plus grande volatilité des rôles assumés par les principaux types d'acteurs. On constate en effet un bon degré d'interchangeabilité des rôles assumés dans les communications informatiques. On ne peut plus formuler un ensemble de droits et d'obligations pour chacun en postulant que les rôles assumés par les différents participants à la communication sont toujours constants.

L'objet et la portée des droits et des responsabilités des différents acteurs qui interviennent dans la communication électronique ne tient pas tellement à leur rôle officiel mais plutôt au degré de contrôle et de maîtrise qu'ils exercent ou qu'ils sont réputés exercer sur l'information et les communications qui se déroulent dans les réseaux ouverts ou sur la partie de ceux-ci sur lesquels ils ont une certaine maîtrise[28]. Le degré de contrôle exercé sur ce qui se transmet dans les voies de communication apparaît comme une donnée centrale pour délimiter les droits et les responsabilités des acteurs.

Pour dégager la portée des droits et situer les responsabilités dans un environnement comme celui des réseaux ouverts, il est utile d'avoir recours à des métaphores[29]. Ce procédé aide à dégager l'essentiel des contextes dans lesquels se déroulent les

28. PERRITT Jr, Henry H., «Tort liability, the First Amendment, and equal access to electronic network», (1992) 5 *Harvard Journal of Law & Technology* 65.

29. David R. JOHNSON & Kevin MARKS, «Mapping Electronic Data Communications Onto Existing Legal Metaphors : Should We Let Our Conscience (and our Contracts) Be our Guide?» (1993) 38 *Villanova L. Rev.* 487; Henry H. PERRITT, jr, «Metaphors for Understanding Rights and Responsibilities in Networks Communities : Print Shops, Barons, Sheriffs, and Bureaucracies- Discussion Paper», Affiché dans «Information Law Papers», Serveur Gopher de Villanova University, 24 p.

communications et ce que les acteurs y font. Les métaphores permettent de situer les droits et obligations des acteurs en identifiant la mesure de contrôle qu'ils exercent sur messages et ainsi aider à déterminer les différents niveaux de responsabilité. L'imputation des responsabilités emprunte beaucoup aux régimes développés pour les situations présentant des analogies avec la communication dans des réseaux électroniques ouverts comme le transport par chemin de fer ou la diffusion d'imprimés.

Trois sortes de rôles sont assumés dans un environnement de réseaux ouverts, chacun connaissant des variantes et des recombinaisons qui font parfois en sorte qu'en certaines situations, il arrivera qu'une entité assume plus d'un rôle. Mais en tout état de cause, dans les environnements de réseaux ouverts, on trouve invariablement des opérateurs de réseau, des fournisseurs d'information, au nombre desquels il y a les usagers et un ou des transporteurs de l'information. Voyons donc les traits majeurs de chacun de ces rôles principaux.

4.1 Le transporteur

Le transporteur fournit généralement l'accès à un réseau de télécommunication dont il a parfois la maîtrise. Dans la logique actuelle de la réglementation, il donne accès à la capacité de transporter des informations à des conditions équitables pour tous les usagers se trouvant en position équivalente. Dans le cadre de certaines situations, le transporteur peut faire plus que simplement donner accès à un réseau. De fait, il participe souvent à la facturation et à la répartition des revenus générés; il exerce alors une certaine prise sur les contenus véhiculés.

Comme le transporteur exerce parfois un certain leadership dans le choix des services distribués, quelle est sa responsabilité à l'égard des contenus véhiculés, face aux tiers et à l'égard des fournisseurs de services? C'est précisément en raison du fait que l'exploitation de certains réseaux confère un certain droit de regard au transporteur sur les contenus transportés que la question de leur responsabilité à l'égard de ceux-ci se posera parfois[30].

30. Daniel BRENNER, «Telephone company entry into video services : A First Amendment Analysis», (1991) 67 *Notre Dame L. Rev.* 97; Jerome A. BARRON , «The telco, the common carrier model and the First Amendment-The "Dial-a-porn" precedent», (1993) 19 *Rutgers Computer & Technology Law Journal* 371.; Patrick O'NEILL,

Il est acquis que les entreprises de télécommunications et les câblodistributeurs peuvent agir comme transporteurs. D'autres entreprises peuvent aussi jouer ce rôle, notamment en louant certaines installations des entreprises de télécommunications ou de câblodistribution. La diversité des avenues technologiques permet d'entrevoir que le transport peut avoir lieu de multiples façons. En raison de la polyvalence des réseaux de télécommunications, la communication électronique n'est qu'un type parmi d'autres de communications rendues possibles par les divers réseaux.

En principe, les entreprises de télécommunications ne peuvent régir le contenu ou influencer le sens ou l'objet des télécommunications qu'elles acheminent pour le public[31]. Le plus souvent, elles se bornent à fournir des capacités de transmission suivant des conditions qui doivent correspondre à des exigences d'équité et être exemptes de pratiques discriminatoires[32].

Par contre, le statut des entreprises de câblodistribution est plus ambigu. Au Canada, elles sont actuellement considérées comme des entreprises de radiodiffusion. Traditionnellement, elles n'avaient souvent qu'un rôle passif de retransmission des signaux d'autrui. Les capacités des réseaux de câbles coaxiaux sont aujourd'hui telles qu'il a été possible aux entreprises de câble de développer plusieurs services qui leur sont exclusifs, en plus d'offrir aux abonnés des services de programmation et d'autres services d'information. Elle peut aussi offrir des services «interactifs».

