Université de Montréal

Spamming en Cyberespace : à la recherche du caractère obligatoire de l'autoréglementation

par
Éric Labbé

Faculté de droit

Mémoire présenté à la Faculté des études supérieures
en vue de l'obtention du grade de
Maître en droit (LL.M.)

Juin 1999

Université de Montréal
Faculté des études supérieures

Ce mémoire intitulé:

***Spamming* en Cyberespace :**
à la recherche du caractère obligatoire de l'autoréglementation

présenté par:
Éric Labbé

a été évalué par un jury composé des personnes suivantes:

Jacques Frémont, président-rapporteur
Pierre Trudel, directeur de recherche
Karim Benyekhlef, membre du jury

Mémoire accepté le:

15 novembre 1999

Sommaire

L'envoi de courriers électroniques non sollicités, le « pollupostage » et le référencement effréné auprès d'outils de recherche présentent les caractéristiques d'activités abusives. Dans le jargon cybernétique, l'expression *spamming* est employée pour conceptualiser ce type de comportements. Ce nouveau concept suppose une exploitation indue d'une ressource et une mise à profit d'Internet à des fins promotionnelles. En cela, il dénote un besoin normatif susceptible de corriger les manquements à l'éthique des protagonistes du réseau. Proposée par la doctrine, l'autoréglementation est certainement l'approche normative qui apparaît la plus appropriée pour assurer le respect des valeurs sociales et économiques dans l'environnement décentralisé et transnational du Cyberespace.

Or, la première qualité attribuée à une solution normative est sa prévisibilité. Le droit revêt en effet un caractère obligatoire qui permet aux justiciables de prévoir l'interprétation et l'application d'une règle donnée. À ce titre, l'autoréglementation se présente comme une normativité moins certaine. Ce mémoire vise à déterminer de façon précise le caractère prévisible de cette solution. Pour ce faire, il met à profit l'analyse systémale. Cette théorie juridique permet d'étudier la prévisibilité du droit selon une échelle d'intensité.

L'examen détaillé de l'environnement Internet et de ses acteurs indique que le processus autoréglementaire souffre d'un faible degré de prévisibilité. Le caractère obligatoire de cette solution normative dépend substantiellement de la structure décentralisée des ressources Internet telles que le courrier électronique et les groupes de discussion Usenet. On remarque toutefois l'émergence de normes de régulation dont l'objectif est de stabiliser la mouvance des valeurs auquel le Cyberespace est particulièrement sujet. En cela, elles favorisent un degré de prévisibilité supérieur.

Conjuguées à l'impact normatif des mécanismes techniques, nous suggérons que la mise en ligne de normes persuasives puisse donner à la voie autoréglementaire un caractère obligatoire qu'on osait encore lui concéder.

Mots-clefs : autoréglementation, *spamming*, Internet, théorie du droit.

Table des matières

Liste des tableaux

Liste des figures

Liste des sigles et des abréviations

Sigles

AUP.....Acceptable Use Policies
FAI.....Fournisseur d'accès Internet
FTP.....File Transfer Protocol
NNTP.....Network News Transfert Protocol
RFC.....Request for Comments
SMTP.....Simple Mail Transfert Protocol
TCP/IP.....Transmission Control Protocol / Internet Protocol
UCE.....Unsolicited Commercial Email
WWW.....World Wide Web

Abréviations

Berkeley Tech. L. J..... Berkeley Technology Law Journal
Buffalo L. Rev.....Buffalo Law Review
J. Online L.....Journal of Online Law
Tex. L. Rev.....Texas Law Review
W. Va. J. L. & Tech..... West Virginia Journal of Law & Technology

Remerciements

La réalisation de ce projet de recherche n'aurait pas été possible sans l'apport de plusieurs personnes. Parmi elles, je tiens à remercier tout particulièrement mon directeur, Pierre Trudel, qui m'a encouragé à poursuivre dans cette voie moins traditionnelle de la recherche théorique et de l'analyse systémale. Je lui sais gré de ces commentaires stimulants et de son habilité à diriger ce mémoire.

Je tiens également à témoigner de ma gratitude envers ma compagne qui a corrigé avec patience les nombreuses versions de ce mémoire. Je remercie sincèrement Louise Rolland pour l'intérêt qu'elle a su susciter chez moi pour la théorie. Sans elle, ce travail aurait probablement perdu en originalité. Enfin, je désire exprimer toute ma reconnaissance à mes amis et à mon entourage qui m'ont supporté pendant la réalisation de ce mémoire.

À mes parents et à toi, ma chère Élodie.

Introduction

En raison de considérations techniques et juridictionnelles, les pouvoirs étatiques parviennent difficilement à réglementer les activités liées au Cyberespace. Plusieurs remettent en cause le rôle de l'État et envisagent l'autoréglementation. S'interrogeant sur le droit dans un environnement électronique décentralisé et transnational, on propose en effet de recourir « [...] aux normes volontairement développées et acceptées par ceux qui prennent part à une activité[1] ».

L'émergence de normes cybernétiques, telles que l'interdiction du courrier électronique non sollicité (*spamming*), et l'importance accordée aux règles contractuelles d'utilisation du réseau participent à l'élaboration d'une pensée pluraliste du droit sur Internet et à la création d'un nouveau paradigme juridique reposant sur l'observation, dans le Cyberespace, de différents types de rapports sociaux.

Cette nouvelle pensée fait école. Parmi les propositions doctrinales, on distingue d'abord l'émergence d'un système normatif plus ou moins autonome de l'ordre juridique étatique (la *lex informatica* ou *electronica*)[2]. Ce premier postulat concède aux standards techniques et aux normes développées par les internautes un caractère anational et suggère que ces règles soient considérées dans l'élaboration de toute réglementation étatique. Un modèle décentralisé d'autoréglementation opérant par l'interaction des différents acteurs d'Internet - les opérateurs de réseaux, les intermédiaires et les

---

[1] Pierre TRUDEL, « Les effets juridiques de l'autoréglementation », (1989) 19 *Revue de droit de l'Université de Sherbrooke* 251, 251.

[2] Voir Anne W. BRANSCOMB, « Cyberspaces: Familiar Territory or Lawless Frontiers », (1996) 2 *Journal of Computer-Mediated Communication*, http://jcmc.mscc.huji.ac.il/vol2/issue1/intro.html; Juliet M. OBERDING et Terje NORDERHAUG, « A Separate Jurisdiction For Cyberspace? », (1996) 2 *Journal of Computer-Mediated Communication*, http://www.usc.edu/dept/annenberg/vol2/issue1/juris.html; Dan L. BURK, « Jurisdiction in a World Without Borders », (1997) 1 *VA. J.L. & TECH.* 3, http://www.student.virginia.edu/~vjolt/vol1/BURK.htm; Benjamin WITTES, « Witnessing the Birth of a Legal System on the Net », (1995) *American Lawyer Media*, http://www.english.upenn.edu/~afilreis/law-on-net.html.

utilisateurs - interpelle également la doctrine[3]. Cette proposition est davantage tournée vers les rapports contractuels et hiérarchiques qu'engendre la structure d'Internet.

Ces propositions ont comme prémisse les difficultés posées à l'application du droit étatique aux nouvelles situations engendrées dans cet environnement électronique : les problèmes reliés au rattachement juridictionnel, l'anonymat des utilisateurs, le coût des poursuites internationales, les difficultés d'homologation, le changement rapide des nouvelles technologies, etc. La finalité des premières recherches consiste donc à proposer des voies de solutions destinées à remettre un peu d'ordre dans la boîte de Pandore numérique.

Le *self-governance* ou l'approche autoréglementaire suscitent, suite à l'observation d'un contrôle effectif de certains acteurs d'Internet, du pouvoir et de la portée de leurs sanctions, un enthousiasme partagé par plusieurs spécialistes. Cette solution a pour effet de redonner aux Cyberespace une dimension normative cohérente. Cependant, l'autoréglementation, telle qu'envisagée par la doctrine, contribue seulement à expliquer le fonctionnement du processus normatif sur Internet. Elle ne parvient pas à démontrer le caractère prévisible de la solution normative choisie. Pour cette raison, elle ne répond pas aux besoins de certitude engendrés par les difficultés actuelles reliées à l'application du droit étatique. La présente étude vise donc à établir le degré de prévisibilité de l'autoréglementation, c'est-à-dire l'intensité du caractère obligatoire des normes autoréglementaires.

Toutefois, notre analyse ne doit pas se cantonner à l'appréciation de la contrainte des règles issues du Cyberespace. Elle deviendrait, à l'instar des autres propositions, une

---

[3] Voir David R. JOHNSON, « Due Process and Cyberjurisdiction », (1996) 2 *Journal of Computer-Mediated Communication*, http://www.usc.edu/dept/annenberg/vol2/issue1/due.html; David G. POSTet D. R. JOHNSON, « Law And Borders - The Rise of Law in Cyberspace », (1996) *Stanford Law Review*, http://www.cli.org/X0025_LBFIN.html; D. G. POSTet D. R. JOHNSON, « The New 'Civic Virtue' of the Internet », http://www.cli.org/paper4.htm; D. G. POST et D. R. JOHNSON, « And How Shall the Net Be Governed? A Meditation on the Relative Virtues of Decentralized, Emergent Law », (1996), http://www.cli.org/emdraft.html; D. R. JOHNSON, « Lawmaking And Law Enforcement in Cyberspace », http://www.cli.org/DRJ/make.html.

étude misant essentiellement sur la fonction d'instrument normatif du droit et reléguant au second plan sa fonction référentielle, qui est celle de régir les représentations collectives se rattachant aux rapports sociaux concrets : le droit « [...] formalise des normes déjà là, qui sont l'expression des comportements ou des valeurs dominantes dans la société, le reflet d'une idée implicite de la normalité[4] ». Ce faisant, elles négligerait le caractère fondamental du droit qui est, selon Gérard Timsit, « [...] de signifier à l'intention de ceux auxquels il s'adresse, une permission, une obligation, une habilitation[5] ». En effet, le caractère obligatoire d'une norme ne se situe pas seulement sur le plan de la contrainte mais découle aussi de considérations se rapportant à la signification de la norme en ce qu'elle permet ou autorise[6].

Ce désintéressement de la norme en tant que signification évincerait les notions de « valeurs », « stratégies normatives » et « interprétations » pourtant essentielles dans le processus d'acceptation des règles par les destinataires. Or, dans une perspective de recours à des normes volontaires, l'acceptation des règles par les destinataires emportent plus que des considérations, elle en constitue la pierre angulaire. Si le droit est un instrument normatif qui établit des normes et en sanctionne le respect, il est également un discours référentiel qui prétend décrire la réalité en même temps qu'il la régit[7]. En tant que tel, le droit est une notion indissociable des valeurs, de leurs conflits et des circonstances qui les font naître[8].

---

[4] Danièle LOSCHAK, « Droit, normalité et normalisation », dans Jacques CHEVALIER, *Le droit en procès*, Paris, Presses universitaires de France, 1983, p. 51, à la page 65.

[5] Gérard TIMSIT, *Les noms de la loi*, Paris, Presses Universitaires de France, 1997, p. 43

[6] G. TIMSIT, *La surdétermination de la norme de droit : questions et perspectives*, dans Andrée LAJOIE, Roderick A. MACDONALD, Richard JANDA et Guy ROCHER, *Théories et émergence du droit : pluralisme, surdétermination et effectivité*, Montréal, Les Éditions Thémis, 1998, p. 99, à la page 101.

[7] D. LOSCHAK, *loc. cit.*, note 4, 54. L'auteur fait remarquer que « [l]a force agissante du droit ne réside pas seulement dans une violence physique extrinsèque ; elle s'origine (sic) aussi dans la puissance propre du discours : le droit est une parole qui s'impose comme légitime, comme vraie, bien au-delà du cercle finalement restreint de ceux auxquels chacune de ses normes, prise isolément, a vocation à s'appliquer ».

[8] G.TIMSIT, *Archipel de la norme*, Paris, Presses Universitaires de France, 1991, pp. 9-27. L'auteur y énonce l'importante différence entre les conditions de la relation parole/écriture et celles établies lors d'un échange de parole. En effet, lors d'un échange de paroles, la signification des discours échangés est pleinement préservée. À l'opposé, lorsque le texte prend la place de la parole, une triple autonomie se

Sur un réseau transnational où une pléiade d'acteurs de différents acabits acquièrent un pouvoir technique ou politique, de nouveaux conflits peuvent survenir. C'est ce qu'indique le professeur Trudel lorsqu'il a recours à la notion de rationalité, c'est-à-dire aux « [...] valeurs au nom desquelles émergent des demandes afin d'encadrer certains aspects[9] ». Ces demandes ne sont pas étrangères aux difficultés actuelles du droit étatique à préserver les valeurs naissantes et celles qui subsistent. Par conséquent, il y a lieu d'étudier la voie autoréglementaire en fonction du nouvel environnement numérique que constitue Internet[10]. À ce titre, le professeur Katsh expose l'importance des nouvelles technologies sur la normativité :

> What is most necessary is to be sensitive to the qualities of new technologies, to the capabilities they provide, and to the constraints they place on us. The viabiliy, effectiveness, and nature of law in the future depends on wether we understand the changes occuring to the law and are able to respond to them. As a skilled writer, sensitive to the power and constraints of language, or as a creative artist, working to overcome the limits of a particuliar medium, a person interested in the future of law must also be cognizant of the particular qualities of modes of expression.[11]

En plus de nous contraindre à une étude de l'influence de la technologie sur la normativité, l'exploration des circonstances et du milieu dans lesquels s'opérerait

---

crée, d'abord par rapport à l'intention de l'auteur du discours, ensuite par rapport aux destinataires, lesquels peuvent varier avec le temps, et finalement, par rapport aux circonstances économiques, culturelles et sociales de l'époque, qui limitaient alors les significations possibles (p.17). Se questionnant sur le droit, l'auteur insiste sur la fonction du langage en droit : « Renonçant à la loi de Dieu, il eût peut-être fallu pour y répondre, qu'après Babel, l'on s'interrogeât plus avant sur la langue des hommes appliquée au droit – appliquée à la dite du droit ».

[9] P. TRUDEL, France ABRAN, Karim BENYEKHLEF et Sophie HEIN, *Droit du cyberespace*, Montréal, Éditions Thémis, 1997, p. 1-1.

[10] « *The law of any given place must take into account the special characteristics of the space it regulates and the types of persons, places, and things found there* ». D. G. POST et D. R. JOHNSON, *loc. cit.*, note 3.

[11] Ethan M. KATSH, *The Electronic Media and the Transformation of Law*, Oxford, Oxford University Press, 1989, p. 268.

l'autoréglementation impose également une reconnaissance des principales manifestations de la normativité sur Internet. On ne saurait apprécier les qualités de la voie de l'autoréglementation sans identifier la nature et la portée des normes qu'elle a vocation a remplacer.

Par conséquent, il faut indiquer que les premiers utilisateurs d'Internet avaient érigé, bien avant que ce réseau ne devienne le média populaire actuel, un code d'éthique, voire des règles d'utilisation et des principes destinés à assurer un fonctionnement efficace du réseau et à promouvoir un certain ordre dans le Cyberespace. Les internautes de la première génération, scientifiques et universitaires, baptisèrent ce code Netiquette pour « l'éthique du réseau ». À cette époque, ces règles étaient largement suivies et émanaient d'un groupe homogène de personnes. Il s'agissait de règles implicites qui n'avaient pas encore d'histoire.

Lorsqu'Internet s'est démocratisé suite à la venue du Web en 1992, la Netiquette n'a pas eu l'assentiment espéré. Méconnues des nouveaux arrivants, les *newbies*, comme s'amusent à les nommer les plus initiés, certaines règles ont toutefois fait l'objet d'une plus grande publicité. Cela s'explique par les intérêts et les enjeux occasionnés par leur méconnaissance, voire les raisons pour lesquelles elles avaient été créées.

Dans bien des cas, les règles de la Netiquette ressemblent davantage à des règles de politesse qu'à de véritables règles contraignantes. Elles ont un fondement moral et un contenu variable au gré des personnes. Quelques-unes ont toutefois des fondements économiques et techniques. Celles-ci sont plus importantes aux yeux des principaux acteurs du réseau : les fournisseurs d'accès Internet (FAI), les fournisseurs de contenus, les opérateurs de groupes de nouvelles, les utilisateurs initiés, etc. La valeur que leur accordent ces acteurs en fait des règles plus connues des internautes et moins malléables

que la Netiquette en général. La reprise de ces règles au sein de codes de conduites de FAI[12] et leur présence dans certaines législations[13] indiquent leur importance.

Dans le cadre de notre étude, nous nous sommes donc intéressés à la plus importante de ces règles, l'interdiction du *spamming*. Cette règle, présente par sa nature générique dans la quasi-totalité des ressources d'Internet, constitue un précieux objet d'analyse en ce qu'elle est un révélateur d'un trait de la normativité sur Internet.

Le terme *spamming* est employé pour définir les abus quant à la fonctionnalité de l'une ou l'autre des ressources Internet. Les groupes de nouvelles Usenet, le courrier électronique et les outils de recherche forment les ressources où se manifeste le *spamming*. La plus connue de ces manifestations est le courrier électronique non sollicité ou, selon l'appellation anglaise, le *junk email*.

L'étude de la prévisibilité de la solution autoréglementaire du *spamming* doit être précédée par un cadre d'analyse détaillé. Cette tâche préliminaire consiste à venir préciser, dans un premier temps, la notion de « norme » mais également ce que nous entendons par la prévisibilité d'une règle, c'est-à-dire son caractère obligatoire. Nous établirons que cet attribut est l'apanage du droit. Par conséquent, la notion de prévisibilité aura pour effet de venir distinguer le droit de la norme en tant que « norme prévisible » (1). Dans un second temps, nous présenterons comment ces définitions

---

[12] À titre d'exemple, plusieurs codes de conduite de FAI, tel que Sympatico, ont interdit à leurs utilisateurs de représenter faussement les en-têtes de leurs articles postés sur les groupes de discussion, une règle qui provient de la Netiquette. Voir : Sally HAMBRIDGE, « RFC 1855 : Netiquette Guidelines » (Octobre 1995), http://www.sri.ucl.ac.be/SRI/frfc/rfc1855.fr.html.

[13] Plusieurs lois étatiques américaines prohibent la falsification des en-têtes de courrier électronique commercial, une activité déconseillée par la Netiquette. Voir : *Prohibited unsolicited electronic mail*, chapter 149, Laws of 1998 (55th Legislature) (Washington); *AN ACT relating to actions concerning persons; providing that a person who transmits certain items of electronic mail is liable to the recipient for civil damages under certain circumstances; providing that the district court may enjoin a person from transmitting certain items of electronic mail under certain circumstances; and providing other matters properly relating theret*, chapter 341, Laws of 1997 (69th Legislature) (Nevada); *An act to amend Section 17511.1 of, and to add Section 17538.45 to, the Business and Professions Code, and to amend Section 502 of the Penal Code, relating to advertising*, chapter 863, Statutes of 1998 (54th Legislatures) (California).

viendront circonscrire le caractère obligatoire, dans un environnement électronique, des normes relatives au *spamming* (2).

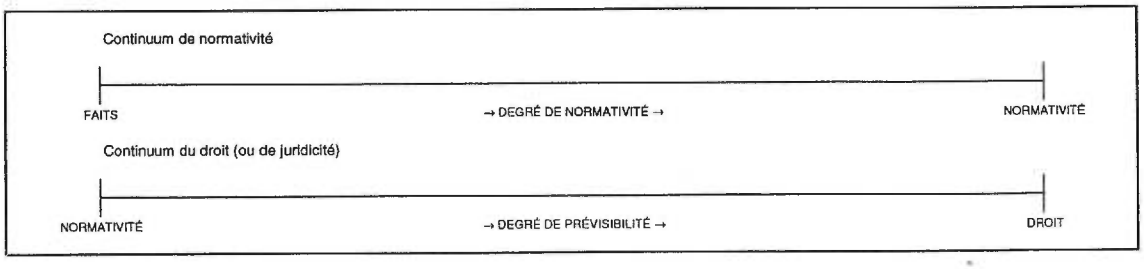
1. Les notions de norme et de droit

Définir les notions de norme et de droit met en exergue la difficulté qui subsiste à les distinguer l'une de l'autre. Cet exercice rend compte d'une traduction dichotomique de la réalité où les tons de gris entre faits, normativité et droit ne reçoivent aucune considération. Il existe en effet une distinction de nature qui empêche l'étude de concepts intermédiaires. Pourtant, la présence de certains phénomènes qui, par nature, ne peuvent être qualifiés avec précision dans l'une ou l'autre de ces catégories, suggère d'élargir la conception actuelle de la normativité et du droit (normativité prévisible) et d'établir une différence de degré plutôt que de nature.

Cet élargissement conduira à considérer le caractère plus ou moins normatif d'un fait, tel l'établissement d'une structure informatique emportant des comportements précis et généralisés chez les internautes. Il permettra également de tenir compte de règles plus ou moins prévisibles (plus ou moins obligatoires). C'est le cas, par exemple, de la règle imprécise susceptible d'être interprétée de plusieurs façons.

Dans la perspective d'une distinction de degré entre les concepts de faits, norme et droit, il est possible d'entrevoir deux continuums, celui de la normativité et du droit :

Figure 1. Continuums de normativité et de droit (Source : l'auteur)



Si l'on accepte que la normativité et le droit sont issus de processus d'émergence, de véritables continuums, il faut admettre l'imprécision d'une vision monochrome des rapports sociaux concrets. Par conséquent, une évaluation qualitative des propriétés normative (a) et juridique (b) devient nécessaire.

a. Définition qualitative de la norme.

Principale théorie du droit, le positivisme juridique maintient une opposition théorique entre le droit et les faits, écartant toute référence à la norme non juridique en la considérant comme un fait. Cette conception du droit se retrouve chez la définition kelsénienne de la norme. Celle-ci s'entend comme une obligation assortie d'une sanction. Fondée sur un syllogisme et une identité parfaite, cette définition produit néanmoins une confusion terminologique : il n'existe de normativité qu'en présence de l'État puisque la sanction est le fait de l'État[14].

La norme juridique apparaît donc comme une tautologie, une notion circulaire insatisfaisante dans la perspective d'un environnement transnational et décentralisé, difficilement contraignable au plan étatique. En effet, l'approche kelséenne de la norme nous prive de solutions normatives extra-étatiques et renie par le fait même les principaux traits du Cyberespace. Pour ces raisons, il est nécessaire d'élargir le concept de « norme » pour y inclure un « [...] *decentralized process that does not closely resemble those we have used in the past to past laws and enforce behavioral norms* [15]». Sans cet enrichissement, Internet apparaît comme un espace imperméable aux solutions normatives. Nous préférons donc opter pour la définition adoptée par le *Programme interuniversitaire de recherche sur le droit et les technologies*:

---

[14] Voir G. TIMSIT, « Sur l'engendrement du droit », (1988) *Revue de droit public* 39, 44.

[15] D. G. POST et D. R. JOHNSON, *loc. cit.*, note 3.