«Structural implications of telephone content regulation : Lessons from the audiotex controversy», (1991) 13 *Hastings Comm/Ent L.J.*379.; Pour le droit français, voir Jean LITINGRE, «La responsabilité de l'État français en qualité de transmetteur d'informations», dans *La télématique, Actes du colloque organisé à Namur les 5 et 6 décembre 1983 par le Centre de Recherches Informatique et Droit des Facultés Notre-Dame de Namur*, Gand, Story Scientia, 1983, pp. 81-91. Pour le droit québécois, non seulement faut-il déplorer la rareté des travaux sur le droit relatif aux entreprises de télécommunications comme telles, mais il faut en plus constater la quasi inexistence de travaux sur la responsabilité des entreprises de télécommunications pour les messages transmis.

31. *Loi sur les télécommunications*, L.C. 1993, c. 38, art. 36.

32. Michael H RYAN, *Canadian Telecommunications Law and Regulation*, Toronto, Carswell, 1993, p 3-6 et ss.

Ces multiples facettes des activités et des services offerts par les entreprises de câblodistribution leur ont valu un statut hybride. Pour certaines de leurs activités, on les traite comme des radiodiffuseurs, avec les conséquences qui en découlent, au premier chef, elles sont responsables des contenus qu'elles choisissent d'acheminer. Pour d'autres aspects de leurs activités, on pourrait juger plus approprié de traiter les câblodistributeurs de manière semblable aux entreprises de télécommunications.

Il n'est pas indifférent d'assimiler l'entreprise de transport des communications télématiques à un journal ou de la considérer comme un télécommunicateur. Dans le premier cas, on lui reconnaît un important degré de liberté éditoriale, lui laissant pleine liberté de choisir les services qu'elle juge approprié de transmettre. Par contre, si l'on devait considérer l'entreprise comme un télécommunicateur, elle pourrait être assujettie à des obligations plus strictes en matière de tarification et d'accès à ses réseaux telle l'obligation de traiter ses abonnés et autres clients sans discrimination[33]. Évidemment, tout un éventail de statuts intermédiaires est envisageable.

Le statut des transporteurs tient donc, pour un avenir prévisible, une place importante parmi les interrogations et incertitudes juridiques contribuant à freiner le développement de certains types de services.

4.2 Le gestionnaire de réseau

La communication électronique est possible grâce à la mise en place de raccordements entre les différents terminaux de tous ceux qui veulent entrer en communication : c'est la notion de réseau. La constitution de réseaux permet de raccorder les correspondants; ces réseaux peuvent être eux-mêmes raccordés à d'autres réseaux et donner un accès à une multitude de correspondants.

---

33. Diane L. HOFBAUER, «"Cableporn" and the First Amendment : Perspectives on content regulation of cable television», 35 *Federal Communications Law Journal* 139; Pierre TRUDEL et France ABRAN, *Un état des questions juridiques posées par l'avènement de la télématique grand public*, Rapport rédigé pour la direction générale des technologies de l'information, Ministère des communications du Québec, Montréal, Centre de recherche en droit public, Juillet 1989, 70 p..

Le réseau est l'élément névralgique de cet environnement virtuel souvent appelé «cyberspace». C'est à la fois la porte d'entrée et le lieu dans lequel il est possible d'exercer une certaine forme de contrôle, ce qui ne veut pas dire que ce contrôle soit toujours pratiquement possible ou souhaitable. Le gestionnaire de réseau joue donc un rôle majeur dans la régulation des communications électroniques.

Les réseaux sont de dimensions variables. Par exemple, l'Internet est composé de réseaux locaux (Local Area Networks [LAN])[34], de réseaux régionaux ou métropolitains (Metropolitan Area Networks [MAN]) et de réseaux à aire étendue[35] à l'échelle de pays entiers. L'interconnexion de tous ces réseaux a pour effet de créer un espace virtuel aux dimensions de la planète. Les administrateurs de réseaux exercent toutefois un certain contrôle sur les accès et sur ce qui transite par leur réseau en provenance ou à destination de l'extérieur.

Les réseaux ont la possibilité de déterminer des politiques d'information. C'est généralement par le truchement de ces politiques, parfois explicitées dans des documents officiels ou dans les contrats d'adhésion que signent les membres ou les clients que les administrateurs de réseaux font connaître leur ligne de conduite sur des questions comme :

- le caractère privé du courrier électronique;
- les conditions d'utilisation des logiciels disponibles sur le réseau
- l'obligation d'utiliser son nom véritable;
- le droit de faire de la publicité commerciale;
- le droit d'utiliser les ressources du réseau pour des fins personnelles

34. Diane W. Savage explique que : «A LAN is a data communications facility that interconnects a number of data transmitting devices, like computers and terminals (these transmitting devices are frequently referred to as «nodes» and allows for the exchange of data.» Voir : Diane W. SAVAGE «Law of the LAN» [1993] 9 *Computer & High Technology Journal*, 193, 194.

35. Tracy LAQUEY, *The Internet Companion- A Beginner's Guide to Global Networking*, Reading Mass., Addison Wesley, 1993, p.21.

- la responsabilité pour les comportements des abonnés ou des clients.