> [U]ne norme est un discours (plus ou moins explicite) ou un comportement, descriptif ou prescriptif, dans la mesure où cette description ou cette prescription permet d'évaluer ou de mesurer (et à la limite de sanctionner) la conformité de son sujet à son objet.[16]

Comportant plus que les normes admises par les tribunaux, cette définition procède d'une approche pluraliste[17]. Toutefois, cette précision ne règle pas la question de l'appréciation qualitative de la normativité. À ce titre, la traduction de l'opposition droit/faits en une opposition normes/faits conduirait à une impasse. Comme l'écrit Danielle Pinard avant de s'interroger sur le caractère fonctionnel de la distinction, « [...] il semble acquis que la distinction entre le fait et le droit ne repose sur aucune différence de nature - on parlera même d'un tracé qui repousse toute forme de systématisation théorique, ou encore d'une série d'accidents historiques [...][18] ». Nous n'entrevoyons aucune raison à ce qu'une distinction entre la norme et le fait ne puisse faire l'objet des mêmes critiques. C'est pourquoi il est nécessaire de relever l'existence de phénomènes dont la nature se rapproche intimement de la normativité.

Si la normativité se conçoit comme un processus d'émergence, voire un continuum, il est possible de traduire certains phénomènes comme des éléments du processus, qualifiables de faits potentiellement contributifs ou déclencheurs; bref, de faits normatifs. Ceci nous amènera à prendre en considération l'impact normatif de la technologie...[19]

---

[16] René CÔTÉ, Pierre MACKAY, G. ROCHER et P. TRUDEL, *Bilan et perspectives. Cadre conceptuel et propositions sur l'émergence des normes dans l'univers technologique*, Montréal, Édition conjointe des Cahiers du Centre de recherche en droit public et *Recherche*, 1992, p. 6.

[17] *Id.*, p. 1. Cependant, elle n'a pas le mérite de circonscrire les formes de la normativité mais en assure l'existence. En cela, elle n'est pas antinomique à la typologie de la norme proposée par R. A. Macdonald. Voir : R. A. MACDONALD, « Les Vieilles Gardes. Hypothèse sur l'émergence des normes, l'internormativité et le désordre à travers une typologie des institutions normatives », dans Jean-Guy BELLEY(dir.), *Le droit soluble; Contribution québécoise à l'étude de l'internormativité*, Paris, L.G.D.J., 1996, p. 233.

[18] Danielle PINARD, « Le droit et les faits dans l'application des standards et la clause limitative de la Charte canadienne des droits et libertés », (1989) 30 *Cahiers de droit* 137, 149. Nous omettons les notes infrapaginales.

[19] *Infra*, sous-section I, section I, chapitre I, seconde partie.

b. Définition qualitative du droit

Afin d'affranchir le droit d'une conception étatiste, il faut convenir que l'effectivité n'est pas une condition *sine qua non* de la qualité juridique d'une norme. L'effectivité désigne, selon le professeur Guy Rocher, « [...] tout effet de toute nature qu'une loi peut avoir [20]». Cette notion renvoie nécessairement à la mise en œuvre de la norme et aux sanctions étatiques, sociales et morales qui lui sont associées. À cet égard, Timsit indique que le droit n'est pas une obligation assortie d'une contrainte, cette définition tautologique ancrée au critère de la sanction, étatique selon Kelsen, et attachée à une réalité fausse de l'État « [...] monolithique, pyramidal, unitaire [et] hiérarchique [...][21] ».

Selon Timsit, une norme ne serait juridique que lorsqu'elle possède un caractère obligatoire, seul critère de la définition positiviste perméable à une conception empirique du droit. Le caractère obligatoire ou la prévisibilité d'une norme dépend de ce qu'il est tenu d'appeler la juridicité, le plan de la signification du droit. L'effectivité se situe plutôt sur un plan du droit distinct de la signification, celui de la contrainte[22]. À ce titre, Timsit explique qu'il existe, à l'égard du droit, de la signification sans contrainte et de la contrainte sans signification[23]. Par exemple, un acte de « recommandation » peut être porteur d'une règle précise dont la signification est peu discutable, sans toutefois être muni d'une sanction qui en assure le caractère contraignant. Mais une norme constitutionnelle, applicable par les tribunaux à titre de loi suprême, peut comporter une règle si imprécise qu'elle en demeure imprévisible. Le professeur considère donc

---

[20] G. ROCHER, « L'effectivité du droit », dans A. LAJOIE, R. A. MACDONALD, R. JANDA et G. ROCHER, *op. cit.*, note 6, p. 134, à la page 135. L'effectivité serait une notion plus large que l'« efficacité » d'une norme qui « [...] réfère au fait qu'elle atteint l'effet désiré par son auteur ou, si ce n'est celui-là même, à tout le moins un effet qui se situe dans la direction souhaitée par l'auteur et non pas en contradiction avec elle ».

[21] G. TIMSIT, *loc. cit.*, note 14.

[22] G. TIMSIT, *loc. cit.*, note 6. Néanmoins, le critère de la sanction pourrait influencer la détermination du caractère obligatoire.

[23] *Id.*

la définition du droit du point de vue de la signification et nous invite à une analyse systémale du droit :

> Il faut donc définir le droit par son caractère obligatoire, mais le faire de manière que cette obligation - d'une part ne soit pas nécessairement référée à l'État, que d'autre part sa portée puisse varier en fonction du degré de spécificité des inter-relations qui rendent la norme obligatoire. Or, ce caractère obligatoire de la norme n'a d'autre traduction objective que celle que lui donnent l'interprétation et l'exécution qui en sont faites.[24]

Cette définition emporte deux considérations. D'abord, la première concerne le rôle de la contrainte et de l'effectivité. Celles-ci se situent, comme l'expose Timsit, en amont ou en aval de la juridicité et constituent un problème social ou politique[25]. En somme, elles ne sont pas autant une question de droit qu'un problème d'application du droit.

La seconde considération s'impose au regard de l'exercice du pouvoir. À cet égard, la définition systémale du droit ne sous-tend pas l'existence d'un ordre juridique caractérisant une définition plus institutionnaliste. En effet, l'institutionnalisme exclut toute régulation sociale « [...] que les acteurs sociaux exercent entre eux de façon autonome et toute régulation fondée sur un pouvoir diffus exercé par une collectivité sur ses membres sans intervention directe ou distincte des détenteurs de pouvoirs[26] ». Une telle définition masquerait tôt ou tard la spécificité d'un environnement où le pouvoir est justement diffus. Dès lors, il serait impossible de faire intervenir une appréciation qualitative de la juridicité d'une norme, c'est-à-dire d'identifier son degré de juridicité. Par conséquent, choisir la conception institutionnaliste reviendrait à restreindre le droit à la dichotomie du « être ou n'être pas » juridique.

---

[24] G. TIMSIT, *loc. cit.*, note 14, 45.

[25] G. TIMSIT, *op. cit.*, note 5, p. 49.

[26] J.-G. BELLEY, « L'État et la régulation juridique des sociétés globales: pour une problématique du pluralisme juridique », (1986) 18.1 *Sociologie et sociétés* 11, p. 27. Ce constat vaut également pour la définition du droit de Guy Rocher selon Andrée LAJOIE, « La normativité professionnelle dans le droit: trajets et spécificité formelle », dans J.-G. BELLEY(dir.), *op. cit.*, note 17, p. 150, à la page 176.

N'ayant que pour seule traduction objective l'interprétation et l'application qui en est faite, le professeur Timsit indique que le caractère obligatoire (la prévisibilité) d'une norme réside dans les conditions du décodage de la norme. La norme porte une signification provenant d'un code, un répertoire des possibles, « [...] qui s'applique à elle et qui commande à l'interprétation - aux interprétations - qu'elle reçoit[27] ». Le degré de juridicité d'une norme correspond donc à la préservation de sa signification initiale en considération des conditions dans lesquelles s'effectue son interprétation et son application.

En somme, une norme aspire à un haut degré de juridicité lorsque sa signification n'est pas disséminée soit par la présence de blancs ou d'indéterminations de la norme, soit par l'existence de conditions défavorables. Cela ne veut pas dire que la juridicité d'une norme n'est jamais malléable. L'élaboration d'une règle s'effectue généralement selon certaines techniques normatives, propres à imposer la signification désirée. Le droit est donc un exercice de contrôle du décodage de la norme.

S'agissant d'une question de contrôle, il peut exister différents degrés de contrôle selon lesquels le décodage sera plus ou moins assuré, et la norme plus ou moins obligatoire. Andrée Lajoie résume les facteurs déterminants du contrôle du décodage, soit la prédétermination, la surdétermination et la codétermination :

> Ce degré de contrôle du décodage d'une règle résulte des stratégies normatives auxquelles ont recours, dans une société, aussi bien l'instance qui l'émet (précodage: degré de discrétion que réserve, à celui qui l'applique, l'auteur de la règle aussi bien quant à ses conditions d'application qu'au champ de compétence qu'elle vise) que ceux auxquels elle s'adresse (cocodage: direction donnée à la norme par son interprétation et son application).
>
> S'y superpose un *sur-codage*, résultant des contraintes qui découlent, pour l'application du droit, de la présence d'un champ

[27] G. TIMSIT, *op. cit.*, note 5, p. 46.

> de valeurs qui lui sert de support interprétatif. Ces contraintes seront nécessairement plus impératives si elles sont sous-tendues par un seul système de valeurs juridiques, un seul principe intégrateur.[28]

Selon Timsit, l'intégration qui résulte de ces trois facteurs permet d'identifier trois degrés de juridicité selon la présence des stratégies normatives de l'auteur (prédétermination) et l'existence d'un seul champ de valeur à titre de support interprétatif (surdétermination) :

> Quand il y a la fois pré- et surdétermination, l'intégration du système de contrôle du décodage des normes est maximal, le système monologique, et le degré de juridicité est le plus élevé. Quand il y a prédétermination sans surdétermination, ou surdétermination sans prédétermination, l'intégration est moindre [...]. Quand il n'y a ni pré- ni surdétermination, la codétermination joue à plein, le système est dialogique, le degré de juridicité est encore moindre, sans cependant être inexistant [...].[29]

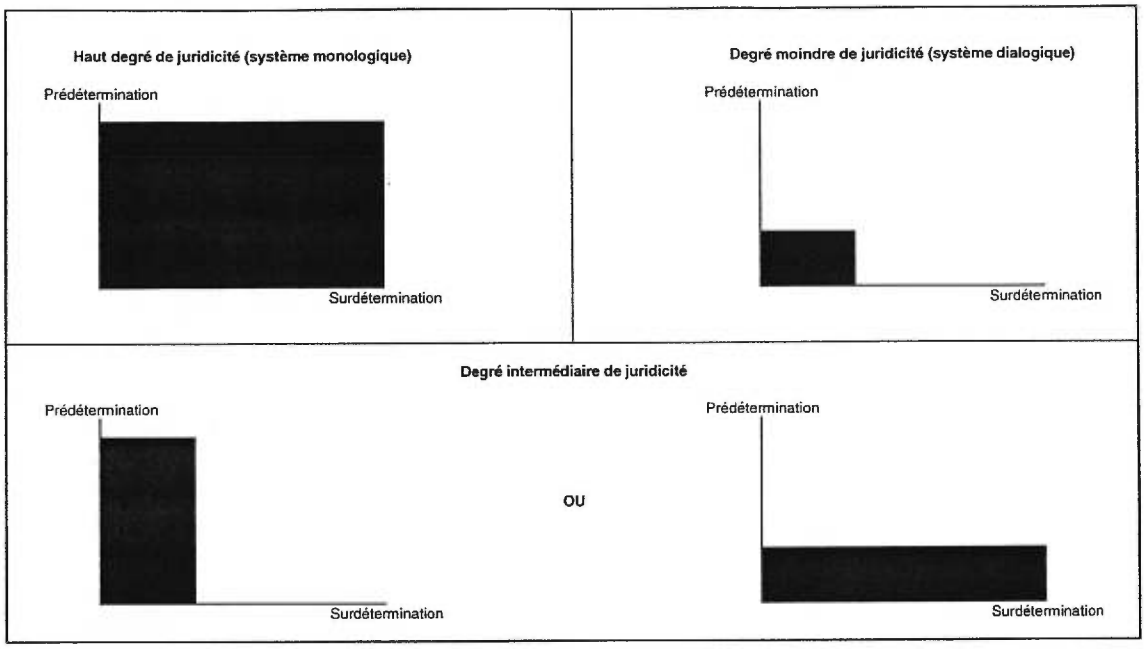
Par conséquent, si nous concluons que la solution autoréglementaire relative au *spamming* constitue une règle précise (prédétermination) interprétée et appliquée selon les mêmes croyances, valeurs et idéologies que celles qui précèdent son élaboration (surdétermination), nous devrons certifier le caractère prévisible de cette voie normative. Dans le cas contraire, l'absence de l'une de ces conditions emportera un degré intermédiaire de juridicité, la norme n'étant prévisible qu'à moitié. Si aucune de ces conditions ne se présentent, il faudra alors déduire que l'autoréglementation est le produit d'un système dialogique et que son caractère obligatoire est presque nul. Les tableaux suivants illustrent ces différentes conclusions :

---

[28] A. LAJOIE, *loc. cit.*, note 26, 177-178.

[29] G. TIMSIT, « Sept propositions pour une définition systémale du droit », (1989) 10 *Droits. Revue française de théorie juridique* 93, 95.

Figure 2. Représentation des trois degrés de juridicité (source : l'auteur)



La vérification de l'un ou l'autre de ces conclusions suppose que l'on procède à une application du continuum de juridicité à la solution autoréglementaire du *spamming*. Cet exercice requiert, dans un environnement aussi complexe que le Cyberespace, de préciser les modalités qu'emporte l'application de cette vision non traditionnelle du droit.

2. Application de la définition systémale du droit à l'interdiction du *spamming*

Les jalons que pose l'analyse systémale nécessitent, au regard de l'étude de la juridicité de l'interdiction du *spamming*, une reconnaissance des textes la prescrivant.

La recherche du sens premier, celle prédéterminée par l'auteur de la norme, est donc l'objet sur lequel portera notre étude. Elle constitue notre outil de vérification. La perte du sens premier d'une norme s'avère fatale à sa juridicité. Ainsi, notre cadre d'analyse se construit tout autour des textes proscrivant le *spamming* et des sens qui y sont inscrits.

Le droit est toutefois sujet aux doubles conditions d'immanence et de transcendance[30]. Il n'est pas que prédétermination mais aussi surdétermination. Non seulement doit-on découvrir la signification exacte des multiples manifestations du *spamming* mais également son essence : retrouver les fondements du mépris que génère un tel comportement. En effet, une signification n'est saisissable que par l'adhésion à un réseau de valeurs, déterminé par un ensemble de facteurs tels que la présence de contextes et de circonstances particuliers. Or, le réseau Internet offre justement, par sa nature hétérogène et sa forme intransitive[31], une possibilité de contextes électroniques et de circonstances particuliers. Il s'agit, en l'occurrence, des ressources Internet telles que le Web, Usenet et le courrier électronique. Chacune d'elles se caractérise par un contexte de nature et de structure propres, susceptible de faire varier le degré de juridicité des normes issues d'Internet. Ainsi, il semblerait que :

- La **nature** publique d'une ressource Internet favorise une ambiance communautaire propre au partage d'intérêts alors que la nature privée individualise les usagers. Nous supposons que le partage des intérêts entre les usagers contribue à prendre part aux mêmes valeurs, favorisant ainsi la réception de la norme par les destinataires.

- La **structure** centralisée d'une ressource autorise une interprétation et une application plus uniformes de la norme alors qu'une structure décentralisée, contrôlée par plusieurs acteurs, en permet une multitude. Nous supposons qu'une interprétation et une application par l'auteur même de la norme concourent à réduire le nombre de sens pouvant être conférés à la norme.

Nous posons donc l'hypothèse principale que les ressources centralisées et propices au développement d'intérêts communs procurent un haut degré de juridicité de

---

[30] G. TIMSIT, *op. cit.*, note 5, pp. 41-44.

[31] *Infra*, section I, chapitre II, première partie.

l'interdiction du *spamming*. Les techniques efficaces d'encodage que permettent ces ressources, l'absence d'interprétation qui en découle et la présence d'un champ de valeurs unique constituent les causes dominantes du contrôle élevé de son décodage dans ces contextes électroniques.

Cette hypothèse crée en somme quatre situations générant des degrés de juridicité différents. D'abord, une ressource centralisée et publique devrait entraîner un haut degré de juridicité de l'interdiction. À l'opposé, une ressource décentralisée et privée établirait un environnement électronique où, en raison de la présence d'une pluralité de champs interprétatifs, la préservation de la signification serait faible. Enfin, une ressource centralisée et privée, de même qu'une ressource décentralisée et publique, constitueraient des lieux favorables à un degré intermédiaire de juridicité.

Visant à éclaircir les propositions doctrinales sur l'autoréglementation d'Internet, cette étude impose une analyse du Cyberespace, des normes et de leur acceptation par les destinataires. Elle tend à démontrer que l'acceptation d'une norme par ses destinataires dépend du contexte dans lequel s'inscrit la réception de la norme. Plus précisément, elle constitue un examen des environnements informatiques et de leurs conséquences sur la normativité issue d'Internet. Elle souhaite déterminer l'influence de la nature et de la structure des contextes électroniques sur les éléments du processus normatif, voire sur les stratégies normatives des principaux acteurs, l'interprétation et l'application de la norme et les valeurs des groupes en présence.

Ces objectifs rendent nécessaires, dans un premier temps, de faire état des éléments d'analyse (partie I). Il s'agit d'exposer les sens concourants, ainsi que l'essence, c'est-à-dire les rationalités révélées par les enjeux du *spamming* (chapitre I). Devront être examinés par la suite les lieux de décodage d'Internet, les ressources, et les acteurs en présence (chapitre II).

Dans un deuxième temps, il importe de reprendre ces éléments et d'en déduire la normativité existante et le degré de juridicité y afférent (partie II). Cette dernière opération ne peut s'effectuer qu'en étudiant les techniques normatives au moment de l'encodage (chapitre I) et l'existence de champs de valeurs concurrents ainsi que la place alors laissée à la codétermination (chapitre II).

De fil en aiguille, de nouveaux usagers s'initient au monde virtuel, enthousiasmés par les nouvelles possibilités qui s'offrent à eux. Ces « cybernovices » abordent de nouveaux lieux, de nouvelles ressources. Ils cherchent à comprendre l'Outil, à trouver le mode d'emploi. Le courrier électronique est souvent la première expérience qu'ils s'offrent. D'autres préfèrent découvrir le World Wide Web, naviguer sur le Net à la recherche d'informations ou de divertissements. Certains parcourent les guides d'utilisation à la mode et d'autres, moins méthodiques, avancent à tâtons. Ils découvrent un nouveau monde.

Cette initiation participe à la création et au développement de besoins liés à une toute autre réalité. Les interactions naissantes et les structures informatiques conduisent à de nouvelles demandes normatives. La présente partie vise donc à déterminer les raisons particulières de l'interdiction du *spamming* en considération des rapports entretenus dans le Cyberespace et de l'organisation de cet environnement. Cet exercice procède d'une démarche d'exploration du réseau et des conflits qui y surviennent.

La poursuite de cette démarche est précédée de plusieurs questionnements : pourriez-vous m'indiquer comment envoyer une image par courrier électronique? Comment utilise-t-on le mode de communication Telnet? Où puis-je trouver un guide sur les groupes de discussion?

Le nouvel usager s'évertue ainsi à conquérir « l'Outil cybernétique » et son mode d'utilisation. Pour ce, il bénéficie, sur le réseau, du concours des plus initiés, de son fournisseur d'accès et d'une panoplie d'explications sous forme de questions/réponses, que l'on nomme « Foire Aux Questions » (FAQ).

Plus tard, il s'apercevra que le mode d'emploi fait parfois office de code de conduite. Une véritable grammaire qui semble, par les lectures qu'il fait et les expériences qu'il

vit, s'imposer. Il cherche donc à comprendre la Netiquette, cette fois-ci, non pas dans l'objectif d'utiliser le médium mais bien dans celui de saisir les raisons qui sous-tendent les règles choisies.

Dans sa quête, il se bute occasionnellement à des sens multiples, voire des définitions nuancées, plus ou moins précises et mouvantes. Pour ces raisons, les règles de la Netiquette lui apparaissent peut-être moins certaines et l'interdiction du *spamming* n'y échappe pas.

Il découvre effectivement que cette interdiction revêt plusieurs sens. Selon les ressources qu'il utilise, les lieux virtuels qu'il visite, la règle se transforme. D'apparence figée, elle se révèle, en définitif, malléable. Il constate que chacun réécrit la règle, qu'il existe manifestement plusieurs auteurs et que leur discours se construit tout autour de la ressource, différente par sa destination et l'organisation de son contrôle, dont ces créateurs sont souvent les détenteurs ou bénéficiaires.

Mais peu à peu, il vient à saisir le fondement de la règle, son essence, qui revient constamment se juxtaposer aux différents sens de l'interdiction, par une série d'informations dont la nature est plutôt argumentative…

Cette première partie nous convie donc, dans un premier temps (chapitre I), à rechercher les sens de l'interdiction, de ces mots qui la composent, et déterminer son essence, c'est-à-dire les rationalités qui justifient la proscription du *spamming*.

Dans un second temps (chapitre II), elle nous amène à apprécier la nature et la forme d'Internet ainsi que les principaux détenteurs des pouvoirs technique et politique. Cet exercice impose une description des ressources de cet environnement et une présentation des auteurs de l'encodage, à savoir les autorités provenant du réseau ou celles qui y sont présentes.

Chapitre I - Le *spamming* : les sens et l'essence

Le dépouillement dont il s'agit n'est pas uniquement celui du mot *spamming* et de ses sens, mais également celui des maux causés par cette activité. L'identification des problèmes engendrés par le *spamming* conduit à l'essence de cette règle, c'est-à-dire aux rationalités et aux valeurs qui en déterminent le caractère dommageable. En d'autres termes, les fondements de l'interdiction du *spamming* reflètent les angoisses et les intérêts des acteurs - internautes et fournisseurs de services - et déterminent ce qu'ils perçoivent comme une nuisance du réseau, voire un abus d'Internet.

Par conséquent, la recherche du degré de juridicité de cette règle requiert, dans ce premier chapitre, de s'interroger non seulement sur les différents sens de l'interdiction (section I) mais aussi sur le(s) champ(s) de valeurs en présence, les rationalités à l'origine de ses significations : l'essence (section II).

Section I - Les sens du mot

Le *spamming* se manifeste sur trois ressources Internet, soit les groupes de discussion Usenet, le courrier électronique et les outils de recherche[32]. La définition du *spamming* offerte par l'Office québécois de la langue française ne prend en considération que la première de ces activités abusives sous l'appellation proposée de pollupostage :

> **Spamming** : V. o. spaming (pollupostage n. m.; inondation-réseau n. f.; arrosage-réseau n. m.; multipostage abusif n. m.). Action d'inonder de nombreux groupes de nouvelles Usenet ou groupes de discussion utilisant Internet, avec le même message,

---

[32] Le terme *spam* est également utilisé sur les *Multi-User Dungeons* (MUDs) pour exprimer l'interruption d'un programme dû à une surcharge de données, voire un « excès de mots ». Lee-Ellen MARVIN, « Spoof, Spam, Lurk and Lag: the Aesthetics of Text-based Virtual Realities », (1996) *Journal of Computer-Mediated Communication*, http://209.130.1.169/jcmc/vol1/issue2/marvin.html. Cependant, il n'existe pas de coûts économiques associés à ce comportement sur les MUDs et la question, à notre connaissance, n'a pas été abordée par les principaux acteurs d'Internet.