Doug Schuler[36] identifie les questions suivantes qui peuvent être envisagées dans la mise en place de politiques relatives à l'accès, à l'usage et aux contenus véhiculés dans un réseau. Il écrit que :

> An information policy must anticipate and address questions and issues such as the following :
>
> How private is my email?
>
> Can you deny me access to the community network?
>
> Can I post «adult material»?
>
> Do I have to use my real name?
>
> How can I register a complaint against a moderator?
>
> I'm receiving abusive email. Can you put an end to it?
>
> I'd like to use the network to advertise my product. Is that OK?
>
> I have a commercial database service. Canyou let people login to it?
>
> The doctor in your question and answer forum gave you bad advice. I'm suing you!
>
> Someone reprinted my posting in a magazine without my permission!
>
> Somebeody on your network posted stolen credit card numbers. We're confiscating your equipment!

Schuler ajoute que ces questions et bien d'autres reflètent les différentes sortes de conflits qui peuvent se manifester dans un réseau qu'il s'agisse d'un réseau communautaire ou d'un réseau dédié à des

36. Doug SCHULER, «Community Networks : Building a New Participatory Medium», *Communications of the ACM*, january 1994, vol 37, no 1, p.39.

fins plus spécifiques. Il constate que plusieurs de ces questions n'ont pas jusqu'à présent trouvé de réponse faisant l'unanimité.

Ainsi le gestionnaire de réseau assume une bonne part du fardeau de délimiter les conditions d'accès au réseau et de la mise en place de mesures destinées à prévenir et éventuellement à faciliter le règlement des conflits.

L'ampleur des responsabilités incombant à l'administrateur du réseau dépend en bonne partie de la vocation du réseau. Certains réseaux sont définis comme étant uniquement un conduit d'acheminement des informations. D'autres se considèrent responsables des contenus qui s'y retrouvent.

Pour faciliter la détermination de la nature et de l'intensité des obligations assumées par les réseaux, on peut avoir recours à des métaphores permettant de les situer à partir des analogies qu'ils présentent avec des situations déjà connues.

Un réseau peut être envisagé comme un conduit de communication. Il joue alors un rôle semblable à un transporteur de télécommunications. Il offre des possibilités de transmission à autrui mais n'exerce aucun droit de regard sur les contenus véhiculés. Sa responsabilité découlant des informations circulant dans le réseau est alors mineure. On est dans la situation d'une entreprise de téléphone qui fournit la ligne téléphonique par laquelle se répandrait une information dommageable.

À l'autre extrémité du continuum, l'administrateur du réseau peut se reconnaître une responsabilité pour ce qui transite dans le réseau dont il a la maîtrise. On est alors dans la situation d'un réseau qui se définit comme un diffuseur-éditeur : il se comporte comme s'il disposait d'un droit de regard sur ce qui est transmis sous ses auspices.

Par exemple, en octobre 1990, Prodigy annonçait une nouvelle tarification pour les messages transmis par courrier électronique via son réseau. Un groupe d'usagers afficha un message dans un babillard électronique du réseau protestant contre cette tarification et appelant à un boycott des annonceurs. Prodigy répliqua en interdisant de tels messages sur son réseau et alla même jusqu'à

interrompre le raccordement des protestataires ayant continué leur campagne en faisant usage d'autres moyens[37].

Une métaphore intermédiaire est celle de la bibliothèque. Les réseaux électroniques constituent des environnements qui ressemblent à des bibliothèques. Un bibliothécaire peut se sentir concerné par le fait que certains livres de sa collection sont susceptibles de causer des torts. Il n'assume toutefois pas de responsabilité pour tout le contenu de ce qui se trouve sous sa garde. Il lui incombe toutefois de faire preuve de diligence pour retirer les informations qui lui sont signalées comme étant dommageables ou manifestement en infraction avec les règles établies lorsqu'il en a connaissance. C'est cette approche qui a été retenue dans l'affaire *Cubby v. Compuserve.*

Dans *Cubby v. Compuserve*[38], le réseau Compuserve était poursuivi comme co-défendeur dans une action en diffamation. Ce recours découlait d'informations publiées dans une lettre d'information électronique intitulée «Rumorville USA». Cette lettre d'information était publiée par un abonné du réseau qui n'avait aucun autre lien avec Compuserve. Le juge Leisure exonéra Compuserve en constatant qu'en l'espèce :

> Compuserve has no opportunity to review Rumorville's contents before DFA uploads it unto Compuserve's computer banks, from which it is immediately available to approved CIS subscribers. Compuserve receives no part of any fees that DFA charges for access to Rumorville, nor does Compuserve compensate DFA for providing Rumorville to the Journalisme Forum; the compensation Compuserve receives for making Rumorville available to its subscribers is the standard online time usage and membership fees charged to all CIS subscribers, regardless of the information services they use.[39]

37. Edward V. DI LELLO, «Functional Equivalency and Its Application to Freedom of Speech on Computer Bulletin Boards», [1993] 26 *Columbia Journal of Law and Social Problems*, 199, p. 207.

38. *Cubby inc. v. Compuserve Inc.*, (1991) 776 *F. Supp.*, 135; Voir aussi : SASSAN, Anthony J., «Comparing apples to oranges :The need for a new media classification (case note) Cubby v. Compuserve Inc. 776 F. Supp. 135 (S.D.N.Y. 1991)», (1992) 5 *Software Law Journal* 821..