> inutile, souvent provocateur et sans rapport avec le sujet de discussion, causant ainsi une véritable pollution des réseaux.[33]

Le *spamming*, selon cette définition, consiste à expédier plusieurs articles identiques à un grand nombre de groupes de discussion Usenet. Il s'agit du multipostage abusif (EMP) ou, selon la méthode employée, du postage croisé abusif (ECP)[34]. Le nombre d'articles envoyés et la méthode utilisée déterminent généralement le caractère préjudiciable des postages sur la ressource Usenet[35].

D'abord associé aux groupes de discussion Usenet, le terme *spamming* a également été appliqué pour décrire le courrier électronique non sollicité et le bombardement d'une boîte de courrier électronique par l'envoi d'une quantité astronomique de messages (*mail bombing*). Souvent qualifié de *e-mail spam*, le courrier électronique non sollicité est la version française du *junk e-mail*. Ce sens, l'Office québécois de la langue française le traduit par le mot pourriel:

> ***junk e-mail***: *junk electronic mail*, Quasi-syn. *junk mail* (pourriel n. m.; courrier électronique-rebut n. m. Quasi-syn. courrier-poubelle n. m.; publicité-rebut n. f.; pub-rebut n. f.) Courrier électronique importun et souvent sans intérêt, constitué essentiellement de publicité, qui est envoyé massivement à un grand nombre d'internautes et que l'on destine habituellement à la poubelle.[36]

Les auteurs de cette définition notent toutefois que le mot «[p]ourriel est un terme générique pouvant aussi désigner les messages électroniques envoyés par pollupostage (spamming) ou par bombarderie (mail bombing), lesquels sont appelés plus

---

[33] Marcel BERGERON, Corinne KEMPA et Yolande PERRON, *Vocabulaire d'Internet : vocabulaire anglais/français*, 2e ed., Ste-Foy, Publication du Québec, 1997, p. 93. Voir également le site Internet de l'Office de la langue française : http://www.olf.gouv.qc.ca/service/pages/internet2.html.

[34] Le postage croisé fait référence à l'envoi d'un seul message à plusieurs groupes de discussion par l'inscription de leurs adresses dans le champ réservé aux destinataires. J. D. FALK et Scott SOUTHWICK, «The Net-Abuse FAQ», (23 décembre 1998), http://www.cybernothing.org/faqs/net-abuse-faq.html.

[35] Ce degré est établi par le *Breidbart Index*. *Id.* Voir *Infra*, par. A, sous-setion I de la présente section.

[36] M. BERGERON, C. KEMPA et Y. PERRON, *op. cit.*, note 33.

spécifiquement pollu ou polluriel (spam) et bombard ou bombarde (mail bomb)[37] ». Le terme pourriel constitue donc la version française du terme générique *spam* employé tant pour désigner le courrier électronique non sollicité que l'EMP ou l'ECP.

Enfin, le mot *spamming* est utilisé, depuis 1997, par plusieurs outils de recherche dont Alta Vista et Infoseek pour dénoncer l'indexation abusive exercée par les créateurs de sites Web auprès de leurs robots de recherche, des logiciels permettant l'ajout automatique de sites dans leurs bases de données respectives. Motivés par le désir de faire connaître leurs informations, créations, biens ou services, de nombreux internautes réussissent à profiter des défaillances de ce genre de robot et se hissent au sommet des résultats d'une requête adressée à un outil de recherche. Le professeur David E. Sorkin, auteur d'une compilation sur le droit du Cyberespace, place ce type de comportement sous la rubrique *spamdexing*[38]. L'expression *engine spamming* a également été proposée[39].

De ces trois manifestations, on observe que le *spamming* revêt deux aspects. D'une part, il se caractérise par le nombre de messages expédiés et se conçoit comme une activité quantifiable (sous-section I). D'autre part, il s'apprécie par la nature de l'activité ou, dans le cas du *spamdexing*, par les techniques utilisées. Cette appréciation s'opère par la qualification, voire l'apposition d'une étiquette selon la nature du contenu des messages ou du comportement visé (sous-section II).

Sous-section I - Les activités quantifiables

Si l'expression *spamming* qualifie actuellement plusieurs abus du réseau Internet, elle désignait essentiellement le pollupostage, l'activité la plus répréhensible de la ressource

---

[37] *Id.*

[38] *Cyberspace Law Subject Index* : http://host1.jmls.edu/cyber/index/index.html.

[39] Whit ANDREWS, «Beating (Up) the System», (1997), 22 sept., *Web Week* 38, 41, http://www.internetworld.com/print/1997/09/22/industry/19970922-beating.html.

télématique Usenet. Le nombre d'articles expédiés permet d'identifier un pollupostage d'un message ordinaire :

> *The term "spam" [...] means the same article (or essentially the same) posted an unacceptably high number of times to one or more newsgroups. Content is irrelevant. Spam doesn't mean ads. It doesn't mean abuse. It doesn't mean posts whose content I object to. Spam is a funky name for a phenomenon that can be measured pretty objectively : did that post appear X times?*[40]

À cet égard, le multipostage abusif (EMP) (A) doit être distingué du postage croisé abusif (ECP) (B).

A. Le multipostage abusif

La contenu des articles Usenet n'est d'aucune pertinence dans l'appréciation d'un pollupostage puisqu'elle s'opère objectivement par le dénombrement des articles identiques. Toutefois, cet exercice peut être laborieux lorsque ceux-ci se retrouvent sur plusieurs groupes de discussion. Cette difficulté est contournée par l'utilisation d'un moteur de recherche tel que *Deja News*. Ce dernier permet en effet d'établir facilement le nombre de fois qu'un même article se retrouve sur un ou plusieurs groupes de discussion[41].

De façon générale, un pollupostage est un article posté plus de 20 fois sur la ressource Usenet[42]. Une formule inventée par Seth Breidbart permet de prendre en considération le nombre de groupes de discussion sur lesquels ont été postés un ou plusieurs articles. Il s'agit du *Breidbart Index* (BI):

---

[40] J. D. FALK et S. SOUTHWICK, *loc. cit.*, note 34.

[41] Greg BYSHENK, «I've been spammed! What do I do?», http://www.tezcat.com/~gbyshenk/ive.been.spammed.html.

[42] J. D. FALK et S. SOUTHWICK, *loc. cit.*, note 34. Une définition dissidente est à l'effet qu'un article posté au moins 5 fois pendant une période de dix jours est qualifiable de pollupostage s'il comporte un contenu semblable ou identique.

(vNb de groupes de discussion) + (vNb de groupes de discussion) + …[43]

Selon Tim Skirvin, un article atteignant un indice Breidbart de 20 est susceptible d'être supprimé pour pollupostage. Toutefois, la détermination objective du multipostage abusif par le *Breidbart Index* ne se révèle pas concluante en tout point : elle n'a pas pour effet d'assimiler à un pollupostage un article posté 19 fois sur un seul groupe de discussion, un multipostage qui apparaît pourtant abusif.

À cette première condition, s'ajoute la période durant laquelle les articles « identiques » ont été postés. Un pollupostage correspond à un article ayant obtenu un indice de 20 à l'échelle *Breidbart* pendant une période de 45 jours[44].

Visiblement, l'échelle Breidbart n'est pas une panacée mais apporte un outil essentiel à la qualification objective et quantifiable du multipostage abusif. Elle offre également la possibilité de déterminer le caractère abusif du postage croisé.

B. Le postage croisé abusif

Le postage croisé fait référence à l'envoi d'un seul article à plusieurs groupes de discussion par l'inscription de leur adresse dans le champ réservé aux destinataires[45]. Contrairement au multipostage où le destinateur expédie un ou plusieurs messages à

---

[43] Somme des racines carrées du nombre de groupes de discussion auxquels chaque message identique ou comportant essentiellement le même contenu a été expédié. On propose actuellement une seconde version, le BI2 : ((vNb de groupes de discussion + vNb de groupes de discussion + …) + (Nb de groupes de discussion + Nb de groupes de discussion + …)) /2. Cette version serait plus agressive puisqu'elle ne permet, pour un seul article, que 35 groupes de discussion alors que la version originale en permet 125. Une dernière formule, le *Skirvin-Breidbart Index* (SBI) prendrait en considération le caractère moins nuisible des articles postés avec la mention « faire suivre ». Tim SKIRVIN et Chris LEWIS, «Current Usenet Spam Tresholds and Definitions», (11 octobre 1998) http://www.cen.uiuc.edu/~tskirvin/faqs/spam.html.

[44] *Id.*

[45] J. D. FALK et S. SOUTHWICK, *loc. cit.*, note 34.

chacun des groupes de discussion choisis, le postage croisé ne génère qu'un seul message. Un postage expédié de cette manière est donc moins volumineux que le multipostage[46] et se trouve généralement mieux reçu par les administrateurs de la ressource Usenet. Pour cette raison, un article posté à moins de 20 groupes de discussion ne constitue pas, par application de la formule de Breidbart, du postage croisé abusif ou, selon une autre appellation, du *Velveeta*[47].

Cependant, le postage croisé est soumis, tout comme le multipostage, aux critiques des utilisateurs et des administrateurs de cette ressource quant aux nombre d'articles identiques expédiés sur un ou plusieurs groupe de discussion. Si l'échelle Breidbart tient compte du caractère inoffensif d'un postage croisé en ne considérant que le carré du nombre de groupes de discussion destinataires de l'article, elle pénalise toujours la répétition des articles « identiques » au sein d'un même groupe[48].

Sous-section II - Les activités qualifiables

Le *spamming* ne se définit pas seulement comme une activité quantifiable. Devenant une étiquette pour plusieurs comportements abusifs, cette activité ne s'évalue pas seulement par un critère mathématique mais aussi par son contenu ou sa nature. Si les activités quantifiables sont associées à la ressource télématique Usenet, les activités qualifiables réfèrent à d'autres contextes électroniques d'Internet, le courrier électronique et le *World Wide Web*. Les différentes significations de notre objet d'analyse semblent donc varier en fonction des ressources Internet.

---

[46] *Id.* Il est suggéré aux personnes exerçant le postage abusif d'expédier un seul article accompagné de la mention «faire suivre à un autre groupe». Si l'article s'avère intéressant, il y a de fortes chances qu'il soit expédié à nouveau.

[47] *Id.*; Scott Hazen MUELLER, «Fight Spam on the Internet», http://spam.abuse.net.

[48] Il a été proposé qu'un postage croisé ne soit qualifié de *spamming* que dans les cas d'*alpha-spam*, c'est-à-dire lorsqu'un article est posté à tous les groupes de discussion par ordre alphabétique. G. BYSHENK. *loc. cit.*, note 41.

En considération de certains autres abus, cette observation doit être vérifiée. En effet, la ressource Usenet semble avoir été le premier contexte électronique où la signification du terme *spamming* a porté sur le contenu des articles et non sur leur nombre. Par conséquent, avant de présenter le courrier électronique non sollicité (B) et l'indexation abusive auprès des outils de recherche (C), nous préférons aborder la thématique des groupes de discussion (A), un sujet qui a certainement contribué à la formation des activités qualifiables.

A. La thématique des groupes de discussion

Les groupes de discussion faisant partie du réseau mondial Usenet traitent de sujets particuliers selon sept racines principales de discussion : *comp* (ordinateur), *misc* (divers), *news* (nouvelles Usenet), *sci* (sciences), *soc* (sociologie) et *talk* (sujets chauds)[49]. En règle générale, un postage destiné à un groupe de discussion Usenet doit respecter le thème qui y est consacré. Il s'agit là d'une règle importante pour les internautes désireux de promouvoir leur biens et services[50].

Comme nous l'avons vu, cette règle n'est pas assimilée à l'expression *spamming* telle qu'entendue sur la ressource télématique Usenet. Cependant, l'expérience des utilisateurs révèle que les postages abusifs se retrouvent généralement parmi les articles postés sans considération pour les thèmes des groupes de discussion destinataires du postage[51]. Un article hors sujet, sans être déterminant pour la qualification d'un pollupostage, représente un indice-clef.

Prenons ici l'exemple d'un article dont le contenu est une publicité pour une entreprise de création de site Internet. Bien qu'expédié douze fois sur un groupe de discussion dont

---

[49] M. BERGERON, C. KEMPA et Y. PERRON, *op. cit.*, note 33, pp. 102-103.

[50] Joel K. FURR, « Advertising on Usenet: How To Do It, How Not To Do It », ftp://rtfm.mit.edu/pub/faqs/usenet/advertising/how-to/part1.

[51] S. H. MUELLER, *loc. cit.*, note 47.

le thème se rapporte, par exemple, à la philatélie, cet article ne représente pas, selon l'échelle *Breidbart*, un postage abusif. Cependant, la pertinence de son contenu par rapport à la thématique du groupe de discussion et son objectif promotionnel infèrent un comportement abusif. Ce postage devient donc susceptible d'être contrôlé sur l'ensemble de la ressource. Suite à cette vérification, les acteurs pourront prendre, selon les règles auxquelles ils adhèrent, des mesures contre l'expéditeur. En somme, l'absence de lien entre le sujet du postage et le thème d'un groupe de discussion constitue une présomption du caractère abusif d'un postage mais n'est jamais déterminant.

Cette dernière observation met en exergue la corrélation existante entre le sens accordé à l'expression *spamming* et la possibilité, sur la ressource Usenet de dénombrer techniquement les articles postés. Sans cette alternative, il est probable que la signification actuelle du *spamming* n'existerait pas. En effet, il aurait été nécessaire de s'en remettre à la nature des postages, le critère du nombre ne pouvant être véritablement apprécié.

La signification du terme *spamming* appliqué au courrier électronique soutient cette idée. N'offrant à ses utilisateurs aucun moyen technique permettant de dénombrer les articles identiques, cette ressource favorise une conception qualitative du *spamming*. Le *e-mail spam* se détermine donc selon le contenu des messages expédiés et se confond avec le courrier électronique non sollicité (*junk e-mail*).

B. Le courrier électronique non sollicité

Les principaux acteurs de la ressource Usenet conviennent généralement que le courrier électronique non sollicité est une activité différente du *spamming*, préférant définir le *e-mail spam* comme un envoi abondant de courriers électroniques indépendamment du caractère non sollicité du message expédié. Admettant les similitudes entre les diverses expressions, ils insistent néanmoins sur la distinction entre le *e-mail spam*, le courrier

électronique commercial non sollicité (UCE) et le courrier électronique non sollicité de masse (UBE)[52].

À ce sujet, les différents acteurs opposés au courrier électronique non sollicité se révèlent moins pointilleux et n'ont pas de scrupules à qualifier tout courrier électronique non sollicité de *spamming*. Il en est ainsi de la *Coalition Against Unsolicited Commercial Email*[53] et de la campagne en faveur d'une réglementation de l'UCE dans l'État de Washington[54].

Par ailleurs, aucun doute ne persiste quant à l'usage courant de l'expression *spamming* pour ce type d'activité. Les juristes américains ne dressent aucune distinction et rappellent souvent la synonymie de ces termes[55].

La sollicitation apparaît donc comme l'unique critère de la qualification du *spamming* bien que la détermination du caractère non sollicité d'un message se présente comme un exercice incertain. En effet, en l'absence de définition claire de ce qui doit être considéré comme un message non sollicité, les internautes, administrateurs et fournisseurs de services demeurent dans un flou cybernétique!

---

[52] G. BYSHENK, *loc. cit.*, note 41; W. D. BASELEY, « The Email Abuse FAQ », (25 juin 1998), http://members.aol.com/emailfaq/emailfaq.html.

[53] *CAUSE* : http://www.cauce.org/

[54] *Spam Free Washington!* : http://www.mcnichol.com/spam.htm. Voir également *Junk Email Resource Page* : http://www.junkemail.org/.

[55] Voir : Lorrie Faith CRANOR et Brian A. LAMACCHIA, « Spam! », (1998) 41 *Communications of the ACM* 74 (version définitive : http://www.acm.org/pubs/citations/journals/cacm/1998-41-8/p74-cranor/); Jonathan BYRNE, « Squeezing Spam Off the Net: Federal Regulation of Unsolicited Commercial E-mail », (1998) 2 *W. Va. J. L. & Tech.* 4, http://www.wvjolt.wvu.edu/v2i1/byrne.htm; Michael W. CARROLL, « Garbage In: Emerging Media and Regulation of Unsolicited Commercial Solicitations », (1996) 11 *Berkeley Tech. L.J.* 233, http://www.law.berkeley.edu/journals/btlj/articles/11-2/carroll.html; David E. SORKIN, « Unsolicited Commercial E-Mail and the Telephone Consumer Protection Act of 1991 », (1997) 45 *Buffalo L. Rev.* 1001, http://www.jmls.edu/faculty/sorkin/tcpa.html.

Néanmoins, les différents protagonistes s'entendent sur le caractère essentiellement publicitaire du courrier électronique non sollicité. Ainsi, la signification de l'expression *spamming*, au regard du courrier électronique, se retrouve principalement dans la définition de publicité :

> Publicité : Le fait d'exercer une action sur le public à des fins commerciales; le fait de faire connaître (un produit, un type de produit) et d'inciter à l'acquérir; ensemble des moyens qui concourent à cette action.[56]

La deuxième signification de l'expression *spamming* s'entend donc comme un message promotionnel reçu par courrier électronique et dont l'objectif est habituellement commercial[57].

Reposant substantiellement sur le caractère promotionnel du contenu des messages expédiés, le courrier électronique non sollicité se rapproche étroitement d'une autre activité qualifiable, l'indexation abusive auprès des outils de recherche.

C. L'indexation abusive auprès des outils de recherche

Les contenus disponibles sur le réseau Internet peuvent être retrouvés par l'utilisation des outils de recherche. Sans être de véritables modes de communication comme le sont Usenet, le courrier électronique et le Web, ces derniers représentent d'inestimables ressources du réseau. Dénommé chercheur ou moteur de recherche, un outil de recherche est un «[p]rogramme qui indexe le contenu de différentes ressources Internet, et plus particulièrement de sites Web, et qui permet à l'Internaute qui utilise un navigateur Web de rechercher de l'information selon différents paramètres, en se servant de mots-clefs, et d'avoir accès à l'information ainsi trouvée[58] ».

---

[56] *Le nouveau petit Robert*, édition 1995.

[57] Cette définition n'empêcherait pas un message à caractère religieux, politique ou éducatif d'être qualifié de la sorte dès lors qu'il comporte un objectif de promotion.

[58] M. BERGERON, C. KEMPA et Y. PERRON, *op. cit.*, note 33, p. 90.

Plus que de rendre possible la recherche d'informations, les outils de recherche permettent aux diffuseurs d'indexer leurs contenus. Ces derniers sont libres de participer activement ou passivement au référencement de leurs sites Internet. En effet, si ces programmes sont généralement munis d'un robot de recherche dont le rôle est de récupérer automatiquement les contenus diffusés sur Internet[59], ils offrent également à leurs utilisateurs la possibilité de soumettre leurs propres adresses Internet. Cette méthode représente une stratégie essentielle pour les diffuseurs soucieux de promouvoir leurs créations, biens et services. Toutefois, le fonctionnement des outils de recherche occasionne plusieurs abus générés par des diffuseurs avertis.

Les abus qu'autorise ce fonctionnement sont reliés à l'utilisation par la plupart des outils de recherche, d'un algorithme de classement qui détermine l'ordre dans lequel un contenu, par exemple une page Web, est présentée à un utilisateur suite à l'interrogation de l'outil de recherche[60]. Pour un diffuseur de contenus, un classement supérieur, c'est-à-dire de la dixième position à la première, occasionne généralement des revenus supplémentaires correspondant à une augmentation des ventes[61] et à un accroissement du potentiel publicitaire. Il n'est donc pas surprenant que plusieurs diffuseurs de contenus tentent de bénéficier des défaillances des algorithmes de classement.

Essentiellement fondées sur la fréquence des termes recherchés dans un document, sur leur emplacement ainsi que sur la distance les séparant, les méthodes de classement des outils de recherche reposent sur les mots-clefs[62]. L'astuce utilisée par plusieurs consiste à répéter indéfiniment à l'intérieur de leurs documents, des mots susceptibles d'être

---

[59] Cette automatisation s'effectue en parcourant, tout comme les internautes, les liens hypertextes.

[60] Ce n'est généralement pas le cas des répertoires tel que Yahoo!. Ce type d'outil de recherche indexe manuellement toutes les soumissions qui lui sont expédiées.

[61] Voir : W. ANDREWS, *loc. cit.*, note 39.

[62] Le populaire outil de recherche Alta Vista utilise un tel procédé.

recherchés par les utilisateurs, indépendamment de leur pertinence avec le contenu diffusé[63]. Cette astuce, les outils de recherche l'ont qualifiée de *spamming*.

L'expression *spamming*, au regard des outils de recherche, ne serait pas limitée à la stratégie promotionnelle de la répétition de mots-clefs. En effet, l'outil de recherche Infoseek estime que le mot *spamming*, lorsqu'il est associé aux outils de recherche, constitue une « [...] *alteration or creation of a document with intent to deceive an electronic catalog or filing system*[64] ». Plusieurs autres techniques subversives entreraient donc dans le champ de cette nouvelle signification.

À titre d'exemple, notons l'utilisation de plusieurs noms de domaine comportant le même contenu de même que l'adoption de la stratégie des pages satellites. Cette dernière pratique consiste à indexer, auprès d'un outil de recherche, plusieurs pages dont l'unique fonction est de rediriger le visiteur vers la page d'accueil du contenu diffusé, créant ainsi un nombre disproportionné de pages indexées se rapportant au site du diffuseur.

Si de nouvelles techniques sont susceptibles d'être développées rapidement par les diffuseurs de contenus, une énumération exhaustive de celles considérées abusives ne serait, en définitive, qu'un défi lancé aux plus ingénieux d'entre eux. Par conséquent, cette nouvelle signification de l'expression *spamming* ne dépend pas d'une formule mathématique mais de critères assez vagues : tromper, abuser un outil de recherche. De tels critères, rappelant les standards[65], renvoient à des valeurs, à un champ interprétatif : l'essence.

---

[63] Une répétition se fait généralement par l'inscription de balises « <!> » permettant aux mots-clefs de demeurer invisibles pour le visiteur du contenu indexé. Le même résultat peut être obtenu en configurant le texte de la répétition de la même couleur que le fond de l'écran.

[64] *Infoseek (What is spamming?)* : http://infoseek.go.com/AddUrl?pg=Spamming.html

[65] Un standard est une notion à contenu variable, par exemple : la notion de personne raisonnable, le critère du manifestement déraisonnable, les termes juridiques «exceptionnels», «imprévisibles», etc. L'auteur de l'analyse systémale l'explique ainsi : «Toutes notions infiniment variables dans le temps et l'espace et qui peuvent être comprises de manières les plus diverses. Notions qui, selon les uns, sont de source discrétionnaire parce que, disent-ils, en raison de leur caractère vague et indéterminé, elles ne lient pas le destinataire de la norme posant le standard, tandis que, pour les autres, elles ont au contraire pour

Section II - L'essence du mot

Revêtant plusieurs significations, l'expression *spamming* nécessite, avant de s'interroger sur son essence, une définition générique susceptible d'englober l'ensemble de ses manifestations sur le courrier électronique, les outils de recherche et les groupes de discussion Usenet. Forcément générale, cette définition ne doit pas avoir pour effet de reprendre le concept de la Netiquette, qui est, rappelons-le, « [...] un ensemble de principes [souvent flous] destinés à assurer un certain ordre dans Internet[66] ». Le *spamming* serait donc un abus affectant la fonctionnalité d'une ressource Internet.

Certes, les notions d'abus et de fonctionnalité laissent une place importante à l'indétermination. Ensemble, ils évoquent un usage excessif, mauvais ou injuste favorisant le déclin du caractère pratique d'une ressource Internet, sans toutefois indiquer clairement au lecteur les applications précises de leur signification. Derrière ces mots, existent pourtant des rationalités, des valeurs permettant de déchiffrer et de mettre au grand jour une signification apparemment obscure.

Représentant l'essence du *spamming*, ces rationalités et valeurs reposent sur l'insistance des différents protagonistes du réseau sur le dévoiement d'une ressource (sous-section I) et sur le caractère promotionnel des comportements abusifs encadrés par les significations de l'expression *spamming* (sous-section II).

Sous-section I - Le dévoiement d'une ressource

L'accentuation par les acteurs du réseau de l'effet négatif du *spamming* relativement à la fonctionnalité des ressources reflète leur attachement non seulement à la notion de

---

objet et pour fonction de lier ceux à qui elles s'adressent et de les enfermer dans un cadre préalablement déterminé». G. TIMSIT, *op. cit.*, note 5, p. 122.

[66] P. TRUDEL, F. ABRAN, K. BENYEKHLEF et S. HEIN, *op. cit.*, note 9, p. 3-62.

propriété (A), privée ou collective, mais également aux rapports économiques que cette notion implique (B).

En effet, le « sentiment propriétaire » est à l'origine des réactions des détenteurs de ressources matérielles et des utilisateurs du réseau. La propriété confère à celui qui en jouit les fruits et les revenus mais également le libre usage. Lorsqu'une ressource est au bénéfice d'une seule personne, la notion de libre usage autorise le propriétaire à protéger son bien de toute atteinte extérieure. Au bénéfice de plusieurs, l'usage que fait chaque utilisateur de la ressource est conditionné par le droit de chacun. Une ressource commune ne supporte pas l'exclusivité à l'intérieur du cercle de ses utilisateurs à moins d'un partage économique préalable.

En l'absence d'un partage proportionnel entre les coûts reliés à l'utilisation et l'usage effectif de chacun, il n'est pas étonnant que la notion d'abus soit utilisée pour qualifier l'emploi indu d'une ressource.

A. Le « sentiment propriétaire » collectif et privé

Ce que nous appelons le « sentiment propriétaire » collectif réfère au droit personnel d'utilisation que chaque internaute possède et qui lui permet de naviguer librement. En insistant sur l'utilité collective du réseau Internet, cette notion a comme principal corollaire le concept largement répandu de communauté Internet.

Toutefois, ce « droit » n'est pas le résultat d'un processus législatif traditionnel mais l'aboutissement de rapports contractuels entre utilisateurs, fournisseurs d'accès Internet, opérateurs de lignes de communication, etc. En effet, le « sentiment propriétaire » collectif ne peut exister qu'en rapport avec autrui. Or, ce « droit » est un service pour lequel chaque internaute paie une somme déterminée par le jeu du marché. Apparaît donc une relation entre fournisseurs et usagers, assimilable à un démembrement de propriété, dans laquelle l'usage est autorisé par le fournisseur d'accès, le propriétaire des

installations rendant possible l'accès aux ressources et à leur utilisation. En droit positif québécois, cette relation serait qualifiée de contrat de service dans lequel l'entreprise prestataire de services « [...] s'engage envers une autre personne, le client, [...] à fournir un service moyennant un prix que le client s'oblige à lui payer[67] ».

Bien qu'il s'agisse d'une relation de service, nous devons admettre l'existence d'un « sentiment propriétaire » collectif créé par le droit d'usage de chaque internaute, lequel ne se limite pas en terme d'utilisation mais en temps d'utilisation. Effectivement, les contrats de prestations de service Internet engagent les usagers à payer une somme soit forfaitaire soit en fonction du temps d'utilisation, mais jamais selon le nombre de communications effectuées par l'usager ou, en d'autres termes, selon les coûts variables générés par l'utilisation du client.

L'usage des ressources Internet se caractérise donc par l'absence d'un partage proportionnel entre les coûts reliés à l'utilisation et l'usage effectif de chacun. En conséquence, il existe une étroite relation entre la notion d'abus et le « sentiment propriétaire » collectif. Cette relation n'est pas dissociable de la présence de regroupements contre les détracteurs du réseau.

Le « sentiment propriétaire » privé se retrouve davantage au niveau de la réalité matérielle, des installations permettant l'utilisation d'Internet. À ce titre, les fournisseurs d'accès ne sont pas les seuls acteurs à disposer d'équipement. Les communications de ce réseau traversent également des « câblages » appartenant à des « transporteurs publics ou privés » : lignes téléphoniques, câbles optiques, satellites, etc.

Contrairement à l'idée répandue que ce réseau est une ressource inépuisable, il existe un trafic dépendant de la structure matérielle du réseau et qui en altère la fonctionnalité. Par ailleurs, l'utilisation de certaines ressources implique la mémorisation des communications par les prestataires de services, une mémoire qui n'est pas illimitée.

---

[67] *Code civil du Québec*, art. 2098.

L'étroitesse des « câblages » et les espaces disques insuffisants représentent, en terme de ressource matérielle, un manque, une rareté à laquelle correspond une valeur. Les propriétaires des installations Internet supportent, directement ou indirectement, les coûts reliés à cette rareté.

En effet, l'usage abusif d'Internet engendre des coûts d'opérations aux détenteurs des ressources matérielles et emporte une diminution des profits réalisés par ces entreprises. Les usages abusifs pervertissent la bonne marche des affaires des propriétaires des ressources matérielles puisque leurs pertes sont répercutées sur l'ensemble de leurs membres par une hausse des prix de leurs services, cette décision pouvant s'avérer non compétitive. Ce « sentiment propriétaire » privé justifie l'existence de règles d'utilisations énoncées par les fournisseurs d'accès Internet dans leurs clauses contractuelles.

B. Les coûts d'opération de l'usage abusif

L'usage abusif que représente le *spamming* génère des coûts d'opération supportés tant par les fournisseurs que par leurs usagers. Ces frais supplémentaires deviennent considérables lorsque plusieurs utilisateurs profitent abusivement du réseau. En illustration, on peut évoquer le célèbre pollupostage envoyé par les sympatisants de l'église de Scientologie sur le groupe de discussion alt.religion.scientology[68]. L'histoire veut que 1200 articles aient été reçus en 15 jours, l'équivalant de 50 mégaoctets[69]. Le fournisseur d'accès Internet America On-Line (AOL) affirmait quant à lui, recevoir 1.8 million de courriers du renommé mais défunt abuseur Cyberpromotion[70].

---

[68] L'objectif de ce groupe est de dénoncer les agissements de l'Église de Scientologie.

[69] ANONYME, «The What is Scientology? (ARSBOMB) Spam Team FAQ for Los Angeles Area ISPs », (22 décembre 1996), http://www.panix.com/~tbetz/WIS_Spam_Team_FAQ.shtml.

[70] S. H. MUELLER, *loc. cit.*, note 47. D'abord connue sous le nom de *Promo Enterprises* lorsqu'elle expédiait des publicités par télécopieur, *Cyberpromotion* fut ensuite considérée comme le plus important abuseur du réseau Internet. Débranchée à plusieurs reprises par ses fournisseurs d'accès Internet suite aux

En plus de diminuer la vitesse de transmission des communications Internet, le *spamming* corrompt la bonne gestion des administrateurs de systèmes et dérobe aux utilisateurs l'utilité des groupes de discussion, de leurs boîtes de courrier électroniques et des outils de recherche en les submergeant de barrages publicitaires.

La société Bright Light Technologies, instigatrice d'un projet de filtrage global des courriers non sollicités, estime qu'au moins 25 millions de courriers électroniques sont expédiés chaque jour sur Internet et que chaque courrier électronique non sollicité coûte environ 2.8 cents américains à chaque internaute en temps perdu et en bande passante.

M. Barry D. Bowen résume les coûts du pourriel pour les fournisseurs d'accès Internet (FAI) et leurs utilisateurs[71]. Selon lui, cet usage abusif impose aux fournisseurs d'accès un élargissement continuel de la bande passante afin de contrer l'augmentation du trafic Internet. Il requiert également l'achat de mémoire supplémentaire rendue nécessaire par l'entreposage des messages additionnels et l'embauche de personnel pour gérer les problèmes techniques et répondre aux plaintes des « victimes ». Enfin, il rend indispensable l'achat (et la gestion) d'ordinateurs supplémentaires afin d'assurer la sécurité et l'intégrité des fournisseurs d'accès Internet régulièrement menacés par cette activité[72].

---

plaintes d'usagers, Cyberpromotion créa son propre fournisseur du nom d'*ISpam*. *Cyberpromotion* fut membre du conglomérat des *spammers*, l'*Internet E-Mail Marketing Council*, qui favorise des pratiques responsables de la promotion par courrier électronique. Enfin, le propriétaire de *Cyberpromotion*, Stanford Wallace, décida, suite au jugement auquel il a consenti en mars 1998 dans *Earthlink Network Inc.* v. *Cyber Promotions*, Inc. No. BC 167502 (Cal. Super. Ct. L.A. County May 7, 1997), d'arrêter toutes ses activités reliées au *spamming*.

[71] Barry D. BOWEN, « Controlling unsolicited bulk e-mail (Who's taking action? What's being done?) », (1997), http://www.sun.com/sunworldonline/swol-08-1997/swol-08-junkemail.html.

[72] En effet, certains expéditeurs de pourriels et polluposteurs utilisent les installations de tiers pour envoyer leurs messages dans l'espoir de ne pas être facilement identifiés par les destinataires et leurs fournisseurs d'accès Internet.

M. Bowen ajoute que l'un des effets du pourriel est d'augmenter les coûts reliés au temps de chargement des courriels, gonflant la facture mensuelle des utilisateurs. Ces coûts accessoires n'existent toutefois que lorsque l'usager ne dispose pas d'une connexion Internet ou d'une connexion téléphonique locale forfaitaire. Si les connexions Internet sont généralement à forfait, les connexions téléphoniques locales sont susceptibles, selon les différentes réglementations nationales, d'être facturées en fonction du temps d'utilisation. À titre d'exemple, le marché français n'a pas encore établi de mode de paiement forfaitaire malgré la pression exercée par les internautes français. Par ailleurs, les coûts supplémentaires reliés au temps de chargement deviennent beaucoup plus apparents pour les usagers des régions éloignées utilisant une communication interurbaine.

Les circonstances entourant le *spamming* ne sont pas éloignées du problème de la télécopie commerciale. Parce que les coûts promotionnels des entreprises étaient supportés par les destinataires, elle fut interdite dans plusieurs pays. Ainsi, les États-Unis d'Amérique ont estimé nécessaire d'adopter le *Telephone Consumer Protection Act of 1991* (TCPA)[73]. Les raisons justifiant l'adoption de cette loi apparaissaient alors plus préoccupantes que les motifs avancés contre le courrier « traditionnel » non sollicité. Le représentant Edward J. Markey insistait déjà sur l'importance d'une telle réglementation avant l'introduction du *Facsimile Advertising Regulation Act*, l'un des premiers projets de loi destiné à prohiber la télécopie commerciale aux États-Unis :

> *Unsolicited advertising is beginning to clog FAX lines, restricting the owners' ability to use their machines for the purposes they originally bought them for and generating operating costs the users can't control. Unlike junk mail, which can be discarded, or solicitation phone calls, which can be refused or hung up, junk FAX ties up the recipient's line until it has been received and printed. The recipient's machine is unavailable for business and*

[73] Pub. L. No. 102-203, 105 Stat. 2394 (codifié tel qu'amendé à 47 *U.S.C.* § 227 (1994))

> *he or she incurs the high cost for supplies before knowing whether the message is either wanted or needed.*[74]

De ce constat ressort le facteur déterminant de l'action réglementaire américaine, c'est-à-dire le déplacement des coûts (*cost-shifting*) des télécopies commerciales de l'expéditeur vers leurs destinataires. À ce titre, il est probable que le « sentiment propriétaire » a contribué à faire avancer la cause des destinataires. Cette rationalité dresse un important parallèle entre la télécopie commerciale et le *spamming*, et pose, pour chacune de ces activités, un problème d'iniquité.

Au regard du courrier électronique non sollicité, l'iniquité que crée le transfert des coûts est sujet à l'évolution de la technologie. Si le marché actuel des prestations de services Internet justifie des actions réglementaires, des types de connexion plus rapide comme les connexions par câble, déjà très populaires, le LMDS (*Local Multipoint Distribution Services*), transmettant par signal radio à 500 kpbs, les connexions par câbles électriques découvertes par Northern Telecom et la société britannique NorWeb, les connexions satellite, utilisant le réseau téléphonique pour l'émission, sont susceptibles de changer la donne

La prise en considération de ces avancées technologiques mine considérablement l'argument du transfert des coûts. En effet, si les nouveaux types de connexion ont pour conséquence de résorber toute augmentation directe des coûts de chargement pour les utilisateurs, le « sentiment propriétaire » ne peut qu'en être moins affecté.

Dans cette optique, seuls les frais supportés directement par les fournisseurs d'accès Internet pour la mémorisation des messages, la sécurisation des systèmes et l'embauche de nouveau personnel risquent d'être répercutés sur les usagers. S'agissant pour chaque utilisateur de coûts dérisoires, l'argument économique du *spamming* risque d'être

---

[74] 135 Cong. Rec. E1462 (daily ed. May 2, 1989) (statement of Rep. Markey). Nous tenons cette citation de D. E. SORKIN, *loc. cit.*, note 55, 1018.

réservé aux détenteurs des ressources matérielles. Ne justifierait encore l'interdiction du *spamming* que son caractère promotionnel.

Sous-section II - Le caractère promotionnel des comportements abusifs

Le problème du *spamming* révèle non seulement le malaise d'un « sentiment propriétaire » bafoué, mais également l'indisposition de plusieurs acteurs face au caractère promotionnel et généralement commercial des comportements abusifs visés.

Cette indisposition n'est pas étrangère au concept de réseau informatique. Ce concept, dont la définition met en relief « l'échange d'informations numériques », induit une perception du réseau Internet davantage reliée aux interactions entre plusieurs personnes qu'à une simple relation client/serveur, plus proche de la réalité matérielle du réseau. La réalité virtuelle, construite autour de cette perception, emporte une pléiade de phénomènes nouveaux que les premiers arrivants ont rapidement cristallisés sous forme de nouveaux concepts. Ainsi, la « philosophie d'Internet[75] » représente les principes ou idées directrices guidant l'utilisation du réseau par les « membres de la communauté virtuelle ». La notion de communauté virtuelle, autre nouvelle conceptualisation, figure également au chapitre des effets socialisants d'un réseau informatique permettant de nombreux types d'interactions.

Créée par la première génération d'internautes, la « philosophie d'Internet » se présente comme un concept figé par les pionniers d'Internet lorsque celui-ci était encore le réseau d'une communauté scientifique et universitaire. Depuis, les circonstances ont évolué, attribuant à un réseau devenu populaire une indéniable connotation commerciale : un effet incontournable des barbares, les *newbies*[76], prenant possession du continent virtuel.

---

[75] Le concept de « philosophie d'Internet » correspond à l'expression anglaise « *Internet culture* ». Cette culture serait menacée depuis la création du Web par l'appropriation du réseau par les entreprises commerciales. Voir : Peter DEUTSCH, « Preserving and Promoting the "Internet Culture" », (mars 1994), http://www.eff.org/papers/eegtti/eeg_268.html.

[76] L'Office de la langue française propose le terme cybernovice : « Internaute nouvellement arrivé dans Internet ». M. BERGERON, C. KEMPA et Y. PERRON, *op. cit.*, note 33, p. 78.

Par une réaction légitime d'autodéfense, les internautes de la première génération ont tenté de protéger la philosophie initiale en prônant les vertus d'un réseau de « l'information » qui trouvent actuellement écho dans les médias de masse. En effet, la promotion du partage des recherches, de la dynamique de coopération, de l'échange de liens et de l'accès rapide à l'information, réfère à des idées que véhiculent encore la presse et la télévision dans leur généreuse appréhension des possibilités offertes par Internet.

S'en suit un sentiment d'inconfort associé à la transformation rapide d'Internet vers un réseau à forte utilité commerciale. Sans préconiser un frein à l'activité publicitaire en ligne, la « philosophie d'Internet » pose toutefois de sérieuses balises à son exercice, comme le démontre la Foire Aux Questions (FAQ) concernant la publicité sur la ressource Usenet :

> *One such custom is the tradition and belief that it is rude to advertise for profit in Usenet newsgroups.*
>
> *Advertising is widely seen as an 'off-topic' intrusion into the discussions of any particular newsgroup (newsgroup is the Usenet word for discussion group or bulletin board). Each newsgroup has a specific set of subjects it is intended to cover, and in order for newsgroups to function as effective discussion forums, it is important that people stay 'on-topic'.*[77]

Le document de travail de l'IETF (*Internet Engineering Task Force*) traitant de la publicité sur Internet affiche les mêmes couleurs :

> *A lot of the population which is new to the Internet think that the Internet "old guard" (defined as anyone who was using the Internet before the invention of Web browsers) are diametrically opposed to using the Internet for advertising. This is not true.*

---

[77] J. K. FURR, *loc. cit.*, note 50.

> *But in general, Internet culture opposes use of the network in irresponsible ways and this usually includes people who advertise by sending unsolicited information to Netnews groups and Internet mailing lists.*[78]

L'existence de ces balises implique un aménagement de la définition générique du *spamming*. Indissociable d'une activité promotionnelle, les comportements visés par cette expression ne s'expliquent pas seulement par une entrave au « sentiment propriétaire ». En effet, les objectifs publicitaires des détracteurs conduisent les différents acteurs du réseau à « démoniser » certaines activités. La notion de *spamming* doit donc être comprise comme une expression générique destinée à identifier une activité généralement accomplie pour des raisons promotionnelles et affectant la fonctionnalité d'une ressource Internet.

[78] Sally HAMBRIDGE et Donald EASTLAKE 3rd, « IETF RUN Working Group draft-ietf-run-adverts-00.txt : $$$$$ MAKE ENEMIES FAST $$$$$ or How to Advertise Responsibly Using the Internet », (Mars 1998), http://search.ietf.org/internet-drafts/draft-ietf-run-adverts-00.txt (Expiré depuis le 9 septembre 1998).

Chapitre II - Cyberespace : les inductions sociales d'un réseau informatique

En introduisant cette analyse systémale de l'interdiction du *spamming*, nous avons considéré que le caractère obligatoire des normes (la juridicité) était susceptible de varier en fonction des contextes dans lesquels s'effectue le décodage de la norme. De cette relation de dépendance, nous avons déduit que la nature et la forme des différentes ressources Internet agissaient sur le degré de prévisibilité de l'interdiction du *spamming*.

Cette hypothèse nécessitait, dans un premier chapitre, un portrait du concept de *spamming* et des valeurs sous-tendant son interdiction. Nous avons observé trois manifestations de cette activité et conclu à sa connotation abusive et commerciale. L'existence d'un besoin normatif doit maintenant être confrontée à l'organisation sociale d'Internet.

Par conséquent, la recherche du degré de juridicité de l'interdiction de cette activité requiert une attention particulière, dans ce second chapitre, aux ressources Internet (section I) et aux acteurs disposant d'un quelconque pouvoir à l'origine de l'élaboration de cette règle (section II).

En effet, il importe d'étudier en détail les différentes structures informatiques du Cyberespace en fonction des rapports sociaux qu'elles permettent. Cette organisation particulière dévoilera les détenteurs de pouvoirs susceptibles de répondre, pour chaque ressource du réseau atteinte par le *spamming*, à la demande normative. Ces résultats emporteront, dans notre seconde partie, des différences de degré de prévisibilité de l'interdiction du *spamming* en fonction des contextes électroniques pour lesquels s'effectue l'interprétation et l'application de cette règle, c'est-à-dire en fonction des lieux du décodage de la norme.

Section I - Les lieux du décodage

Avant d'examiner les lieux du décodage, rappelons d'abord qu'Internet est un réseau décentralisé créé à l'origine pour des raisons de stratégie militaire. Cette organisation informatique devait empêcher le bris des communications lors d'un arrêt inopportun de l'une ou l'autre des parties du réseau. En conséquence, la structure d'Internet suppose qu'aucune partie n'est essentielle à son fonctionnement. Contrairement à un réseau informatique centralisé, cette caractéristique implique que nulle entité n'exerce de contrôle sur l'ensemble du Cyberespace. Chaque ordinateur relié au réseau « [...] acts autonomously, coordinating traffic with its nearest connected neighbors, and guided only by the « invisible hand » that arises from the sum of millions of such independent actions[79] ».

Toutefois, Internet n'échappe pas à certaines considérations techniques. Comme chaque réseau informatique, il nécessite l'utilisation de langages informatiques régissant l'exécution des opérations sur le réseau, les protocoles. À ce titre, l'exécution des opérations Internet est gouvernée par des protocoles dits ouverts. Un protocole ouvert est (contrairement à un protocole privé) un protocole accessible au public et qui peut être employé pour créer des systèmes compatibles. Ainsi, le protocole de communication TCP/IP est un protocole ouvert qui regroupe « [l]'ensemble des protocoles de communication utilisés dans Internet et permettant de gérer la circulation des données dans le réseau tout en assurant le bon échange des données entre un point et un autre du réseau[80] ». Par la création de systèmes compatibles, les protocoles Internet facilitent l'intégration d'environnements informatiques différents. Cette caractéristique fondamentale fait d'Internet un « réseau ouvert ». En d'autres termes, des ordinateurs de différents types peuvent entretenir des communications malgré leur langage informatique respectif.

---

[79] D. L. BURK, *loc. cit.*, note 2.

[80] M. BERGERON, C. KEMPA et Y. PERRON, *op. cit.*, note 33.

Si l'ouverture et la décentralisation d'Internet sont des particularités qui ont contribué à son internationalisation, il faut concéder aux ressources Internet un rôle prépondérant dans le processus de démocratisation rapide de ce nouveau mode de communication. Ces ressources se matérialisent sous forme de services particuliers fournis par un ou plusieurs serveurs informatiques et généralement accessibles par des logiciels clients. Le modèle client/serveur est « [u]n modèle informatique basé sur le traitement distribué selon lequel un utilisateur lance un logiciel client à partir d'un ordinateur relié à un réseau, déclenchant simultanément le lancement d'un logiciel serveur situé dans un autre ordinateur possédant les ressources souhaitées par l'utilisateur[81] ». Les logiciels client et serveur communiquent ensemble par le biais d'autres langages informatiques, des protocoles spécifiques. À titre d'exemple, la ressource télématique Web est constituée de serveurs Web utilisant le protocole HTTP (*HyperText Transfer Protocol*) dont se servent les logiciels de navigation pour exploiter ce service.