39. *Id.* p. 137

Dans la mesure où Compuserve ne pouvait avoir connaissance du caractère dommageable de l'information transmise, elle n'assume pas de responsabilité à cet égard. Toutefois, lorsque le réseau acquiert la connaissance du caractère dommageable d'informations qui y sont véhiculées, il lui incombe de faire le nécessaire pour qu'elles soient retirées. Comme l'explique Di Lello :

> Judge Peter K. Leisure applied the technique of «functional equivalency» to categorize an on-line information service and thus determine the legal standard applicable to it. The plaintiff in Cubby advanced a theory that Compuserve, an online information service that permits subscribers to access hundreds of different specialized databases, was a publisher rather than a distributor and therefore liable for any defamatory statements published. Judge Leisure determined, however, that defendant Compuserve is functionnally equivalent to a news distributor, such as a bookstore, library, or newsstand. Once that functional equivalency was established, relevant precedent led the court to the inevitable conclusion that Compuserve was not liable for defamatory statements that appeared in a database it offered to subscribers.[40]

Une telle approche mène à conclure que l'ampleur de la responsabilité de l'administrateur de réseau est étroitement liée au degré de contrôle qu'il exerce ou est réputé exercer sur l'information transmise ou autrement disponible sur son réseau. C'est dire l'importance cruciale de la qualification du rôle assumé par les fournisseurs d'informations.

4.3 Le fournisseur d'information

Les fournisseurs d'information sont de plusieurs types. À la limite, dans les réseaux ouverts, tout le monde peut devenir un fournisseur d'information. L'individu doté d'un ordinateur et de logiciels appropriés peut expédier du courrier électronique à une pluralité de personnes ou encore mettre en place un babillard électronique. Il devient dès lors difficile de distinguer ce qui constitue de la diffusion de masse et de la correspondance de caractère privé.

40. DI LELLO, *loc cit.*, p 210-211.

Les usagers sont aussi, en tant que tels, des fournisseurs d'information. Soit qu'ils entreprennent de diffuser de l'information par le truchement de listes ou par courrier électronique. On parle alors de fourniture volontaire d'information. Mais en certaines circonstances, les usagers sont fournisseurs involontaires d'information. Les communications informatiques laissent des traces. Il est en effet possible et même facile de tenir et de compiler un journal des connexions et des transactions réalisées par chacun des utilisateurs. En ce sens, les utilisateurs fournissent, par leur activité dans le réseau, des informations utiles pour diverses fins de prospection, de surveillance, de détermination de profils de consommation etc.[41]

On trouve dans les réseaux informatiques une multitude de lieux de diffusion et d'échange d'informations. Leur désignation comme babillards électroniques évoque bien leur nature : les usagers raccordés à un réseau y inscrivent des informations qui, de ce fait, deviennent accessibles à tous les autres usagers. Les babillards électroniques, aussi appelés listes, sont soit ouverts, accessibles à tous les usagers du réseau, ou fermés, on y accède sur invitation ou moyennant certaines conditions.

Pour cerner le statut des babillards électroniques, il faut se demander quelle est l'ampleur du contrôle que le maître de la liste exerce sur les informations qui s'y retrouvent. Si l'on se reporte aux critères énoncés dans la décision *Cubby*, le niveau de contrôle ou de supervision exercé par le maître du babillard électronique serait déterminant. À la vérité, il est difficile d'exclure la responsabilité du maître du babillard électronique dès lors que celui-ci exerce un pouvoir de décision sur l'affichage des messages. Cette grille permet de déterminer le niveau de responsabilité qui incombe aux responsables de listes ouvertes, des listes fermées et autres babillards électroniques. Leur responsabilité est étroitement liée au degré de contrôle qu'ils exercent sur l'affichage de l'information.

41. FLAHERTY, David H., *Telecommunications privacy : A report to the canadian radio-television and telecommunications commission*, London, 1992, 140 p.; CRUSE JR., Rubin E., «Invasion of privacy and computer matching programs : A different perspective», (1992) 11 *Computer/Law Journal* 461; KAPLAN, Marilyn R., «Commercial speech and the right to privacy : Constitutional implications of regulating unsolicited telephone calls», (1980) 15 *Columbia Journal of Law and Social Problems* 277; GROUPE DE RECHERCHE INFORMATIQUE ET DROIT, *L'identité piratée*, Montréal, La Société québécoise d'information juridique, 1986.

La manière dont le droit envisage les situations de communication varie selon que le message est diffusé au grand public ou seulement échangé entre deux interlocuteurs. Le droit traite la conversation privée de manière différente de la diffusion d'informations vers le public. Selon les problèmes soulevés, la communication de messages par réseaux informatiques est assimilée, soit à la conversation téléphonique, soit aux services de télévision, ou encore aux revues ou aux magazines.

4.3.1 Médias écrits, médias électroniques ou conversations privées?

Il y a des différences importantes dans la manière dont est envisagée, juridiquement, la conversation, la diffusion au moyen de l'écrit, l'usage des fréquences radio et les communications ayant lieu dans les réseaux. D'où l'importance de la question du régime applicable aux babillards électroniques. Pour la délimitation de leurs responsabilités, les lieux de diffusion d'information que sont les babillards électroniques doivent-ils être régis par les principes applicables aux médias imprimés, par ceux qui régissent les médias électroniques ne seraient-ils pas tout simplement assimilables à la conversation privée ou, enfin, ne sont-ils pas dans une catégorie différente de ces trois premières?