Caractérisée par des protocoles spécifiques, chaque ressource Internet dévoile un usage de nature différente et une forme d'organisation particulière. On remarque en effet que les ressources Internet sont à usage soit communautaire soit individuel et que l'organisation du contrôle du flux de l'information est centralisé ou décentralisé. Ce constat fait d'Internet un réseau hétérogène (sous-section I) et intransitif (sous-section II).

Sous-section I - Un réseau hétérogène

L'hétérogénéité du réseau Internet s'explique par la présence de ressources communautaires et individuelles. À l'exemple de la séparation du droit public et privé, l'existence de ressources de natures opposées résulte des différents rapports qui s'établissent entre les individus.

---

[81] *Id.*

À ce titre, la différenciation des ressources Internet ne repose pas, à l'exemple des composantes matérielles du réseau, sur le concept de propriété. Elle se fonde plutôt sur les interrelations des usagers lorsqu'ils exploitent ces ressources. Ces dernières donnent lieu à des rapports de nature privée ou publique. La distinction révèle le caractère individualisant de certaines ressources, les ressources dites « individuelles » (B), et l'existence de communautés pour d'autres, dénommées ressources « communautaires » (A). En dressant cette frontière, nous pensons pouvoir établir un lien entre la juridicité de l'interdiction du *spamming* et le développement d'un sentiment communautaire lié à une ressource Internet.

A. Les ressources « communautaires »

Représentative des interrelations existantes entre les internautes utilisant une ressource spécifique, la notion de « communauté » n'est pas indifférente de la proposition doctrinale de l'autoréglementation. S'agissant de normes volontairement développées et acceptées par ceux qui prennent part à une activité, cette voie de solution sous-tend la présence d'un groupe de personnes unies par un élément commun[82]. La présence de « communautés » est donc, en principe, une condition favorable à l'autoréglementation.

Le sens ordinaire du terme « communauté », tel qu'indiqué par le petit Robert, se définit comme un « [g]roupe social dont les membres vivent ensemble, ou ont des biens, des intérêts en commun[83] ». En relation avec le Cyberespace, le concept de « communauté »

---

[82] L'expression « communauté » est également familière avec le débat théorique de l'émergence de normes coutumières, tel que le débat sur l'existence de la *lex mercatoria*. Voir : Filali OSMAN, *Les principes généraux de la Lex Mercatoria : contribution à l'étude d'un ordre juridique anational*, Paris, L.G.D.J., 1992; Vincent GAUTRAIS, Guy LEFEBVRE et K. BENYEKHLEF, « Droit du commerce électronique et normes applicables : l'émergence de la *lex mercatoria* », (1997) 5 *RDAI/IBLJ* 547.

[83] Dans une autre optique, le concept traditionnel de « communauté » ferait référence à un projet commun, aux institutions, à la rationalité et à la productivité. Dans le cyberespace, il n'existerait pas de communautés au sens traditionnel mais des communautés virtuelles. Ces dernières favoriseraient une culture post-moderne et un retour de la technique dans la culture où « [...] le projet commun, compris dans la modernité comme l'engagement politique, laisse la place à des intérêts ponctuels et communs, ancré sur la sympathie et le plaisir esthétique, ayant son épuisement dans l'action quotidienne ». André LEMOS, « Les Communautés virtuelles », (1994) in *Société*, Paris: Dunod, 1994, no 45, pp. 253-261.

virtuelle apparaît plus approprié. Le professeur Howard Rheingold propose une définition reprenant les éléments classiques du concept de communauté, c'est-à-dire des rapports sociaux et un intérêt partagé par plusieurs individus :

> Les communautés virtuelles sont des regroupements socioculturels qui émergent du réseau lorsqu'un nombre suffisant d'individus participent à ces discussions publiques pendant assez de temps en y mettant suffisamment de cœur pour que des réseaux de relations humaines se tissent au sein du Cyberespace.[84]

Au regard d'une ressource dite « communautaire », cette définition appelle une observation intéressante. On remarque en effet l'absence de l'utilisation commune d'une ressource comme critère essentiel de l'existence d'une communauté virtuelle. L'explication du professeur Rheingold fait fi du moyen particulier de communication des internautes au profit de « discussions publiques » ayant cours sur l'ensemble du réseau, la ou les ressource(s) Internet utilisée(s) étant sans importance.

L'élément de « discussion publique » constitue néanmoins une condition révélatrice. N'autorisant pas des discussions à caractère public, c'est-à-dire des discussions auxquelles chaque internaute est invité, certaines ressources Internet ne sont pas favorables à la formation de communautés. Celles-ci, opérant par des protocoles particuliers, avantagent plutôt des communications privées. C'est pourquoi la formule « *Email community* » ou « *Email user community* » ne s'emploie pas pour qualifier les utilisateurs du courrier électronique alors que les expressions « *Usenet community* », « *IRC community* » et « *Mud's community* » désignent respectivement les utilisateurs des ressources Usenet, IRC et Mud.

Ce nouveau langage souligne l'existence de certaines ressources Internet « communautaires » où l'usage du même protocole parvient, par le caractère public des

---

[84] Howard RHEINGOLD, *Les communautés virtuelles*, (trad. Lionel Lumbroso), Paris, Éditions Addison-Wesley France, SA, coll. Mutations Technologiques, 1995, p. 6.

échanges qu'il permet, à créer le sentiment de partage d'un bien commun, d'un espace public.

Usenet constitue un exemple significatif d'une ressource dite « communautaire ». Cette ressource télématique peut se définir comme un « [r]éseau mondial distribué de groupes de discussion, constitué d'un ensemble de serveurs où sont centralisés les articles traitant de sujets particuliers et auxquels les internautes ont accès sur demande[85] ». Le caractère public des articles postés sur les serveurs Usenet s'explique par la possibilité d'accéder aux contenus sur demande.

Connue pour sa juste description du Cyberespace, la célèbre décision *American Civil Liberties Union* c. *Reno*[86], portant sur la constitutionnalité du *Communications Decency Act of 1996*[87], met en évidence l'ouverture des groupes de discussion. La Cour observe cependant que « [*s*]*ome USENET newsgroups are "moderated" but most are open access. For the moderated newsgroups, all messages to the newsgroup are forwarded to one person who can screen them for relevance to the topics under discussion*[88] ».

Dans la même décision, la Cour dresse un parallèle entre les groupes de discussion Usenet et les listes de distribution. Elle présente ces ressources comme des moyens de communication similaires et insiste sur le caractère public des échanges qu'elles rendent possible. Les listes de distribution sont des « [l]istes identifiées par un pseudonyme et vers lesquelles sont expédiés les messages qui seront transmis par courrier électronique à

---

[85] M. BERGERON, C. KEMPA et Y. PERRON, *op. cit.*, note 33. La ressource Internet Usenet utilise le protocole NNTP.

[86] 929 F. Supp. 824 (E.D. Pa. 1996), http://www.ciec.org/decision_PA/decision_text.html, réaffirmée dans *Reno* v. *American Civil Liberties Union*, 117 S. Ct. 2329 (1997)

[87] 47 U.S.C. §§ 223.

[88] *American Civil Liberties Union* c. *Reno*, précitée, note 86, par. 25.

tous les participants du groupe de discussion dont l'adresse est enregistrée dans cette liste[89] ».

À l'instar des groupes de discussion Usenet, les listes de distribution peuvent être modérées ou non. Il existe cependant une distinction fondamentale entre ces moyens de communication. Contrairement aux groupes de discussion Usenet, l'utilisation des listes de distribution est précédée d'une inscription auprès de l'administrateur de la liste. Dans le cas des listes dites ouvertes, cette requête est acceptée automatiquement. Cependant, lorsqu'une liste de distribution est dite fermée, certaines inscriptions peuvent être refusées, les requérants ne correspondant pas au type d'interlocuteur recherché.

Le caractère public des messages est fonction de l'ouverture de chaque liste de distribution. Néanmoins, une liste de distribution fermée peut comporter un nombre appréciable de membres, ces derniers pouvant constituer une communauté virtuelle. L'ouverture à un certain nombre d'individus forme l'élément-clef des « discussions publiques ». Ainsi, le caractère public d'une ressource Internet ne repose pas sur l'ouverture inconditionnelle de leurs communications mais sur un minimum d'individus y ayant accès.

Le développement d'une communauté virtuelle n'est pas pour autant conditionné par l'existence de ressources Internet. En effet, certaines communautés pourront utiliser plusieurs ressources Internet et « [...] participer à des discussions publiques pendant assez de temps en y mettant suffisamment de cœur pour que des réseaux de relations humaines se tissent au sein du Cyberespace[90] ».

À cet égard, la ressource télématique Usenet ne favorise pas la présence que d'une unique communauté. En effet, un bon nombre de groupes de discussion Usenet offre,

---

[89] M. BERGERON, C. KEMPA et Y. PERRON, *op. cit.*, note 33. Notons que les listes de distribution ne sont pas réellement des ressources Internet. Elles sont plutôt des lieux virtuels, privés ou publics, utilisant le courrier électronique et donc, le protocole SMTP.

[90] H. RHEINGOLD, *op. cit.*, note 84.

selon Tamir MALTZ, une continuité et une cohésion suffisante pour être considéré comme des communautés virtuelles[91]. Il n'y aurait donc pas, au sens de la définition de Rheingold, une véritable communauté Usenet mais une ressource Internet favorisant la création de multiples communautés virtuelles comportant plus ou moins de rapports sociaux.

Le concept de « ressource communautaire » que nous proposons vient pallier au flou des expressions « *Usenet community* », « *IRC community* », « *Web community* » et « *Mud's community* ». En mettant l'accent sur le sentiment communautaire d'une ressource, ce concept n'a pas pour effet d'insinuer l'existence d'une communauté virtuelle propre à l'une ou à l'autre des ressources Internet. Elle démontre seulement que le caractère public des communications favorise le développement d'un sentiment communautaire à l'égard de certaines ressources Internet.

B. Les ressources « individuelles »

Contrairement aux ressources « communautaires », les ressources « individuelles » ne se caractérisent pas par des communications publiques et sont moins susceptibles d'être considérées comme un bien commun. Le développement d'un sentiment communautaire n'est pas même favorisé par l'utilisation de cette ressource pour dénoncer publiquement les problèmes de fonctionnement. À cette fin, les discussions doivent être menées sur des moyens de communication à caractère public.

Parmi les ressources « individuelles » d'Internet, le courrier électronique est la plus utilisée. Fonctionnant avec les protocoles SMTP et POP, cette ressource accorde à chaque usager une boîte de courrier électronique et un compte usager lui permettant de recevoir et d'expédier des courriers électroniques. D'un point de vue technique, le courrier électronique rend possible, à l'exemple du courrier traditionnel, l'envoi de

---

[91] Tamir MALTZ, « Customary Law & Power in Internet Communities », (1996) *Journal of Computer-Mediated Communication*, http://www.ascusc.org/jcmc/vol2/issue2/.

messages à un ou plusieurs autres usagers. Mais à l'inverse des listes de distribution, il n'engendre pas la création d'un espace public. Il s'agit seulement d'une fonction offrant la faculté d'envoyer ponctuellement un message à des usagers préalablement sélectionnés par le destinateur. Le courrier électronique occasionne plutôt des communications à caractère privé.

Constituant des espaces imperméables aux intrusions publiques, les boîtes de courriers électroniques sont également de nature privée. Dès lors, les messages importuns ne nuisent qu'à l'usager destinataire[92]. Du moins, ces messages ne trahissent pas leur nuisance aux yeux de tous, au contraire des pollupostages.

Soucieux de maintenir leurs boîtes de courriers électroniques exemptes de messages incommodants, un bon nombre d'internautes se sont tournés vers les solutions techniques, vers des programmes permettant de filtrer plus ou moins efficacement les messages indésirables. Cet enthousiasme pour les outils de filtrage a révélé une inquiétude partagée par maints usagers. Né d'un problème affectant l'ensemble des internautes, cet intérêt commun doit toutefois être dissocié du désir collectif de préserver la fonctionnalité d'une ressource à caractère public. La distinction est importante. Il existe en effet une différence notable du point de vue de l'émergence de la rationalité. Au regard du courrier électronique non sollicité, la valeur accordée au droit de propriété par les protagonistes du réseau s'explique davantage par le souhait personnel d'épurer sa boîte de courriers électroniques des messages importuns que par le développement d'un sentiment communautaire. À cet égard, une comparaison entre le pollupostage et le courrier électronique non sollicité s'avère convaincante.

Dans les premières années de la ressource Web, le phénomène du courrier électronique non sollicité était « l'apanage » de la partie nord-américaine du réseau. À cette époque, les premiers fournisseurs d'accès Internet étrangers venaient se greffer au réseau. Des

---

[92] Ces messages nuisent aussi au fournisseur d'accès Internet de l'usager lorsqu'il doit mémoriser une quantité importante de courriers électroniques non sollicités.

internautes de toute nationalité bénéficiaient à leur tour des avantages du courrier électronique et des groupes de discussion Usenet. Alors que la plupart d'entre eux recevait peu de courriers électroniques non sollicités, les usagers nord-américains souffraient déjà largement de cette pollution. Contrairement au pollupostage, le pourriel représentait alors un problème régional méconnu des nouveaux arrivants.

Caractérisée par des communications publiques, la ressource Usenet avait en effet rapidement révélé la nature abusive des pollupostages : des groupes de discussion bondés d'articles promotionnels répétitifs et sans pertinence avec le thème initial. Une emprise commerciale d'une ressource « communautaire » qui a sûrement fait reculer plusieurs des nouveaux utilisateurs.

Cet exercice de comparaison met en exergue l'existence d'un facteur favorisant l'individualisation des intérêts. S'agissant du caractère privé des communications, cet élément varie en fonction des ressources du réseau. Toutefois, il ne représente pas un obstacle infranchissable à la mise en commun des intérêts de chacun. Il est seulement susceptible d'en retarder l'accomplissement et de différer la mise en œuvre de solutions collectives. Récemment dévalisé, un citoyen se dotera d'un système de sécurité alors que la situation nécessite une amélioration des services de gardiennage. Une décision collective que ses voisins refusent, du moins jusqu'au cambriolage de leur résidence. La dynamique ne serait-elle pas autre s'il s'agissait de leur fond commun de retraite?

Le courrier électronique n'est pas l'unique ressource « individuelle » où se manifeste le *spamming*. Les outils de recherche sont également caractérisés par des communications privées. S'agissant de programmes de recherche opérés par des compagnies privées et financés par des revenus publicitaires, ces outils ne disposent d'aucune fonction permettant une discussion publique. Les recherches effectuées par leurs utilisateurs constituent des requêtes ponctuelles ne bénéficiant qu'à chacun d'entre eux.

Par ailleurs, le désir de préserver la fonctionnalité de ces ressources ne semble pas s'être développé chez les utilisateurs. Du reste, ils ont pris l'habitude de décrier les défaillances des outils plutôt que leurs détracteurs, au grand dam des propriétaires de ces ressources.

En effet, ces derniers supportent seuls les difficultés de leur entreprise et perçoivent leur résolution comme une obligation :

> *According to Sue LaChance, senior product manager of search technologies for Infoseek, spamming is becoming more prevalent and has created a big headache for search engine administrators who want to provide the best service possible for Internet users.*
>
> [...]
>
> *« Search engines are here to provide a service to our customers and we have a responsibility to do everything we can to beat spammers, » says Pritchard [managing director for search services for Hotbot].*[93]

Pour respecter cette obligation, les opérateurs d'outils de recherche bénéficient de la constitution centralisée de leurs ressources malgré la décentralisation du réseau Internet.

Sous-section II - Un réseau intransitif

En raison du caractère décentralisé d'Internet, il s'avère difficile de rompre une communication entre deux serveurs du réseau. Cet exercice nécessite la collaboration d'un bon nombre de serveurs susceptibles d'isoler l'un des deux interlocuteurs. Mais cette structure décentralisée n'est pas entièrement transitive. Les organisations des ressources Internet n'obéissent pas toutes à cette structure particulière. Certaines opèrent sous un modèle centralisé contrôlé par une seule et unique entité. La différenciation des ressources Internet selon leur structure s'effectue donc sur le plan du contrôle des

---

[93] Lori PIQUET, « Search Engines Battle the New Spam » (1998) *ZDNet*, http://www.zdnet.com/devhead/stories/articles/0,4413,1600389,00.html.

communications. Plus précisément, il importe de se référer à la capacité d'un ou de plusieurs acteurs à s'immiscer dans le contenu diffusé par un serveur tiers.

L'exercice du contrôle se présente comme un principe inébranlable : chaque administrateur maîtrise la totalité du serveur qu'il gère. Il peut à son aise limiter son accès, filtrer son contenu et même cesser ses opérations. Chaque administrateur surveille donc, pour sa « part du réseau », les communications Internet. Ainsi, les ressources centralisées sont celles qui ne dépendent pas du filtrage d'administrateurs tiers.

La qualification des ressources Internet selon l'exercice du contrôle a pour objectif de vérifier le lien entre le morcellement du pouvoir et le degré de juridicité de l'interdiction du *spamming*. En effet, lorsqu'une seule entité contrôle l'ensemble du contenu d'une ressource, il est probable que les règles émises soient appliquées et interprétées dans le respect de la signification voulue par leur auteur.

Parmi les ressources où se manifeste le *spamming*, celles fonctionnant par l'emploi de programmes particuliers sont généralement centralisées (A) alors que les ressources n'utilisant que des protocoles Internet demeurent décentralisées (B).

A. Les ressources centralisées

Seule une ressource affectée par le *spamming* opère sous un modèle centralisé. En tant que programmes, les outils de recherche n'autorisent pas leurs utilisateurs à filtrer les résultats de leurs requêtes. En effet, chaque mot-clef ou association de mots-clefs génère systématiquement les mêmes résultats. Seul le gestionnaire du programme de recherche est en droit de modifier le contenu soit en retirant de sa base de données un site, soit en le déclassant dans la présentation des résultats. Également, lui seul a le loisir de refuser l'indexation d'un contenu. En somme, le gestionnaire est l'unique maître à bord.

La centralisation du contrôle s'explique par le rôle de pilier que joue un outil de recherche envers ses utilisateurs. Pour bénéficier d'un outil de recherche, ces derniers sont contraints d'utiliser son programme spécifique situé sur un serveur Web. À l'inverse des ressources fondées essentiellement sur un protocole et son modèle client/serveur, un outil de recherche s'impose donc comme un « serveur central ».

Un MUDs (*Multi-User Dungeons*) fonctionne également par exécution d'un programme et constitue, en tant que tel, une ressource centralisée. Un MUDs se définit comme :

> [...] *a software program that accept connections from multiple users across some kind of network (e.g., telephone, line on the Internet) and provides to each user access to a shared database of " rooms ", " exits " and other " objects ". Each user browses and manipulates this database from " inside " one of those rooms, seeing only those objects that are in the same room and therefore is a kind of virtual reality, an electronically-represented " place " that users can visit.*[94]

Contrairement aux ressources décentralisées, un MUDs est entièrement contrôlé par :

> [...] *the persons running the actual MUD program, commonly referred to as Gods* [...]. *They have direct access to the computer files which comprise the system, enabling them to modify the MUD database in any way they please. They can design any virtual setting into the system, and so create a MUD universe of any flavour they wish. Within the game world, they have access to a range of commands which allow them to edit the world while interacting with it. They can edit and destroy any object on the MUD system--including the objects that represent players' characters.*[95]

---

[94] Pavel CURTIS, « Mudding : Social Phenomena in Text-Based Virtual Realities », (1992), ftp://parcftp.xerox.com/pub/MOO/papers/DIAC92.

[95] Elizabeth REID, « Cultural Formations in Text-Based Virtual Realities », (1994), ftp://ftp.lambda.moo.mud.org/pub/MOO/papers/CulturalFormations.txt.

Précisons que les MUDs ont été qualifiés de structures hiérarchiques eu égard à la faculté pour l'administrateur de déléguer son pouvoir à quelques personnes[96]. Toutefois, il s'agit d'une centralisation qui peut être tempérée par les demandes, les interrogations et les besoins de la communauté MUDs que chapeaute l'administrateur[97].

B. Les ressources décentralisées

Les groupes de discussion Usenet et le courrier électronique présentent les attributs de ressources décentralisées. N'étant pas sujettes à une centralisation du pouvoir, leur fonctionnement repose essentiellement sur l'application du modèle client/serveur. Tout administrateur est donc autorisé à effectuer une opération de filtrage, offrant à l'utilisateur un contenu différent du contenu original.

Selon le processus de distribution des groupes de discussion sur USENET, les serveurs s'échangent le contenu des groupes qu'ils maintiennent et celui de ceux provenant de serveurs tiers. Chaque administrateur a donc la possibilité de refuser de distribuer l'un ou l'autre des groupes qu'il gère et de choisir ceux qu'il désire diffuser[98].

Les serveurs de courriers électroniques peuvent filtrer les messages qu'ils reçoivent selon des critères particuliers, tels que le nom de domaine du serveur ayant autorisé l'envoi de messages abusifs par ses utilisateurs. Généralement, le filtrage des messages est effectué soit par le « propriétaire » de la boîte de courriers électroniques soit par son serveur. Principal intéressé, l'utilisateur est libre de filtrer les messages selon ses propres critères. À cette fin, plusieurs programmes sont disponibles sur le réseau. Nous en ferons

---

[96] T. MALTZ, *loc. cit.*, note 91.

[97] Jennifer BEAULIEU , « Les muds ou l'art de réussir le renouveau communautaire par la Coopération », (1997) *Espace Droit*, http://www.droit.umontreal.ca/espacedroit/fr/crdp/ 1997/beauliej.html.

[98] Jon BELL, « News.newusers.questions : What newsgroups are and how they work? », (1999) http://www.geocities.com/ResearchTriangle/Lab/6882/how-it-works.html.

une courte description dans notre deuxième partie lorsque nous aborderons les solutions techniques au problème du *spamming*.

Caractérisée par des communications publiques, la ressource Usenet autorise également ses utilisateurs à annuler leurs propres postages. De cette façon, ils ont la faculté d'éviter la diffusion d'un article s'avérant dommageable. Un bon nombre de serveurs permettent aussi l'annulation des articles postés par un tiers. L'annulation doit être justifiée autrement que par le contenu du message[99]. Généralement, sept critères sont admis par les administrateurs de serveurs Usenet[100] :

> 1. Lorsque le groupe de discussion où réside l'article est modéré, le modérateur peut l'annuler;
> 2. Lorsque l'article est un multipostage (EMP) ayant un indice Breidbart de 20 ou plus;
> 3. Lorsque le mauvais fonctionnement d'un programme cause le postage et le repostage d'une série d'articles (*spew*);
> 4. Lorsque l'article est un postage croisé (ECP) ayant un indice Briedbart de 20 ou plus;
> 5. Lorsque l'article contenant un fichier binaire, tel qu'une image, est posté sur un groupe de discussion n'autorisant pas ce type de fichier;
> 6. Lorsque l'identité de l'auteur de l'article est falsifié, et
> 7. Lorsque l'article constitue une violation de la propriété intellectuelle.

Si un administrateur peut s'opposer à la diffusion de certains groupes de discussion, il peut également refuser les annulations de messages qu'il reçoit en propre ou celles qui lui proviennent des serveurs de son entourage[101]. L'annulation de messages par des tiers est donc une délégation du pouvoir aux usagers[102].

---

[99] T. SKIRVIN, « The Cancel FAQ », (1997), http://www.ews.uiuc.edu/~tskirvin/faqs/cancel.html. La section 7.1 du document de travail proposé RFC 1036bis voulait proposer quelques raisons valables pour annuler un article. Henry SPENCER, « News Article Format and Transmission (INTERNET DRAFT to be), (1994), http://www.ews.uiuc.edu/~tskirvin/faqs/rfc1036b.

[100] *Id.*

[101] *Id.*

[102] L'exercice de ce pouvoir s'avère toutefois laborieux pour le commun des internautes. *Id.*

En plus de permettre une distinction entre les ressources centralisées et décentralisées, l'exercice du pouvoir rend possible d'identifier l'origine de l'interdiction du *spamming*.

Section II - Les auteurs de l'encodage : l'origine des normes

L'origine des normes est traditionnellement attribuée au processus législatif. Or, caractérisé par un environnement électronique transnational et décentralisé, le réseau Internet regorge de foyers normatifs. En règle générale, ces derniers ont pour corollaire l'exercice d'un pouvoir : politique, naturel, technique, législatif, judiciaire, etc.

Au regard de nos sociétés modernes, les pouvoirs législatif, judiciaire et exécutif sont, au sommet de nos constructions étatiques, les principaux pouvoirs concurrents. Manifestations essentielles de la souveraineté, ceux-ci n'autorisent aucune autre autorité. La branche législative ne peut déléguer sa compétence qu'en vertu de la norme suprême de l'État, une constitution élaborée par les instances politiques, représentantes du peuple. On retrouve ici la conception positive du droit et de l'État de Kelsen.

Selon Gérard Timsit, cette conception repose sur un système de droit homogène et transitif. Un système monologique, absolu et statocentrique où toute norme est nécessairement reliée au domaine public, l'autonomie des volontés étant autorisée par le droit objectif, et où aucune norme n'est autonome, chacune étant subordonnée à une norme supérieure[103]. Un tel système favorise un degré élevé de juridicité alors que les systèmes dialogiques, systèmes hétérogènes et intransitifs, entretiennent une faible intégration du contrôle du décodage[104].

Cette remarque ne doit pas avoir pour effet d'assimiler les systèmes normatifs aux environnements électroniques. En effet, l'intransivité et l'hétérogénéité d'un système ne

---

[103] G. TIMSIT, *Thèmes et systèmes de droit*, Paris, Presses Universitaires de France, 1986, pp. 57 et 73.

[104] G. TIMSIT, *op. cit.*, note 5, pp. 187 et s.

correspondent pas à celles d'un réseau. Il ne faut confondre ni « le mode d'engendrement du droit » avec « l'organisation du contrôle des données » ni « le type de situations où se trouvent placés les destinataires de la norme » avec « la nature des ressources Internet ».

Toutefois, un système normatif est susceptible d'évoluer en fonction de son environnement. Ainsi, « l'organisation du contrôle des données » peut influencer « le mode d'engendrement du droit ». De même, « le type de situation où se trouvent placés les destinataires de la norme » risque de varier selon « la nature des ressources d'Internet ». Une ressource de nature « individuelle » et de forme décentralisée peut donc encourager la création d'un système normatif dialogique.

La vérification de cette relation impose de situer les normes étatiques au même niveau que toute norme résultant de l'exercice d'un autre pouvoir. En effet, les règles issues du processus législatif ne s'inscrivent pas en marge de cette relation : leur degré de juridicité demeure dépendant de la pré-, co- et surdétermination.

Cette présente section est donc consacrée au pouvoir des autorités du réseau (sous-section I) mais également au pouvoir législatif. (sous-section II).

Sous-section I - Les autorités du réseau

Les autorités détiennent un pouvoir technique issu de la structure physique du réseau ou jouissent d'un ascendant politique révélé par un regroupement d'intérêt.

Le pouvoir technique découle du contrôle d'un serveur ou d'un programme informatique. Ainsi, ce sont les propriétaires de ressources qui bénéficient de ce pouvoir (A). La sanction privilégiée par ces acteurs est l'exclusion du système, serveur ou programme, que l'administrateur contrôle. L'éviction d'un système s'effectue soit par le retrait du droit d'accès à la ressource soit par le filtrage des communications de l'usager.

Le pouvoir politique fait plutôt référence aux mouvements de pression constitués par des internautes partageant les mêmes intérêts. Leurs activités consistent à mener des campagnes d'information et à persuader les pouvoirs législatifs des différents pays. Les sanctions favorisées sont la marginalisation des fauteurs et la dénonciation aux autorités détenant un pouvoir technique. Les « communautés », leurs représentants et les internautes sont tous susceptibles de bénéficier du pouvoir politique (B).

A. Les propriétaires de ressources

Les fournisseurs d'accès Internet et les administrateurs de serveurs et de ressources centralisées sont les principaux propriétaires disposant d'un pouvoir technique.

Jouissant d'une plus grande autorité, les FAI agissent également à titre d'administrateurs de ressources décentralisées, c'est-à-dire de ressources reposant sur un modèle client/serveur. Un fournisseur d'accès Internet (FAI) est une « [s]ociété permettant à des particuliers ou à des compagnies, moyennant une rétribution, d'utiliser son système pour naviguer dans le réseau Internet[105] ». Un FAI ordinaire possède donc ses propres serveurs Web, SMTP, POP et Usenet, ce qui le place dans une double position d'autorité.

La première manifestation de l'autorité des FAI consiste à pouvoir rompre leurs contrats de service. Qualifiables de contrats d'adhésion, ces conventions comportent généralement des règles de conduite communément dénommées *Acceptable Use Policies* (AUP). Par exemple, le fournisseur d'accès Internet Sympatico introduit ses « Règles d'utilisation acceptable » en stipulant que « [l]es activités énumérées constituent des violations de la Convention du Service Sympatico et peut (sic), à la discrétion exclusive du service Sympatico, être considérées comme motifs pour

[105] M. BERGERON, C. KEMPA et Y. PERRON, *op. cit.*, note 33. Les FAI offrent également à leurs abonnés la possibilité d'héberger leurs documents sur un espace Web mis à leur disposition.

l'annulation d'un compte, pour la facturation de frais supplémentaires ou pour la demande de participation d'autorités chargées de l'application des lois[106] ». Les activités énumérées incluent certains comportements abusifs reliés au *spamming* dont le courrier électronique non sollicité et le pollupostage :

> Courrier électronique
>
> Il vous est interdit d'utiliser votre compte de courrier électronique Sympatico afin de :
>
> - transmettre des messages électroniques non sollicités à caractère commercial ou d'entreprendre du publipostage de masse qui, selon le jugement exclusif du service Internet Sympatico, provoque un dérangement important ou suscite des plaintes de la part d'autres utilisateurs d'Internet.
> - transmettre des lettres à chaîne ou des offres de vente en pyramide de quelque façon que ce soit.
> - harceler d'autres individus ou groupes de quelque façon que ce soit.
> - représenter faussement les en-têtes de vos messages électroniques de quelque façon que ce soit.
>
> [...]
>
> Groupes de discussion
>
> Tout article affiché dans un groupe de discussion doit être conforme à la FAQ ou à la charte de ce groupe. Lorsque vous contribuez aux groupes de nouvelles, il vous est interdit de (d') :
>
> - afficher des messages publicitaires ou à caractère commercial de toute sorte, à moins que de tels messages soient permis spécifiquement par la charte ou la FAQ du groupe en question.
> - afficher les fichiers binaires (p. ex., images, sons ou applications) à moins que l'affichage de fichiers binaires soit permis spécifiquement par la charte ou la FAQ du groupe en question.

---

[106] *Règles d'utilisation acceptable du service Sympatico* du 27 août 1998 : http://www2.sympatico.ca:80/Aidez/local/bell/aup.bell.html.

- afficher des messages ayant une grande ressemblance entre eux à plus de dix groupes de discussion.
- harceler d'autres individus ou groupes de quelque façon que ce soit.
- représenter faussement de quelque façon que ce soit les en-têtes de vos contributions aux groupes de discussion.[107]

Constituant un moyen rapide et efficace de sanctionner leurs usagers, l'annulation de comptes repose toutefois sur des règles contractuelles sujettes à la sanction d'un tribunal à titre de loi des parties. À cet égard, il faut reconnaître la double origine technique et étatique de ces normes.

La seconde manifestation d'autorité suggère moins de références à l'autorité étatique. En tant qu'administrateurs de ressources décentralisées, les FAI possèdent un droit de regard sur les communications qui empruntent leurs systèmes. Bien qu'aucune relation contractuelle n'existe entre eux et les utilisateurs non abonnés à leurs services, les FAI ont le pouvoir de filtrer, bloquer ou annuler les communications qui occupent leurs serveurs Usenet, SMTP et Web. Ainsi, plusieurs FAI ont édicté des règles d'utilisation pour les internautes utilisant un accès Internet autre. Par exemple, certains affichent leur politique concernant le courrier électronique non sollicité. Au même titre, les administrateurs de serveurs Usenet soutiennent une politique contre le pollupostage, politique reprise dans les Foires aux Questions des groupes de discussion résidants.

Au regard du droit étatique, la légitimité de ces normes s'appuie sur le droit de propriété et la responsabilité civile extracontractuelle. En effet, le droit positif québécois stipule que « [l]e propriétaire d'un bien a le droit de le revendiquer contre le possesseur ou celui qui le détient sans droit; il peut s'opposer à tout empiétement ou à tout usage que la loi ou lui-même n'as pas autorisé[108] ». Or, lorsqu'il est question de *spamming*, les installations informatiques sont utilisées d'une manière qui n'est pas autorisée par leurs propriétaires, les fournisseurs d'accès Internet.

---

[107] *Id.*

[108] Code civil du Québec, art. 953.

Le courrier électronique non sollicité ou le pollupostage risquent également de constituer une faute qui engagerait la responsabilité extracontractuelle de leurs auteurs[109]. À cet égard, il n'est pas certain que le *spamming* puisse être considéré comme la conduite d'une personne raisonnable. La connotation abusive que plusieurs protagonistes attribuent à cette activité pourrait devenir le témoin de son caractère fautif. Le lien de causalité et le préjudice, si on ignore les possibilités d'anonymat, devraient être établis facilement par les FAI.

Toutefois, le coût de poursuites internationales et les difficultés qu'elles supposent nous amènent à convenir que les facultés d'annulation, de filtrage et de blocage assurent aux propriétaires de ressources décentralisées un pouvoir moins « théorique » que l'application des règles étatiques. Ceci est d'autant plus vrai lorsqu'il s'agit d'une ressource centralisée.

B. Les « communautés », leurs représentants et les internautes

L'exercice du pouvoir politique est assuré par la prise d'initiatives publiques ou privées destinées à politiser le Cyberespace. La principale caractéristique des auteurs détenant un pouvoir politique est de s'estimer les défenseurs de la « communauté cybernétique ». En présentant leurs énoncés politiques comme issus de consensus, ils établissent des règles soit disant élaborées par une communauté et dignes d'application dans le

---

[109] *Id.*, art. 1457 :

> « Toute personne a le devoir de respecter les règles de conduite qui, suivant les circonstances, les usages ou la loi, s'imposent à elle, de manière à ne pas causer de préjudice à autrui.
> Elle est, lorsqu'elle est douée de raison et qu'elle manque à ce devoir, responsable du préjudice qu'elle cause par cette faute à autrui et tenue de réparer ce préjudice, qu'il soit corporel, moral ou matériel.
> Elle est aussi tenue, en certains cas, de réparer le préjudice causé à autrui par le fait ou la faute d'une autre personne ou par le fait des biens qu'elle a sous sa garde. »

Cyberespace. On peut ainsi découvrir que le *spamming* est un comportement prohibé par les internautes.

Se rapprochant du jeu argumentaire propre aux débats politiques, les campagnes d'information révèlent, dans un environnement soumis à plusieurs foyers normatifs, un discours prescriptif susceptible de répondre aux besoins et aux valeurs de certains utilisateurs.

L'organisation *CAUCE* (*Coalition Against Unsolicited Commercial Email*) est sans doute le premier regroupement d'intérêts digne d'attention. Elle rassemble des volontaires désireux d'obtenir une solution législative au courrier électronique non sollicité. Le *spamming* serait, selon elle, « [...] *the leading complaint of Internet users*[110] ».

Née de la Vieille Garde d'Internet, la hiérarchie Usenet *news.admin.net-abuse* est composée d'administrateurs et d'utilisateurs de groupes de discussion[111]. Elle a pour objectif de définir les abus du réseau, de recevoir des plaintes et d'élaborer des solutions. Postées régulièrement sur la ressource Usenet, leurs Foires aux Questions relatives au courrier électronique non sollicité et au pollupostage constituent une source documentaire impressionnante.

Plus vindicatives, les campagnes de boycottage du *spamming* bénéficient d'un battage publicitaire sur plusieurs sites personnels. De loin la plus connue, la campagne *Combattez le Spamming sur Internet* est disponible en plusieurs versions linguistiques. Chacune d'elles comporte une liste imposante de participants ainsi qu'une panoplie d'informations sur le problème du *spamming*[112]. Moins significatives, d'autres

---

[110] *CAUCE* : http://www.cauce.org/index.html.

[111] *news.admin.net-abuse.** *Homepage*, en date du 1er juillet 1997 : http://www.ews.uiuc.edu/~tskirvin/nana/.

[112] *Combattez le Spamming sur Internet* : http://www.cypango.net/~spam/ et http://spam.abuse.net/.

formations, telles que le *Mouvement Insurrectionnel Contre le Spamming* (MICS), participent également à la dénonciation des abus du réseau. D'origine québécoise, cette campagne a comme visée la promotion de l'information et la recherche de solutions[113].

Dépourvues d'ascendant technique, les autorités politiques favorisent la dénonciation et le boycottage comme moyens de sanction des polluposteurs et des expéditeurs de pourriels. À titre d'illustration, la célèbre *Blacklist of Internet Advertisers* d'Alex Boldt contient un nombre appréciable de noms d'usagers dont on a dénoncé le comportement abusif[114]. Accompagné d'un résumé des activités reprochées, chaque dénonciation est retirée de la liste après une période de trois mois. Le gestionnaire conserve toutefois ces informations dans des archives publiques. Convié à boycotter les mauvais annonceurs, le lecteur dispose donc de renseignements utiles au filtrage. Il jouit aussi d'une liste de distribution créée pour dénoncer les comportements abusifs[115].

De nature publique, la ressource télématique Usenet permet également la dénonciation. Celle-ci s'effectue par l'envoi d'un article sur les groupes de discussion *sightings*, *usenet* et *email* de la hiérarchie *news.admin.net-abuse* (*n.a.n-a.*) [116]. La procédure apparaît toutefois fastidieuse. Ainsi, l'utilisateur est obligé de mentionner le nombre d'articles postés et de groupes de discussion destinataires du pollupostage. Il a également la charge de faire suivre la dénonciation à l'utilisateur fautif ainsi qu'à son administrateur Usenet (généralement son FAI). Enfin, il doit inviter l'administrateur à détailler publiquement les actions qu'il a prises ou qu'il entend prendre.

Ne participant à aucune démarche de dénonciation, l'*Internet Engineering Taskforce* (IETF) n'est pas non plus une association de nature politique. Cette organisation

---

[113] *MISC* : http://pages.hotbot.com/politics/tetsuo/fr_intro.html.

[114] *Blacklist of Internet Advertisers* : http://math-www.uni-paderborn.de/~axel/BL/blacklist.html.

[115] *Spam-L FAQ*, en date du 16 mai 1999 : http://oasis.ot.com/~dmuth/spam-l/.

[116] J. D. FALK et S. SOUTHWICK, *loc. cit.*, note 34.

internationale est formée de spécialistes en télécommunication, les « gourous d'Internet », et a pour but d'assurer la croissance du réseau. Fonctionnant par groupes de travail, l'IETF développe chaque année une série de recommandations et de documents de travail afin de rendre compte des meilleures façons d'utiliser les ressources Internet. Dénommées *Requests For Comments* (RFC), les recommandations officielles de l'IETF sont généralement acceptées par les différents acteurs du réseau.

Seuls deux documents de travail traitent spécifiquement du pollupostage et du courrier électronique non sollicité. Le premier expose les principes à suivre pour effectuer des activités publicitaires respectueuses de l'esprit de coopération d'Internet[117]. Le *spamming* y est fortement déconseillé. Le second document explique les effets dommageables de cette activité et offre aux internautes et aux administrateurs de systèmes des lignes directrices pour aborder les difficultés qu'elle engendre[118].

Malgré la nature officieuse de ces textes, plusieurs autorités s'y réfèrent sans ambages. Ne relevant pas d'une autorité proprement politique, les initiatives de l'IETF profitent donc de la crédibilité de ses membres et du pouvoir persuasif des scientifiques, un pouvoir différent de la contrainte étatique.

Sous-section II - Les autorités sur le réseau : l'État et la réglementation américaine du *spamming*

Sur le plan de la contrainte, les normes étatiques sont traditionnellement placées dans une situation de force. Les institutions chargées de l'exécution des lois obtempèrent au principe intégrateur de la primauté du droit. Or, les circonstances actuelles changent la donne. Les frontières posent une balise sérieuse à l'application du droit étatique sur un réseau transnational. Elles révèlent l'incapacité de sanctionner rapidement et

---

[117] S. HAMBRIDGE et D. EASTLAKE 3rd, *loc. cit.*, note 78.

[118] S. HAMBRIDGE et Albert LUNDE, « IETF RUN Working Group draft-ietf-run-spew-08 : DON'T SPEW. A Set of Guidelines for Mass Unsolicited Mailings and Postings (spam*) », (avril 1999), http://search.ietf.org/internet-drafts/draft-ietf-run-spew-06.txt> (expire le 21 octobre 1999).

efficacement les étrangers et suggèrent des coûts de poursuite disproportionnés par rapport aux préjudices subis.

Sur le plan de la juridicité, les normes étatiques ne représentent qu'une réponse supplémentaire au besoin normatif lié au *spamming*. Les mouvements de pressions exercés sur le pouvoir législatif par les différents acteurs du réseau n'étonnent pas. Cela témoigne d'un réflexe « social » qui continue de porter ses fruits à l'intérieur des frontières nationales.

Toutefois, les règles étatiques demeurent soumises à l'interprétation et à l'application qui découlent de leur clarté et des valeurs en présence. Leur degré de prévisibilité dépend, à l'instar de toute règle, du contrôle effectif de leur décodage. Rappelons qu'« [i]l faut définir le droit par son caractère obligatoire, mais le faire de manière que cette obligation - d'une part ne soit pas nécessairement référée à l'État, que d'autre part sa portée puisse varier en fonction du degré de spécificité des interrelations qui rendent la norme obligatoire[119] ».

Le droit étatique s'insère donc, dans cette étude, comme un foyer normatif additionnel dont le caractère obligatoire varie, dans la mesure d'une situation transnationale, en fonction des interrelations propres à chacune des ressources Internet.

La présente sous-section expose comment les législateurs tentent de satisfaire les demandes normatives de leurs internautes nationaux. Ce faisant, elle révèle un indice significatif de l'émergence d'un consensus - avec les acteurs du réseau - sur le problème du *spamming*.

C'est aux États-Unis d'Amérique que les propositions législatives de réglementation du *spamming* sont les plus nombreuses. À l'instar des autres initiatives étatiques, les

---

[119] G. TIMSIT, *loc.cit.*, note 14, 45.

mesures projetées ne se rapportent qu'au courrier électronique non sollicité. En quête d'une solution à cet épineux problème, des institutions américaines ont proposé, en 1997 et 1998, une pléiade de mesures. Seize États américains ont considéré plus de dix-sept propositions[120] dont quatre sont actuellement en vigueur[121]. Au palier fédéral, sept projets de loi ont été étudiés lors du 105e Congrès sans qu'aucun n'ait encore pu satisfaire les parlementaires[122].

Bien qu'il soit un peu tôt pour apprécier l'avancement des nouveaux projets de loi pour l'année 1999, nous pouvons entrevoir l'adoption d'une série importante de mesures étatiques[123]. Toutefois, les activités du 106e Congrès américain susciteront davantage l'attention des principaux intéressés. Malgré l'absence de propositions fédérales depuis

---

[120] Alaska House Bill 491 (1997), California Assembly Bill 1629 (1998); California Assembly Bill 1676 (1998), Connecticut House Bill 6558 (1997), Kentucky Bill Resolution 337/House Bill 41 (1998); Maryland House Bill 1114 (1998); Massachusetts House Bill 4581 (1997), Nevada Senate Bill 13 (1997); New Hampshire House Bill 1633 (1997), New Jersey Assembly Bill 295 (1998); New Jersey Assembly Bill 513 (1998), New York Senate Bill 3524/Assembly Bill 6805 (1997); North Carolina House Bill 1744 (1997), Rhode Island Senate Bill 1073 (1997); Virginia House Bill 1325 (1998), Washington House Bill 2752 (1998); Wisconsin Senate Bill 283 (1997).

[121] *Prohibited unsolicited electronic mail*, précitée, note 13 (Washington); *AN ACT relating to actions concerning persons; providing that a person who transmits certain items of electronic mail is liable to the recipient for civil damages under certain circumstances; providing that the district court may enjoin a person from transmitting certain items of electronic mail under certain circumstances; and providing other matters properly relating theret*, précitée, note 13 (Nevada); . *An act to amend Section 17538.4 of the Business and Professions Code, relating to advertising* précitée, note 13 (California); *An act to amend Section 17511.1 of, and to add Section 17538.45 to, the Business and Professions Code, and to amend Section 502 of the Penal Code, relating to advertising*, précitée, note 13 (California).

[122] *Netizens Protection Act of 1997* (H.R. 1748), *Data Privacy Act of 1997* (H.R. 2368), *E-Mail User Protection Act of 1998* (H.R. 4124), *Digital Jamming Act of 1998* (H.R. 4176), *Unsolicited Commercial Electronic Mail Choice Act of 1997* (S. 771), *Electronic Mailbox Protection Act of 1997* (S. 875), *Anti-Slamming Amendments Act* (S. 1618/H.R. 3888). Le projet *Inbox Privacy Act of 1999* (S. 759) a été introduit au 106e Congrès le 23 mars 1999. Il s'agit encore de la seule proposition relative au *spamming* pour cette année.

[123] À titre d'exemple, l'État de Virginie a déjà promulgué trois législations visant à interdire la falsification d'une adresse de courrier électronique non sollicité (*e-mail message transmission information*) et la possession, vente et distribution de logiciels facilitant la falsification de cette information : *An Act to amend and reenact §§ 8.01-328.1, 18.2-152.2, 18.2-152.4, and 18.2-152.12 of the Code of Virginia, relating to personal jurisdiction*, chapter 886, Acts of the General Assembly (1999 Session); An Act to amend and reenact §§ 8.01-328.1, 18.2-152.2, 18.2-152.4, and 18.2-152.12 of the Code of Virginia, relating to personal jurisdiction, chapter 905, Acts of the General Assembly (1999 Session); An Act to amend and reenact §§ 8.01-328.1, 18.2-152.2, 18.2-152.4, and 18.2-152.12 of the Code of Virginia, relating to personal jurisdiction, chapter 904, Acts of the General Assembly (1999 Session).

le début de cette année, le représentant Tom Bliley, président du *House Commerce Committee*, annonce que son comité soumettra une solution législative qu'il tentera de faire adopter par le nouveau Congrès. De concert avec le secteur privé, ces efforts pourraient bien cette fois se concrétiser par une prohibition stricte du courrier électronique commercial non sollicité.