– Le régime de droit commun : les médias écrits

Les médias écrits diffusés sont assujettis à un régime de liberté éditoriale. À l'égard des imprimés, il est reconnue une liberté d'entreprendre la publication sans entrave autres que celles qui sont raisonnables dans les sociétés démocratiques. La liberté éditoriale est la forme que prend la liberté d'expression lorsqu'elle s'applique aux médias en tant qu'entités. Les tribunaux protègent le pouvoir décisionnel de l'éditeur de publier, sans l'intervention des autorités étatiques[42]. L'arrêt *Gay Alliance Toward Equality* c. *Vancouver Sun*[43] est l'un des rares à avoir traité de la liberté éditoriale dans le contexte canadien. Le juge Martland, écrivant au nom de la majorité, reprend un passage de la décision américaine *Miami Herald Publishing Company* c. *Tornillo*[44], estimant que cette analyse est utile pour examiner un des éléments essentiels de la liberté de la

42. *Renvoi sur les lois de l'Alberta* [1938] R.C.S. 100.

43. [1979] 2 R.C.S. 435.

44. 418 U.S. 241 (1974).

presse. Il en conclut que «le droit a reconnu la liberté de la presse de diffuser ses opinions et ses idées et de choisir ce qu'elle publie».

Le statut des médias écrits est structuré autour des principes du droit applicable à toutes les autres activités (le droit commun); on exclut, en principe la censure préalable et les régimes d'autorisation. Les principes généraux de la responsabilité civile et de la responsabilité pénale régissent les activités des médias écrits. Ces principes déterminent un ensemble d'interdits et aménagent le régime de la responsabilité pour les informations diffusées.

Dans l'hypothèse où l'on considère les fournisseurs d'information comme des médias écrits, leur responsabilité serait celle qui découle des principes applicables aux médias écrits. Les règles générales découlant du droit civil et du droit pénal s'appliquent ou ont vocation à s'appliquer aux communications dans les réseaux électroniques.

Le droit de la plupart des pays occidentaux appréhende les messages en les catégorisant selon le contexte de leur diffusion. Par exemple, un message pornographique échangé dans l'intimité ne sera pas traité de la même façon que s'il était diffusé à la télévision aux grandes heures d'écoute[45]. Ces catégories sont souvent fondées sur les intérêts et valeurs qu'il est nécessaire de protéger lors de la circulation de l'information; le droit appréhende donc les messages en fonction des intérêts et des droits qu'ils sont susceptibles d'affecter.

Les principales règles de droit relatives aux messages susceptibles d'être diffusés dans de tels espaces ouverts des réseaux portent sur :

45. BEALL, Robert, «Developing a coherent approach to the regulation of computer bulletin boards», (1987) 7 *Computer/Law Journal* 499; FAUCHER, John D., «Let the chip fall where they may :Choice of law in computer bulletin board defamation cases», (1993) 26 *U. C. Davis Law review* 1045; GILBERT, Jonathan, «Computer bulletin board operator liability for user misure», (1985) 54 *Fordham Law Review* 439; JASSEM, Harvey C., «Scrambling the telephone : The FCC's dial-a-porn regulations», (1988) *Communications ant the Law* 3; JOHNSON, Deborah G., «The public-private status of transactions in computer network», dans *The Information web : Ethical and social implications of computer networking*, GOULD, Carol C. (Ed.), Boulder CO, Westview Press, 1989, pp. 37-55.

- L'intégrité du processus judiciaire, les règles sur le huis clos et les ordonnances de non publication
- L'atteinte à la réputation [diffamation]
- L'atteinte à la vie privée
- L'outrage au tribunal
- Les lois générales interdisant la diffusion de certains types d'informations : ces lois sont plus ou moins nombreuses selon les pays et portent sur des matières qui peuvent être fort diversifiées.
- L'obscénité
- La propagande haineuse
- La diffusion de signes et symboles discriminatoires
- Le harcèlement
- La contrefaçon d'oeuvres protégées par le droit d'auteur

Ce ne sont là que les principaux domaines sur lesquels il existe des règles de droit concernant la circulation d'informations susceptibles de se retrouver dans des sites électroniques. Il va sans dire qu'il n'existe pas encore d'analyse systématique de la manière dont ces ensembles de règles de droit trouvent ou non application dans des environnements comme les réseaux ouverts[46].

Le principe de responsabilité implique que la personne qui possède la maîtrise des contenus réponde en tout temps de ce qui y serait dommageable ou contraire aux lois. Dans le régime des médias écrits, c'est l'éditeur qui porte cette responsabilité. En contrepartie,

46. Plusieurs des questions relatives à la responsabilité des médias, notamment au plan pénal, sont traitées dans : Robert MARTIN et G. Stuart ADAM, *A Sourcebook of Canadian Media Law*, Ottawa, Carleton University Press, 1989; Nicole VALLIÈRES et Florian SAUVAGEAU, *Droit et journalisme au Québec*, Montréal, Édi-GRIC-FPJQ, 1981; Clare F. BECKTON, *The Law and the Media in Canada*, Toronto, Carswell, 1982; Michael G. CRAWFORD, *The Journalist's Legal Guide*, Toronto, Carswell, 1986; Pierre TRUDEL, *Droit de l'information et de la communication, Notes et documents*, Montréal, Éditions Thémis, 1984.

il possède la liberté éditoriale : il n'a pas l'obligation de diffuser ce qui lui est soumis et on ne peut le contraindre en ce sens.