La portée d'une telle décision implique toutefois un bref retour aux diverses propositions antécédentes et aux mesures législatives récemment adoptées par les différents États américains. Ces initiatives reflètent les options qui se présentent aujourd'hui au Congrès américain. Jusqu'à maintenant, deux systèmes de réglementation ont fait l'objet de ces propositions et mesures.

Généralement, les fournisseurs d'accès Internet (FAI) et les regroupement d'usagers ont souhaité faire adopter un système de réglementation *opt-in*. Cette solution consiste à interdire l'envoi de messages publicitaires à moins d'une acceptation préalable des destinataires. Lorsque cette condition est satisfaite, l'expéditeur doit toutefois fournir une adresse de retour exacte et s'identifier correctement auprès du destinataire. Selon les principaux tenants de ce système, cette solution est susceptible de rompre le transfert des coûts publicitaires aux destinataires de pourriels.

Parmi les propositions législatives fédérales, seul un projet de loi était muni d'un système *opt-in* de réglementation[124]. Ce projet permettait notamment la prise d'action privées de l'ordre de 500 $ (US) par courrier électronique commercial non sollicité ou selon le préjudice établi. Notons que les propositions étatiques ont été beaucoup plus friandes de ce type de réglementation. En effet, six (6) projets lui étaient favorables bien qu'aucun d'eux n'a été adopté.

---

[124] *Netizens Protection Act of 1997* (H.R. 1748)

À l'opposé, les systèmes de réglementation *opt-out* favorisent les partisans du marketing direct. Autorisant l'envoi de courrier électronique non sollicité en l'absence de refus des destinataires, cette solution exige une rôle actif de la part des usagers. Deux options ont été envisagées pour permettre aux destinataires de signifier ce refus. La première alternative consiste en une liste universelle d'exclusion où chaque usager a la possibilité de refuser l'une ou l'autre des catégories de courrier électronique non sollicité - commercial, politique, religieux, etc. La deuxième alternative donne plutôt aux destinataires la possibilité de retirer leurs adresses de courrier électronique de la liste de distribution des expéditeurs; une option qui peut s'avérer extrêmement lourde pour le destinataire. Le nouveau projet fédéral *Inbox Privacy Act of 1999* (S. 759) est à cet effet.

Des mesures proposées, cinq projets de loi fédéraux et sept projets étatiques ont considéré la réglementation du courrier électronique non sollicité selon un système *opt-out*. À l'instar du système de règlementation *opt-in*, ces propositions étaient généralement accompagnées d'une obligation pour l'expéditeur d'identifier correctement ses coordonnées et d'une sanction contre les falsifications d'en-têtes de messages[125]. La loi de l'État de Washington adoptée en mars 1998[126] est à cet effet. Nous pouvons donc envisager qu'une règlementation fédérale conserverait ces mesures complémentaires peu importe le système de réglementation choisi.

---

[125] Il s'agit de la seule exigence de la *Proposition de directive du Parlement européen et du Conseil relative à certains aspects juridiques du commerce électronique dans le marché intérieur*, COM(98) 586, Journal off. 99/C 30 (05/02/1999). En effet, la proposition n'entend pas réglementer outre mesure le courrier électronique non sollicité :

> « Article 7. Communication commerciale non sollicitée
>
> Les États membres prévoient dans leur législation que la communication commerciale non sollicitée par courrier électronique doit être identifiée comme telle, d'une manière claire et non équivoque, dès sa réception par le destinataire. »

[126] *Prohibited unsolicited electronic mail*, précitée, note 13. À l'origine, cette loi devait interdire le courrier électronique commercial non sollicité. La loi telle qu'adoptée crée cependant un groupe de travail destiné à évaluer la suffisance des lois existantes à résoudre les problèmes techniques, légaux et financiers reliés à l'accroissement du nombre de courriers électroniques commerciaux.

Accessoirement, certains aménagements législatifs imposaient aux expéditeurs une classification de leurs messages publicitaires. Cette obligation permettait aux FAI et à leurs usagers de filtrer le courrier électronique non sollicité. L'une des deux nouvelles lois californiennes sur le courrier électronique non sollicité impose aux expéditeurs la classification suivante :

> *(g) In the case of e-mail that consists of unsolicited advertising material for the lease, sale, rental, gift offer, or other disposition of any realty, goods, services, or extension of credit, the subject line of each and every message shall include "ADV:" as the first four characters. If these messages contain information that consists of unsolicited advertising material for the lease, sale, rental, gift offer, or other disposition of any realty, goods, services, or extension of credit, that may only be viewed, purchased, rented, leased, or held in possession by an individual 18 years of age and older, the subject line of each and every message shall include "ADV:ADLT" as the first eight characters.*[127]

Jumelée à un système de réglementation *opt-out*, cette obligation doit être comprise comme une mesure supplétive à la seconde loi californienne[128]. Cette dernière reconnaît aux fournisseurs d'accès Internet le droit d'interdire l'utilisation de leurs systèmes par la diffusion de leurs politiques via le Web. Un FAI californien est donc en droit d'interdire l'envoi de pourriels vers son serveur de courrier électronique et l'emploi de ses ressources par des polluposteurs[129]. Les expéditeurs de messages allant à l'encontre de la politique du serveur du destinataire risquent une amende de 50 dollars américains par message pour un maximum de 25 000 dollars (US) par jour. Il s'agit de la première loi américaine ayant considéré l'approche du droit de propriété.

---

[127] *An act to amend Section 17538.4 of the Business and Professions Code, relating to advertising*, précitée, note 13.

[128] *An act to amend Section 17511.1 of, and to add Section 17538.45 to, the Business and Professions Code, and to amend Section 502 of the Penal Code, relating to advertising*, précitée, note 13.

[129] De la même façon, le nouveau projet de loi H.B. 1037 (1999) de l'État de Washington voudrait interdire le courrier électronique non sollicité pour les fournisseurs d'accès Internet ayant publié leur politique. Cette nouvelle initiative suit les recommandations du groupe de travail créé par la loi de l'État de Washington de mars 1998.

Enfin, signalons l'originalité du projet de loi fédéral H.R. 2368 qui optait plutôt pour la rédaction d'un code de conduite volontaire par un groupe de travail. Une fois adopté, le code de conduite ne devait s'appliquer qu'aux fournisseurs d'accès Internet et aux personnes ayant accepté le code de conduite par leur enregistrement dans un registre déterminé par le groupe de travail. Les FAI et personnes enregistrées pouvaient ainsi bénéficier d'un logo représentant leur adhésion au code de conduite. Le projet de loi prévoyait également la création d'une procédure d'arbitrage pour les conflits survenant entre les FAI et les personnes régis par le code. Notons toutefois que les règles érigées par le groupe de travail devaient contenir l'obligation, pour les expéditeurs, d'identifier leurs noms et coordonnées et de permettre, par l'inscription d'une notification, la possibilité de refuser tout courrier électronique commercial selon un système conçu par le groupe de travail.

Les choix offerts au législateur américains sont donc nombreux. Si la tendance se maintient, le 106^{e} Congrès devrait toutefois orienter sa décision vers une approche du droit de propriété. Le succès de la loi californienne et les récentes recommandations émanant du *Commercial Electronic Messages Select Task Force* (État de Washington) correspondent de plus en plus aux prescriptions des principaux protagonistes du réseau.

Partie II - Les prescriptions des acteurs du réseau

À l'ombre d'une perception positive du droit, s'affrontent ou se complètent les prescriptions d'une multitude d'acteurs légitimés par leur pouvoir technique, politique et étatique. Ces voies de solution aspirent à guérir les maux d'un environnement hétérogène et intransitif.

Préférant l'élaboration de règles de conduite aux solutions techniques, certains protagonistes manifestent leur autorité et accusent un pouvoir de prédétermination. Ils s'exercent à signifier une interdiction du *spamming*. D'autres choisissent une démarche technique susceptible d'affecter le comportement des détracteurs du réseau. La nature des différentes prescriptions et la pluralité des autorités témoignent de l'exercice d'un pouvoir diffus (chapitre I).

La diffusion du pouvoir suppose un bas degré de prévisibilité de la solution autoréglementaire (chapitre II). En effet, l'analyse systémale révèle la présence d'un marché de règles rendant difficile tout contrôle hiérarchique du décodage des normes sur les ressources décentralisées d'Internet. La concurrence de règles et de valeurs a pour conséquence une diminution du caractère obligatoire de l'autoréglementation mais permet d'entrevoir une solution normative en accord avec les besoins de « souplesse » du Cyberespace.

Chapitre I - L'exercice d'un pouvoir diffus

L'exercice des pouvoirs technique et politique n'a pas comme seule expression la production de normes, il engendre aussi la proposition de logiciels de filtrage et de systèmes d'épuration en réseau. En terre nouvelle, la technique concurrence donc la normativité.

À l'origine du continuum normatif se situe le fait. S'intéressant aux mécanismes de production du droit, la présente étude considère les faits comme des facteurs potentiels de l'émergence d'une norme. En conséquence, elle se préoccupe de cette réalité moins neutre de l'effet normatif sur les comportements. Ce concept permet d'établir, au regard de l'engendrement du droit, une distinction utile entre les facteurs d'émergence et les discours ou comportements descriptifs ou prescriptifs. En cela, ce concept évite toute analyse systémale des moyens techniques de contrôle du *spamming*, de ces faits, environnements et circonstances susceptibles d'influencer le comportement des internautes. Seul ce comportement, à titre de norme implicite, pourrait être étudié à cet égard.

Suivant cette distinction préliminaire (section I), nous poursuivrons avec une synthèse des stratégies normatives appliquées par les principaux protagonistes ayant manifesté leur pouvoir par l'élaboration de règles (section II).

Section I - L'effet normatif sur les comportements

Un comportement généralisé ne se justifie pas seulement par l'élaboration d'un discours normatif. En effet, les lois ne bénéficient pas du monopole de l'effet normatif. Il existe des circonstances, des environnements et des faits susceptibles d'engendrer un résultat de même nature. Les comportements généralisés qui ne répondent pas aux exigences d'un discours ont traditionnellement été qualifiés d'usages ou de coutumes. Pierre Trudel expose la différence entre ces concepts :

> Les normes n'équivalent pas nécessairement aux usages. Ce sont, d'abord et avant tout, des normes qui expriment des commandements, tandis que les usages sont des actions répétées pendant un certain temps ne se révélant, en fin de compte, que par l'observation ou l'habitude.[130]

L'observation de comportements généralisés suppose donc une distinction non pas entre le résultat constaté (un effet normatif) mais entre les principaux facteurs à l'origine de ce résultat (une norme ou des circonstances, lieux et faits). Cette considération conduit à différencier les éléments du processus normatif de l'effet normatif sur le comportement. Elle nous amène également à l'étude de ces éléments qui n'entrent pas dans la catégorie du discours normatif.

À cet égard, les sciences humaines admettent, depuis les recherches de Pavlov, que l'environnement influence l'apprentissage des comportements, que la conduite humaine ne s'explique pas que par le choix délibéré des individus ou, plus subtilement, par les mécanismes de la psychologie profonde.

L'étude de l'émergence des normes, particulièrement dans le Cyberespace, révèle un penchant intéressant de la théorie du droit vers le béhaviorisme. Les environnements électroniques forgent, par les choix techniques et les avancées technologiques, des comportements spécifiques au détriment de conduites physiquement impraticables. En d'autres termes, l'apprentissage de l'utilisation des ressources Internet, de ses possibilités et limites, emporte un effet normatif. Autorisant l'envoi de pollupostage, le fonctionnement de la ressource télématique Usenet constitue un stimulus pour les polluposteurs. Dans une perspective différente, une solution technique contrant systématiquement les multipostages abusifs, une sorte de bouclier contre les comportements abusifs, constituerait un neutralisant parfait : l'absence totale de résultats et de profits pour les polluposteurs.

---

[130] P. TRUDEL, *loc. cit.*, note 1, 277.

Mais reste à déterminer le caractère véritablement normatif d'un tel bouclier. Il peut s'agir d'une solution technique résultant d'une règle implicite ou simplement d'un environnement comportant un impact normatif sur le comportement des internautes. Dans ce dernier cas, l'effectivité doit être constante. En effet, il demeure impensable qu'une solution technique puisse être contraignante en elle-même, qu'elle suffise à exercer une force contre la volonté des tiers. Cette solution nécessite également une effectivité permanente, un stimulus continu et systématique. Dans la mesure où l'effectivité s'avère variable, la présence d'un impact normatif ne s'explique que par le partage d'intérêts et de valeurs ou, selon une analyse plus économique, par l'absence de bénéfices à laquelle aboutirait toute tentative de contourner la solution technique[131].

L'existence de logiciels de filtrage et de systèmes d'épuration en réseau destinés à enrayer le *spamming* impose, après lecture de ces commentaires, une présentation générale de l'impact normatif de la technologie. Cette démarche permettra, dans un premier temps, de préciser les relations qu'entretient ce phénomène avec le processus normatif (sous-section I). Dans un deuxième temps, il sera fait état de ces solutions techniques sous une perspective de normativité (sous-section II).

Sous-section I - L'impact normatif de la technologie

Le professeur Reidenberg offre, par sa conception de la *Lex Informatica*, la plus intéressante approche de l'effet normatif de la technologie dans le Cyberespace. Celui-ci est d'avis que :

> [...] *the set of rules for information flows imposed by technology and communication networks form a "Lex Informatica" that*

[131] L'absence d'intérêt pourrait s'expliquer par l'abondance de la ressource protégée par les mesures de sécurité.

> *policymakers must understand, consciously recognize, and encourage.* [132]

Selon lui, la *Lex Informatica* se distingue de la réglementation étatique sous plusieurs aspects : la structure du régime, la juridiction, le contenu, les règles supplétives et leur élaboration, les sources ainsi que le mode d'exécution principal.

De la sorte, Reidenberg expose que cet autre ordre normatif a pour cadre et structure les protocoles et autres standards composant l'architecture du réseau, lequel constitue sa juridiction. Son contenu normatif est formé de règles figées par des standards technologiques inaltérables et de règles flexibles permises par la personnalisation d'environnements plus souples, ces dernières se présentant comme les normes supplétives de ce régime. Reposant sur les choix techniques, les règles de la *Lex Informatica* sont appliquées automatiquement par la personnalisation des programmes informatiques[133].

Par l'emploi du terme *Lex Informatica*, le professeur Reidenberg offre un nouveau sens dérivé du concept de la *Lex Mercatoria*. S'inspirant de la loi marchande médiévale, il dresse un parallèle entre la nécessité de règles non étatiques pour pallier aux besoins des relations économiques internationales et la présence de normes imposées par la structure du réseau Internet.

Cette analogie procède toutefois d'une démarche pragmatique. Ce n'est que pour mieux illustrer son idée que Reidenberg l'emploie. En effet, les deux corpus ont des sources passablement différentes. Rappelons que la loi marchande médiévale consistait en une normativité souple puisant ses origines dans la pratique répétée d'actes commerciaux que la doctrine qualifie d'usages ou de coutumes[134]. Or, la *Lex Informatica* se définit

---

[132] Joel REIDENBERG, « *Lex Informatica* : The Formulation of Information Policy Rules Throught Technology », (1998) 76 *Tex. L. Rev.*. 553, 554.

[133] *Id.*, 554 et s.

[134] Voir : Vincent GAUTRAIS, Guy LEFEBVRE et Karim BENYEKHLEF, *loc. cit.*, note 82, 550 et s.

comme un corps de règles rigides reposant sur la programmation effectuée par des informaticiens, une construction technologique imposant des choix quant à l'accès à l'information et à son utilisation.

Cette remarque dévoile une précision importante sur la nature de l'impact normatif de la technologie. L'existence d'un continuum de normativité et l'absence d'une distinction nette entre la normativité et le « fait normatif » ne conduisent pas à capharnaüm théorique. La norme porte en elle une signification et une contrainte alors que le « fait normatif » contribue à la formation de comportements généralisés. Rien de l'architecture du réseau, de ses protocoles ou des logiciels de filtrage ne révèle une intention, même implicite, de signifier à autrui une habilitation, une permission ou bien une interdiction. Ces considérations matérielles ne façonnent que des obstacles qui, à l'occasion, requièrent des internautes une utilisation précise d'Internet. En somme, elles ne constituent ni un discours ni un comportement descriptif ou prescriptif. Seul le comportement généralisé qui en résulte est susceptible de posséder les qualités d'une norme.

Cette observation conduit à une deuxième remarque. En octroyant une nature normative à la personnalisation des programmes informatiques utilisés sur le réseau, les propos de Reidenberg ont pour résultat d'assimiler la mise en œuvre d'une solution technique à une norme supplétive.

Se rapportant à la liberté contractuelle, la norme supplétive peut se définir comme une règle complémentaire à un ensemble de règles obligatoires auxquelles les destinataires ont la possibilité de déroger. Lorsque deux parties se prévalent de leur liberté contractuelle en adoptant une règle particulière, ils participent à l'élaboration - l'encodage - d'une règle porteuse d'une permission, d'une obligation ou d'une habilitation. Rien de l'entente n'est conclu sans l'assentiment des deux contractants.

Occasionnant l'assimilation de la personnalisation de programmes informatiques à des *customized rules*, l'analogie entre le droit étatique et la *Lex Informatica* octroie une nature normative à des considérations matérielles. Pour étayer ses propos, le professeur Reidenberg mentionne l'enregistrement, par certains fureteurs, des données personnelles de navigation. Cette faculté offre à l'administrateur l'opportunité de consulter les données privées des visiteurs des sites dont il a la gestion. Toutefois, ces informations sont susceptibles, par la personnalisation du logiciel client, d'être modifiées ou tout simplement supprimées. En optant pour cette alternative, l'usager réduit les chances que ses données personnelles soient utilisées par des tiers. Il ne tente pas de signifier un refus mais empêche, par voie technique, l'appropriation d'informations confidentielles. En somme, la mise en œuvre d'un système de sécurité, bien que très efficace, échappe à la définition d'une norme.

Cependant, l'acte unilatéral que représente cette mise en pratique peut comporter une signification implicite, une interdiction sous-entendue mais bien réelle. Dans ce cas, il faut admettre l'existence d'une prédétermination formulée autrement que par un écrit. Néanmoins, cette prédétermination ne doit pas résulter d'une confusion entre l'intention de se prémunir contre les abus de tiers et la personnalisation effective de l'usager.

En effet, la personnalisation apparaît comme le véhicule coercitif d'une intention personnelle. La décision de modifier ou de supprimer les informations de navigation s'explique par la volonté d'assurer leur nature privée mais n'équivaut pas à l'élaboration d'une norme.

À cet égard, la *Lex Informatica* se caractérise par l'application automatique des choix techniques exercés par les usagers. Par exemple, la personnalisation d'un logiciel de vérification d'identité dont l'objet est d'assurer la sécurité des transactions peut être tenue à la fois pour une règle personnalisée et pour son mode d'exécution[135]. La même

[135] Le logiciel permet à la fois de choisir son cocontractant et de refuser toute personne ne possédant pas l'autorisation requise.

considération vaut quant à la mise hors fonction de l'option d'enregistrement des données relatives à la navigation[136].

Se rapportant aux moyens mis en œuvre pour protéger les intérêts des usagers, la personnalisation présente les attributs d'un « fait normatif ». En cela, elle se situe dans l'ombre du droit, plus près de l'effectivité que de la signification.

Toutefois, l'intention personnelle associée à la configuration d'un logiciel équivaut peut-être à une prédétermination implicite. Puisque la signification d'une norme est également le produit de la codétermination et de la surdétermination, la personnalisation est susceptible de révéler une norme implicite que les destinataires pourront interpréter et appliquer.

Cependant, cette hypothèse fond dans l'ignorance de cette prédétermination. En effet, les solutions techniques actuelles visant à enrayer le *spamming* n'ont l'avantage ni d'indiquer, même implicitement, la volonté des internautes d'interdire le *spamming* ni même de comporter une interdiction en soi. À défaut d'observer un véritable comportement généralisé, la méconnaissance d'une intention personnelle implicite ne permet pas de conclure à l'existence d'une norme, au sens de la définition que nous lui avons donné.

Sous-section II - Les solutions techniques envisagées

Parmi les moyens techniques proposés pour solutionner le pollupostage (A), le pourriel (B), et le référencement abusif (C), aucune n'est satisfaisante sans l'obtention d'un large consensus. Seules quelques unes entendent régler le problème à sa source.

[136] L'option d'enregistrement permet de préserver le caractère privé des informations mais aussi de les rendre inaccessibles à chaque fois qu'un administrateur tente de se les approprier.

A. Le pollupostage

Puisque le pollupostage a été la première activité qualifiée de *spamming*, les remèdes techniques ont d'abord cherché à épurer les groupes discussion des milliers de messages commerciaux postés chaque jour. La suppression automatique des messages expédiés par un tiers à l'aide d'un robot d'annulation (cancelboots) a été la première solution technique visant à enrayer le *spamming* sur la ressource Usenet. Cette dernière est généralement acceptée par les administrateurs de serveurs Usenet. Toutefois, elle pose certains problèmes. Elle requiert d'abord une parfaite maîtrise des paramètres de programmation d'un tel robot, une erreur pouvant engendrer l'annulation de messages non abusifs ou la multiplication de messages d'annulation. Elle suppose également une application stricte des raisons pour lesquelles un message peut être supprimé sans l'autorisation de son auteur et donc, une programmation capable de discerner le postage d'un pollupostage.

Sensible à ces difficultés, le légendaire suppresseur de pollupostage *Cancelmoose*^{TM} a proposé un logiciel destiné à remplacer l'annulation de messages[137]. L'objectif de ce logiciel baptisé NoCeM (lire « *no see them* ») est de communiquer aux autres utilisateurs l'existence de pollupostages. Suite à la réception de messages dénonciateurs, l'utilisateur de NoCeM a la possibilité de filtrer les multipostages abusifs. Bien qu'il ne puisse vérifier toutes les dénonciations qu'il reçoit, l'utilisateur peut prévoir l'acceptation automatique de celles provenant d'une personne de confiance. À cette fin, les messages envoyés par ce logiciel doivent être signés avec la clef privée de l'expéditeur.

La solution que propose NoCeM risque toutefois de constituer un moyen de censure s'il est mal utilisé par les opérateurs de serveurs qui sont les principaux clients visés par le concepteur[138].

---

[137] J. D. FALK et S. SOUTHWICK, note 34.

[138] ANONYME, «NoCeM FAQ. VO. 93», http://www.cm.org/faq.html.

B. Le pourriel

Une version de NoCeM a également été créée pour venir en aide aux administrateurs désireux de filtrer le courrier électronique non sollicité[139]. Celle-ci, plutôt que d'opérer par courriers électroniques chiffrés, détient ses informations de filtrage d'une liste de distribution choisie selon les critères de triage souhaités par l'administrateur.