– Le régime des médias radiophoniques et télévisuels

Si l'on devait retenir que les lieux électroniques de diffusion sont assimilables aux médias électroniques comme la radio et la télévision, ils seraient assujettis en plus des obligations qui découlent du droit commun, à certaines règles plus contraignantes.

Par exemple, les entreprises de radiodiffusion sont l'objet d'une surveillance et doivent agir en conformité avec différents principes et objectifs énoncés dans la *Loi sur la radiodiffusion*. Ces principes viennent s'ajouter aux règles découlant du droit commun. Au nombre de ces principes, il y a le principe de l'équilibre qui a des échos dans plusieurs aspects des activités des radiodiffuseurs. On y réfère notamment dans les règles à suivre en matière de traitement des controverses à la radio et à la télévision[47].

La rareté des fréquences radioélectriques utilisées pour la radio et la télévision justifie traditionnellement le traitement différent que réserve le droit aux médias électroniques[48]. Au Canada, le caractère public des fréquences est invoqué pour justifier les limites plus étendues à la liberté d'expression dans les médias électroniques. Les textes internationaux proclamant la liberté d'expression reconnaissent la possibilité d'un traitement différent pour les médias électroniques et le droit des États à assujettir l'accès à l'usage des fréquences de radiodiffusion à un régime d'autorisation préalable. Ainsi, la Convention européenne des droits énonce que l'affirmation de la liberté d'expression n'empêche pas les états de soumettre les entreprises de radiodiffusion à un régime d'autorisation. Toutefois, le régime alors établi doit respecter la liberté d'expression[49].

47. TRUDEL et ABRAN, *Droit de la radio et de la télévision*, précité, ch. 9.

48. Pierre TRUDEL et France ABRAN, «Le caractère public des fréquences comme limite à la liberté d'expression» à paraître dans [1994] *Media and Communications L. R.*, mai 1994.

49. François JONGEN, «La liberté d'expression dans l'audiovisuel : liberté limitée, organisée et surveillée» (1993) *Rev. trim.dr.h.* 95-117; Maguelonne DEJEANT-PONS, «La jurisprudence en matière de liberté d'expression audiovisuelle dans le cadre de la Convention européenne des droits de l'homme», dans Charles DEBBASCH et Claude GUEYDAN, *La régulation de la liberté de la communication*

Aux États-Unis, il est admis que les médias de radio et de télévision, en raison de leurs caractéristiques propres, peuvent être considérés différemment des autres médias à l'égard des garanties constitutionnelles de la liberté d'expression[50]. C'est principalement autour de la rareté des fréquences de radiodiffusion que se sont élaborés les raisonnements judiciaires concluant que la réglementation de la radiodiffusion était en accord avec les garanties du Premier Amendement. Au Canada, cet argument est parfois invoqué, bien que les tribunaux n'aient jamais eu l'occasion de l'analyser. Il ressort cependant de l'histoire de la réglementation de la radiodiffusion canadienne que celle-ci ne puise pas ses justifications uniquement dans la rareté des fréquences; la nécessité d'assurer la protection de la souveraineté nationale a été identifiée comme le motif principal de l'intervention de l'État en ces

audiovisuelle, Paris, Économica, Presses universitaires d'Aix-Marseille, 1991, 285-328; Albert NAMUROIS, «Aspects du droit de la radio et de la télévision dans le monde, en rapport avec la liberté d'expression», (mai 1980) 27 *Études de radio-télévision* 1-42; Marc FALLON, «La radio et la télévision face au juge européen», (1987) 47 *Annales de droit de Louvain*, 153; Sydney W. HEAD, *World Broadcasting Systems — A comparative Analysis*, Belmont, Wadsworth, 1985, p. 377 et suiv.; Donald R. BROWNE, *Comparing Broadcast Systems*, Ames, Iowa State University Press, 1989.

50. Pour mieux cerner la nature et la portée de certains droits désormais garantis dans les textes constitutionnels, le recours aux analyses et aux précédents américains peut s'avérer fort utile. Il est clair que ces précédents n'ont aucunement valeur liante en droit canadien; les législations américaines sont souvent passablement différentes de celles qui prévalent au Canada. Aussi, ces précédents ne sont jamais utilisés afin de prescrire ce qui est ou ce qui devrait être. Ils servent surtout comme indices de la manière dont se définissent les droits fondamentaux ayant valeur supra-légale. Dans *R. c. Keegstra*, [1990] 3 R.C.S. 697, la Cour suprême indique la mesure dans laquelle il est de bon aloi d'avoir recours aux précédents américains. Le juge en chef Dickson (telle était alors sa fonction) note qu' : «aux États-Unis, un ensemble de droits fondamentaux bénéficie d'une protection constitutionnelle depuis plus de deux cents ans. Il en résulte donc une immense expérience pratique et théorique dont les tribunaux canadiens ne devraient pas faire abstraction. Par ailleurs, nous devons examiner le droit constitutionnel américain d'un oeil critique» [...]. Le juge L'Heureux-Dubé, dans la décision *Comité pour la République du Canada c. Canada*, [1991] 1 R.C.S. 139, écrit qu'«il peut être utile de se pencher sur l'expérience américaine, non pas en vue d'appliquer aveuglément leurs décisions, mais plutôt pour tirer profit d'un processus dont elles sont le fruit».

matières[51]. Mais en tout état de cause, le statut des médias électroniques est passablement différent de celui des médias écrits.

La question qui se pose est celle de savoir si les lieux électroniques de diffusion d'information devraient être assimilés à des médias de radiodiffusion ou soumis au régime de la presse écrite. Pour répondre à ce genre d'interrogation, il faut procéder à l'analyse des caractéristiques de ces environnements et déterminer dans quelle mesure les justifications sur lesquelles s'appuyait traditionnellement la réglementation de la radio et de la télévision tiennent encore à l'égard de ces nouveaux médias.

– Les conversations privées

La conversation suppose principalement une relation souhaitée par tous ceux qui y prennent part et se déroule dans un contexte privé; elle échappe presque totalement au droit. Hormis les préceptes de bienséance qui échappent presque toujours à l'emprise du droit étatique, il n'y a pas vraiment d'encadrement juridique spécifique pour la conversation. Lorsqu'elle a lieu par le truchement des réseaux de télécommunication, la conversation est même protégée de certaines intrusions.

L'étude du statut juridique de la conversation et, par extension, à la correspondance, suppose de porter une attention particulière à la notion de vie privée[52]. Il existe en effet un ensemble d'informations qui, en des circonstances données, sont inclues dans le champ protégé de la vie privée. Cet ensemble est délimité par les nécessités qu'impose l'exercice d'autres droits et libertés, comme la liberté d'expression. De ces nécessités résultent les limites au droit à la vie privée[53].

51. TRUDEL et ABRAN, «Le caractère public des fréquences comme limite à la liberté d'expression», précité.

52. Steven WINTERS, «The New Privacy Interest : Electronic Mail in the Workplace», [1993] 8 *High Technology L. J.*, 197.

53. Patrick A. MOLINARI et Pierre. TRUDEL, «Le droit au respect de l'honneur, de la réputation et de la vie privée : Aspects généraux et applications», dans Formation permanente, Barreau du Québec, *Application des chartes des droits et libertés en matière civile*, Cowansville, Yvon Blais, 1988, pp. 197-231. Pierre TRUDEL et France ABRAN (éds), *Droit du public à l'information et vie privée : deux droits irréconciliables?*, Montréal, Éditions Thémis, 208 p.; Pierre TRUDEL, «La protection de la vie privée et de l'image aux États-

Dans le contexte des correspondances privées, il paraît normal de poser d'entrée de jeu que le principe du droit au respect de la vie privée s'oppose aux intrusions et aux pratiques de surveillance. L'article 36 du Code civil du Québec précise d'ailleurs que :

> 36. Peuvent être notamment considérés comme des atteintes à la vie privée d'une personne les actes suivants :
>
> [...]
>
> 2. Intercepter ou utiliser volontairement une communication privée;
>
> 3. Capter ou utiliser son image ou sa voix lorsqu'elle se trouve dans des lieux privés;
>
> 4. Surveiller sa vie privée par quelque moyen que ce soit;
>
> [...]
>
> 6 Utiliser sa correspondance, ses manuscrits ou ses autres documents personnels.

En contrepartie, on ne saurait tenir responsable le transporteur ou l'opérateur de réseau en raison des dommages résultant éventuellement de la circulation d'information dans le cadre de conversations privées. La responsabilité de ces informations n'incombe logiquement qu'à celui qui a décidé de les diffuser. Pourtant, les maîtres de réseaux ne suivent pas tous des pratiques qui

Unis» dans : INSTITUT DE FORMATION CONTINUE DU BARREAU DE PARIS, *Liberté de presse, respect de la vie privée et de l'image en droit comparé*, Supplément de la *Gazette du palais*, 1992, pp. 14 à 24; Pierre TRUDEL, «Des données informatiques personnelles aux données informatiques génétiques», dans B.KNOPPERS, L.CADIET, C.M. LABERGE, *La génétique humaine : de l'information à l'informatisation*, Paris, Litec, 1992, pp. 355-366. C'est sans doute dans l'affaire *R c. Dyment* [1988] 2 R.C.S. 417 que l'on trouve l'énoncé le plus détaillé sur l'ampleur de la protection dont jouit la vie privée dans notre droit constitutionnel. Le juge La Forest y affirme l'existence du droit à la vie privée en matière d'information et ce, non seulement en ce qui a trait au droit du citoyen de s'opposer à une intrusion physique dans son domicile ou sur sa personne mais aussi au droit de sauvegarder sa dignité.

découlent avec cette façon de voir. Par exemple, aux États-Unis, l'on reconnaît un certain droit aux employeurs de procéder à des fouilles dans les effets personnels des membres du personnel, ce qui inclurait le courrier électronique[54].

Ainsi, les maîtres de réseaux qui s'estiment autorisés à fouiller sans motif délimité le courrier électronique de toute personne rattachée au réseau s'exposent à devoir subir un standard de responsabilité plus rigoureux : on pourrait logiquement leur tenir rigueur des dommages causés par les informations qu'ils se sont donnés le droit de surveiller.

Le harcèlement constitue une autre facette du droit à la vie privée. En se fondant sur les approches développées au sujet des appels téléphoniques importuns, il est possible d'entrevoir que le recours au courrier électronique afin de harceler des personnes, leur expédier des messages désobligeants ou agressifs engendre la responsabilité de la personne qui se rend responsable de tels agissements.

4.3.2 Un amalgame de médias écrits de médias électroniques et de conversation

Les règles de droit relatives à la circulation de l'information ont traditionnellement traité de façon passablement distincte les situations de diffusion vers le public et les situations assimilables à une conversation de nature privée. La communication par réseaux informatiques grand public engendre des situations qui sont aux confins de la conversation et de la diffusion; elles possèdent les caractéristiques que l'on retrouve dans plusieurs situations juridiques selon des dosages qui varient. Lorsqu'on passe en revue les standards à partir desquels peut être déterminée la responsabilité des fournisseurs d'informations, on perçoit vite le caractère mixte de leur statut, eu égard aux catégories juridiques traditionnelles. S'agit-il de conversation ou de diffusion de masse?

Dans un environnement de réseaux ouverts, les rôles sont moins définis : les transporteurs, les maîtres de réseaux et les fournisseurs d'information sont tous susceptibles de jouer, en des circonstances spécifiques, un rôle différent de celui qu'ils jouent en temps normal.

54. WINTERS, *loc. cit.*

Tous ceux qui participent aux échanges d'information dans les réseaux ouverts le font à des titres variables selon les circonstances. Pour déterminer les droits et responsabilités de ces acteurs, il importe donc de se livrer à une démarche de qualification de ce qu'ils font. Plus ils exercent un degré considérable de maîtrise sur les informations, plus ils sont susceptibles de répondre des informations dommageables ou des informations engendrant une responsabilité pénale. Se pose alors la question de savoir si la responsabilité du fournisseur d'information est stricte : on se demande quel contrôle il est en mesure d'exercer ou relative : quel contrôle avait-il l'habitude d'exercer ou encore, quel contrôle une personne raisonnable jugerait-elle approprié d'exercer.

Ce modèle de détermination de la responsabilité incombant aux acteurs étant posé, il faut ensuite déterminer quelles sortes d'obligations doivent leur être imposées et surtout, par quelles techniques. Enfin, il faut identifier des mécanismes appropriés de résolution des conflits.

CONCLUSION

La nécessité de protéger les droits fondamentaux et les valeurs essentielles de respect de la dignité des personnes ne disparaît pas avec l'avènement des réseaux ouverts d'information. Il en est de même de plusieurs motifs pour lesquels on juge nécessaire de réguler les comportements. Aussi, il faut sortir du discours simplificateur selon lequel seules les règles du marché seraient susceptibles de procurer les régulations dans cet univers virtuel. Comme ces environnements sont par nature de dimensions mondiales, ils ne peuvent être appréhendés avec les réflexes dérivés des approches juridiques traditionnelles. Ils peuvent encore moins être examinés à partir seulement d'une approche étroitement descriptive des règles de droit.

La protection des droits et des valeurs dans des environnements ouverts requiert une analyse systématique des raisons pour lesquelles il est nécessaire de contrôler la circulation de certaines informations de même qu'une analyse rigoureuse des techniques possibles ou envisageables de protection.

Par-delà les difficultés de concevoir des mécanismes de prévention et d'arbitrage des conflits, il faut reconnaître qu'en certaines circonstances, la circulation de l'information est susceptible d'engendrer des dommages et des conflits. Les conflits peuvent être

pris en charge suivant trois modèles d'élaboration et d'application des règles que Perritt identifie de la façon suivante :

- an authoritarian model, in which a supplier of network services, like a corporate employer, compuserve or WESTLAW, sets rules for access and us unilaterally;

- a democratic model, in which a voluntary association of networks users, bulletin board operators or trade association members set rules through informal social norms or more formally through multiparty agreements; and

- a formal legal model, in which contract offers and acceptances, tort law duties, legislative statutes and administrative agency regulations define acceptable conduct.[55]

Bien entendu, ces différents modèles sont interreliés. Ils n'existent jamais à l'état pur. Les règles définies par les entités et regroupements privés sont, elles-mêmes ultimement soumises aux règles de droit relevant de l'État.

L'imputation de la responsabilité pour les conséquences de la diffusion des informations dommageables continuera d'être le principal mécanisme régulateur. Mais l'imputation de la responsabilité à une entité suppose la possibilité d'identifier les acteurs qui ont la maîtrise de l'information dans les divers lieux de cet environnement virtuel. Certes, il est impossible de supprimer complètement la circulation de l'information et les participants aux réseaux ouverts ont toujours une possibilité de rechercher ailleurs l'information dont la circulation est ici encadrée ou interdite. Ils assument toutefois la responsabilité de la dissémination de l'information sur les territoires nationaux.

Au nom de cette responsabilité, les maîtres de réseaux et autres acteurs exerçant une certaine maîtrise de l'information vont trouver sans doute opportun de se donner des règles de conduite qu'ils chercheront à imposer à leurs partenaires. Il est grand temps de se mettre à l'analyse des processus d'émergence et d'application de ces normes de conduite auto-générées plutôt que de continuer de répéter

55. Henry H. PERRITT jr, «Dispute Resolution in Electronic Networks Communities» [1993]38 *Villanova L.R.*, 349, p. 354

que ces normes non étatiques n'ont pas de force juridique. On ne peut à la fois faire le constat de la relative incapacité de la réglementation étatique à procurer tous les équilibres nécessaires dans les environnements ouverts et se refuser à la meilleure compréhension des mécanismes alternatifs de régulation qui ne se confondent pas avec les simples codes de complaisance ou une «éthique» de bon aloi.

CONCLUSION