Plusieurs logiciels de filtrage permettent aussi aux utilisateurs de filtrer leur boîte de courriers électroniques. La plupart de ces logiciels épurent les messages reçus en classant les pourriels dans le répertoire poubelle du logiciel de courrier électronique. Certains d'entre eux offrent à l'utilisateur le choix de ses propres critères de sélection et les actions effectuées lors du triage des courriers. Toutefois, l'utilité de ces logiciels ne fait pas l'unanimité. S'ils parviennent à sauver quelques minutes de triage à l'usager, les logiciels de filtrage ne parviennent pas à empêcher le transfert des coûts publicitaires aux destinataires.

Le système d'épuration en réseau de la compagnie *Bright Mail Technologies*[140] éviterait ce transfert en effectuant l'opération de filtrage par les serveurs SMTP des destinataires, avant la réception des courriers. Ce système profite d'un logiciel de filtrage mis à jour continuellement par un centre d'opération destiné à analyser et identifier les pourriels. Ravitaillé de courriers électroniques par son propre réseau d'exploration, le centre d'opération dispose de ressources humaines empêchant la censure des courriers électroniques acceptables. L'efficacité du réseau d'exploration est assurée par la création d'adresses électroniques fictives chez d'importants fournisseurs d'accès Internet dont AT&T WorldNet, Concentric Network, Earthlink et USA.NET.

---

[139] Voir : *Net Abuse Links* , http://www.novia.net/~doumakes/abuse/.

[140] *Bright Mail Technologies* : http://www.brightlight.com/.

Également, le système *Bright Light* prévoit d'offrir aux destinataires le choix entre différentes catégories de publicités qu'ils désirent recevoir en transmettant des instructions spécifiques au logiciel de filtrage de leur fournisseur d'accès Internet. Notons cependant que cette solution est payante et que les frais déboursés par les FAI seront probablement supportés par les usagers.

Malgré cela, le système d'épuration en réseau proposé par *Bright Light Technologies* répond aux attentes particulières des fournisseurs d'accès Internet. Cette solution rend possible une opération de filtrage minutieuse et, par conséquent, juridiquement moins risquée. À l'opposé, la pratique téméraire de retourner tout courrier électronique à son destinateur lorsque celui-ci est un polluposteur reconnu pose des difficultés reliées à la censure des courriers électroniques légitimes. Le *Mail Abuse Prevention System Realtime Blackhole List* (MAPS-RBL) en constitue le meilleur exemple[141]. Cette organisation rassemble les plaintes d'internautes reliées au *spamming* et compile dans une liste (RBL) les adresses IP retrouvées dans le code source des pourriels rapportés. Continuellement mise à jour, cette liste est disponible sur le serveur de l'organisation (MAPS) et peut être utilisée par un administrateur de serveur SMTP pour filtrer le courrier électronique. Toutefois, l'identification de l'adresse IP du destinataire comme seul critère de filtrage rend impossible la détermination précise des véritables pourriels et expose l'administrateur à l'insatisfaction de ses propres usagers, dès lors limités dans leurs échanges.

Plus que de tenter de réfréner le courrier électronique non sollicité, les divers acteurs d'Internet ont jugé souhaitable de tuer le *spamming* dans l'œuf et ont proposé quelques mesures préventives. Les usagers sont donc invités à utiliser leur adresse de courrier électronique avec diligence. Par exemple, ils doivent éviter de diffuser leur courriel sur un site Web et de le transmettre à la demande. On recommande également d'ajouter l'annotation *no-spam* au nom de domaine de leurs adresses électroniques. Bien intentionnées, ces mesures préventives viennent toutefois limiter l'usager dans l'exercice

[141] *Mail Abuse Prevention System Realtime Blackhole List* : http://maps.vix.com/rbl/.

de ses activités cybernétiques. Il n'est pas certain que cette entrave doive effectivement retomber sur les victimes du *spamming*. Toute balise posée à cet exercice devrait plutôt être supportée par les expéditeurs de courriers électroniques non sollicités.

C. Le référencement abusif auprès des outils de recherche

Contrairement au courrier électronique et aux groupes de discussion, la question de la censure ne s'est pas présentée quant au contrôle du référencement abusif auprès des outils de recherche. S'agissant d'une entreprise de services privés établie sur un serveur HTTP, un outil de recherche est moins susceptible d'être taxé de censeur. En effet, ses services ne dépendent pas d'autres serveurs décentralisés pouvant être gênés par les mesures techniques entreprises pour enrayer le référencement abusif. Cependant, la programmation des moteurs de recherche risque de disqualifier certains sites ne pratiquant aucune technique subversive de référencement. Pour ces raisons, les outils de recherche nivellent généralement leurs critères par le bas. Par exemple, un site contenant plus de sept mots identiques est automatiquement déclassé par le moteur de recherche d'Infoseek, laissant une marge de manœuvre assez large aux Webmestres.

Jusqu'à récemment, les solutions de contrôle du *engine spamming* ne tenaient pas compte des activités déloyales pratiquées par certains compétiteurs. Ces derniers profitaient de la nouvelle programmation des moteurs de recherche pour tenter de déclasser leurs concurrents. La stratégie consistait à référencer les pages du site de la victime une multitude de fois sous les mêmes mots-clefs. L'outil de recherche Infoseek semble avoir résolu ce problème en rassemblant, sous un seul résultat de recherche, les pages hébergées sur un même serveur[142].

Pour conclure cette sous-section, il faut admettre que les solutions techniques envisagées pour contrevenir aux manifestations du *spamming* témoignent d'une interminable et

---

[142] Lori PIQUET, *loc. cit.*, note 93.

silencieuse guérilla numérique. À l'exception de quelques reproches ponctuels d'internautes contrariés, les stratégies techniques de prévention autant que les logiciels et réseaux de filtrage n'ont guère l'avantage de signifier à autrui une interdiction.

Dans la méconnaissance d'une prédétermination implicite, les efforts technologiques sont susceptibles de ne générer que des retombées normatives sur le comportement des internautes. En ce sens, la technique correspond plus à une sanction démunie de toute norme qui l'aurait précédée : l'inattendue et surprenante guillotine.

En parallèle à cet échafaudage technologique, certaines autorités ont manifesté, par la composition de textes normatifs, leur position sur les activités reliées au *spamming*.

Section II - Les normes postulées : l'opération de prédétermination

Bien que d'origine et de qualité différentes, les nombreuses normes élaborées à l'égard du *spamming* tendent fondamentalement à proscrire les comportements abusifs. La quasi-généralisation de cette proscription contribue à donner aux solutions techniques un antécédent normatif, un texte qui aurait signifié une interdiction, même si plusieurs de ces solutions n'en n'ont jamais reçu des usagers qui les utilisent.

En vue de déterminer le caractère obligatoire de la solution autoréglementaire du *spamming*, il importe de révéler comment, à travers les textes normatifs, les différents protagonistes ont manifesté leur volonté d'interdire cette activité. Il est également nécessaire de dévoiler la manière dont ils entendent contrôler l'interprétation et l'application de leurs règles.

La présente section aborde donc l'opération de prédétermination de ces normes en concurrence et expose les stratégies normatives des différents « candidats ». La prédétermination se présente comme une opération permettant à l'auteur d'une norme d'indiquer le degré de discrétion qu'il se réserve quant aux conditions d'application de

cette norme et au champ de compétence qu'elle vise[143]. En d'autres termes, il s'agit de s'intéresser à la manière dont l'auteur de la norme s'assure que le texte exprime exactement sa volonté quant au contenu de la règle (conditions d'application) et qu'il indique clairement, à l'intérieur du système normatif, la place hiérarchique de l'auteur et de la règle édictée (champ de compétence).

Gérard Timsit résume cette explication en définissant la prédétermination comme une « inscription du sujet dans le texte[144] » à titre de substance (conditions d'application) et de puissance (champ de compétence). Par sujet, il se réfère à l'auteur de la norme, de la loi : son Créateur. L'inscription du sujet correspond donc aux stratégies normatives « [...] par lesquelles le sujet *manifeste* son existence, autorité et volonté, puissance et substance[145] ». Conformément à « ces deux espèces essentielles du sujet », il sera fait état des stratégies normatives que les acteurs du réseau emploient pour préciser le contenu de la règle (sous-section I) et le champ de compétence qu'elle vise (sous-section II).

Sous-section I - L'inscription de la substance

Des deux manifestations déterminantes de l'autorité, seuls les textes normatifs dépendent de l'aptitude des protagonistes à indiquer distinctement leur intention de proscrire les comportements abusifs. Par conséquent, la qualité des stratégies normatives repose sur l'habileté respective des propriétaires de ressources (A), des « communautés, de leurs représentants et des internautes » (B) ainsi que de l'État (C).

---

[143] A. LAJOIE, *loc. cit.*, note 26.

[144] G. TIMSIT, *op. cit.*, note 5, p. 73.

[145] *Id.*, p. 77.

A. Les stratégies des propriétaires de ressources

Parmi les propriétaires de ressources se retrouvent les fournisseurs d'accès Internet (1) et les entreprises opérant un outil de recherche (2).

1. Les fournisseurs d'accès Internet

C'est généralement en choisissant des termes simples que les fournisseurs d'accès Internet réussissent à préciser le contenu de leur code de conduite. En effet, ils s'appliquent à « [...] choisir des concepts dont la signification est acquise et ne donne lieu à aucune ambiguïté ou au moins d'ambiguïtés possibles[146] ». Timsit emploie le terme « reproduction » pour nommer cette première stratégie normative par laquelle l'auteur « reproduit » des mots qui ont déjà une signification consacrée.

À ce titre, le FAI canadien Sympatico édicte, dans son code de conduite, une interdiction du *spamming* en prohibant à ses usagers la transmission de messages électroniques non sollicités à caractère commercial ou l'entreprise de publipostages de masse. De cette manière, il désire réduire l'équivoque susceptible d'être produite par l'utilisation du terme *spamming*. Par ailleurs, ils préfèrent interdire l'affichage, sur les groupes de discussion, de messages publicitaires ou à caractère commercial sans avoir recours à cette expression lourde de signification. Les fournisseurs américains AT&T, MCI et Compuserve prennent le même soin :

> AT&T
>
> *You may not post or list articles which are off-topic according to the description of the group or list or send unsolicited mass emailings to 10 people if such e-mail could reasonably be expected to provoke complaints from its recipients.*[147]

---

[146] *Id.*, p. 80.

[147] *AT&T Web Site Agreement* : http://www.att.com/terms.html#exhibit-a.

MCI

> [...] - *To send unsolicited e-mailings to more than twenty-five (25) e-mail users, if such unsolicited e-mailings could reasonably be expected to provoke complaints.*[148]

Compuserve

> *Member agrees not to upload, post or otherwise publish on or over the Service, and not to seek on or over the Service, any software, file, information, communication or other content:*
> [...]*(f) which, without the approval of CompuServe, contains any advertising, promotion or solicitation of goods or services for commercial purposes. This paragraph shall not be interpreted to restrict Member from utilizing mail services in conducting a legitimate business except that Member may not, without the approval of CompuServe, send unsolicited advertising or promotional material.*[149]

D'autres FAI se servent de cette technique normative afin de condamner le *spamming*, ce qui, dans bien des cas, a pour effet de préciser le sens de cette expression. Voici quelques exemples révélateurs :

Netcom

> *Prohibited transmissions include without limitation, viruses, trojan horse programs,* [...], *postings to a newsgroup in violation of its rules, charter or FAQ, unsolicited advertising (whether commercial or informational) and unsolicited e-mail ("SPAM"). Netcom strongly opposes SPAM, which floods the Internet with unwanted and unsolicited e-mail and deteriorates the performance and availability of the Netcom network. All forms of SPAM, and all activities that have the effect of facilitating SPAM, are strictly prohibited.*[150]

---

[148] MCI WorldCom Spamming Policy : http://www.wcom.com/legal/spamming/.

[149] *CompuServe's US and Canada Member Agreement Terms* : http://support.csi.com/cshelp%5Fdocs/sr052.htm.

[150] *Acceptable Use Guidelines for Netcom Services* : http://www.netcom.com/netcom/aug.html.

IBM

- Sending unsolicited bulk mail messages ("junk mail" or "spam") which, in IBM's sole judgment, is disruptive or generates a significant numberof user complaints. This includes bulk-mailing of commercial advertising, informational announcements and political tracts.
[...] - Posting the same or similar messages to large numbers of newsgroups (excessive cross-posting or multiple-posting, also known as "USENET spam").[151]

Digex

Sending unsolicited mail messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material ("e-mail spam"). Customers are explicitly prohibited from sending unsolicited bulk mail messages. This includes, but is not limited to, bulk-mailing of commercial advertising, informational announcements, and political tracts.[152]

La seule application de cette stratégie n'apparaît pourtant pas satisfaisante. Timsit souligne que la doctrine du sens clair n'est qu'une tentative de faire croire à l'univocité des mots[153]. Il remarque que les mots n'offrent jamais de certitude absolue quant au sens qui peut leur être conféré[154]. Toutefois, cette incertitude peut être réduite par l'emploi simultané de plusieurs techniques normatives. Suivant cette stratégie, plusieurs FAI ont su tirer profit de la méthode dite de « déduction ». Celle-ci consiste à adapter les solutions que le texte normatif ne « [...] prévoit pas explicitement mais qu'entraîne nécessairement la simple application des règles de déduction[155] ». L'énumération non limitative d'activités prohibées par le code de conduite du FAI Pacific Bell présente une excellente illustration :

---

[151] *IBM Service Terms* : http://www.ibm.net/terms/index.html.

[152] *Digex Incorporated Acceptable Use Policy* : http://www.access.digex.net/~policy/digex-aup.html.

[153] G. TIMSIT, *op. cit.*, note 5, p. 81.

[154] *Id.*

[155] *Id.*, p. 84.

> *You may not use your account to send unsolicited bulk or commercial messages ("spam")* **[reproduction]**. *This includes, but is not limited to, bulk mailing of commercial advertising, informational announcements, charity requests, petitions for signatures, and political or religious tracts* **[déduction]**. *Such messages may only be sent to those who have explicitly requested it.*

La technique de « déduction » s'oppose à la « réduction partielle », un troisième procédé visant à exclure implicitement d'autres significations par l'inventaire des hypothèses retenues. Régulièrement pratiquée par les législateurs, cette stratégie normative ne semble pas avoir été appliquée par les FAI. Cet état de fait résulte probablement de la volonté des FAI d'interdire toute forme de *spamming* en se réservant le droit d'inclure à leurs listes des abus de même nature.

Au regard de cette intention, la technique dite de « réduction globale » apparaît plus appropriée. S'agissant d'une codification exigeante des nombreux sens donnés au *spamming*, elle implique cependant un alourdissement du contenu des règles des FAI et leur impose un exercice continu de rédaction.

À l'instar de la « reproduction », la « déduction », la « réduction » ou la combinaison de ces techniques ne sont d'aucune rigueur absolue et risquent de laisser des marges d'incertitude[156]. L'auteur peut toutefois diminuer cette latitude par l'emploi de la technique du multicodage. Cette dernière stratégie consiste à référer le lecteur au contexte[157].

Selon le professeur Timsit, le contexte représente à l'étape de la prédétermination, les références expresses ou les liens matériels du texte avec les « [...] préambules, annexes, visas, renvois explicites à des dispositions d'autres textes, intégration[s] du texte à un

---

[156] *Id.*, p. 85.

[157] *Id.*, p. 87.

ensemble législatif ou réglementaire ayant statut de code (au sens juridique du terme), etc.[158] ». Ce terme apparaît donc différent du concept de « conjoncture » qui fait référence aux contextes culturel, économique, politique et social[159]. En conséquence, cette expression ne se rapporte pas aux ressources Internet, aux contextes électroniques, mais bien aux interrelations du texte : « [l]es clauses s'interprètent les unes par les autres, en donnant à chacune le sens qui résulte de l'ensemble du contrat[160] ».

Le contexte réfère le lecteur à un second sens de la norme susceptible de confirmer, lorsque se pose une ambiguïté, celui du texte original[161].

Les codes de conduite des FAI ne comportent pas ou peu de *manifestations* du contexte. Les interdictions du *spamming* ne sont souvent que des règles parties d'une liste d'usages prohibés ne renvoyant, ni objectivement ni expressément, à d'autres textes. Seule la nature abusive des usages qui y sont cités permettrait, par la recherche de l'esprit du texte, de soustraire une ambiguïté. Mais ce serait là ouvrir la porte à la codétermination, voire à l'interprétation, et oublier que la prédétermination est inscription du Sujet dans le texte[162].

2. Les entreprises opérant un outil de recherche

Les normes élaborées par les entreprises opérant un outil de recherche dévoilent des stratégies normatives quasi identiques à celles des prestataires de services Internet.

---

[158] *Id.*

[159] A. LAJOIE, R. A. MACDONALD, R. JANDA et G. ROCHER, *op. cit.*, note 6, pp. 244-245. Nous constaterons plus tard que le concept de conjoncture est lié à celui de surdétermination bien que Gérard Timsit est d'avis qu'il déborde le cadre et les limites de l'analyse systémale (p. 101).

[160] *Code civil du Québec*, art. 1427.

[161] G. TIMSIT, *op. cit.*, note 5, p. 87.

[162] À ce titre, le professeur Timsit indique qu' « [i]l ne saurait être question d'y faire intervenir des considérations qui ne découleraient pas de l'existence d'un texte, et que l'on tirerait, par exemple, de l' « esprit » de la loi ou de la volonté présumée du législateur [...] ». G. TIMSIT, *op. cit.*, note 5, p. 86.

L'utilisation caractérisée des techniques de « reproduction » et de « déduction » confirme la volonté d'indiquer précisément aux destinataires les activités prohibées sans toutefois limiter irrémédiablement la portée de l'interdiction. En effet, ces protagonistes ont cherché à interdire le *spamdexing* par l'emploi de termes simples sans toutefois énumérer l'ensemble des procédés qui tomberaient dans le champ de cette activité. L'outil de recherche Infoseek exprime ainsi sa volonté :

> *Spamming is the alteration or creation of a document with intent to deceive an electronic catalog or filing system* **[reproduction]**. *[...] Infoseek's index detects common spamming practices and penalizes pages that use them. Unfortunately, in some cases this may cause valid pages to be penalized as well. For best results, the following Web publishing techniques should be avoided:*
>
> - *Overuse or repetition of keywords*
> - *Use of keywords that do not relate to the content of the site*
> - *Use of fast meta refresh*
> - *Use of colored text on same-color background*
> - *Duplication of pages with different URLs*
> - *Use of different pages that bridge to the same URL*
>
> *Please note these are only a few examples of what is considered spamming* **[déduction]**. *There are many more types that are not illustrated and will not be permitted on Infoseek's index.*

Rendue nécessaire par la nouveauté de l'expression *spamming* pour désigner le référencement abusif auprès des outils de recherche, la « reproduction » appliquée par les opérateurs s'est révélée d'une grande utilité. D'une manière complémentaire, on a voulu garantir, par la technique de « déduction », une souplesse du texte et s'assurer que d'autres pratiques subversives entreraient ultérieurement dans le champ de l'interdiction. Enfin, aucune *manifestations* du contexte n'a été remarquée, une décision stratégique pouvant occasionner certaines déviations du sens de l'interdiction.

B. Les stratégies des « communautés » : leurs représentants et les internautes

Ayant comme premier objectif de dissuader toute forme de *spamming*, les textes rédigés par les internautes de la Vieille Garde et les différents « représentants » ont pour mérite de s'imbriquer les uns dans les autres, témoignant une utilisation marquée du multicodage. Cette importance accordée au contexte révèle l'existence de rapports étroits entre plusieurs internautes de même acabit. Par l'emploi de liens hypertextes, ces protagonistes offrent une nouvelle application de cette stratégie normative.

Par exemple, les lacunes du *Net abuse FAQ* pourront être comblées suite à l'emprunt de liens vers des documents plus précis. Ainsi, la méthode employée pour qualifier un article de pollupostage, le *Breidbart Index*, est explicitée par le document *Current Usenet spam thresholds and guidelines FAQ* auquel se rapporte le *Net abuse FAQ*[163].

La ferme intention des « représentants » de proscrire les comportements abusifs se traduit par des explications complètes et nuancées. Toutefois, la présence de détails impertinents et la redondance des textes rendent équivoques certaines définitions et minent la clarté de ce qui se voulait précis et exhaustif. Par exemple, le paragraphe suivant laisse entendre que le nombre de 20 articles postés sur Usenet n'est qu'un indice approximatif de la présence d'un pollupostage :

> *Among those who agree that spam should be defined solely by quantity, 20 appears to be the magic number, or at least a number so middle-of-the-road that it provokes very little passionate dissent in either direction. Notably, Cancelmoose[tm] refused to set a firm number, in the belief that people would simply post [X-1] messages. It's safe to say that a couple incidents of 19-post spams would cause the magic number to plummet. Thus, 20 should be considered a vague approximation only.*

---

[163] Les textes suivants font référence les uns aux autres : *Current Usenet spam thresholds and guidelines FAQ, Net abuse FAQ,FAQ: Advertising on Usenet: How To Do It, How Not To Do It, A Primer on How to Work With the Usenet Community, Rules for posting to Usenet, Cancel Messages: Frequently Asked Questions, The Email Abuse FAQ, etc.* Voir : T. SKIRVIN, *loc. cit.*, note 111.

Pourtant, l'auteur de ces lignes renvoie à un autre document, qu'il prétend plus précis, indiquant le nombre 20 comme strict :

> *The thresholds for spam cancels are based only on one or more of the following measures:*
>
> *1. The BI is 20 or greater over a 45 day period.*
>
> *2. Is a continuation of a previous EMP/ECP, within a 45 day sliding window. That is: if the articles posted within the past 45 days exceeds a BI threshold of 20, it gets removed, unless the originator has made a clear and obvious effort to cease spamming (which includes an undertaking to do so posted in news.admin.net-abuse.misc). This includes "make money fast" schemes which passed the EMP/ECP thresholds several years ago. This author recommends one posting cross-posted to no more than 10 groups, no more often than once every two weeks (a BI of 3).*

Cette indétermination pourrait indiquer l'existence d'une distinction entre l'indice Breidbart pertinent pour la désignation d'un pollupostage et l'indice permettant son annulation. Dans ce cas, la référence au contexte aurait pour effet de créer un décalage entre la définition du pollupostage et les normes descriptives destinées à l'enrayer.

C. Les stratégies de l'État

Parmi les normes étudiées, les règles étatiques figurent au sommet de l'échelle de prédétermination. Pour des raisons essentiellement liées à leur habileté et à leur expérience de législateur, les différents États ont élaboré des normes d'une précision laissant peu de place aux indéterminations. L'inscription de définitions, l'apposition d'énumérations limitatives et l'emploi de mots précis en témoignent. Voici comment le législateur californien exprime sa volonté en définissant, au préalable, les termes qu'il utilisera pour signifier son interdiction :

17538.45. (a) For purposes of this section, the following words have the following meanings:

(1) "Electronic mail advertisement" means any electronic mail message, the principal purpose of which is to promote, directly or indirectly, the sale or other distribution of goods or services to the recipient.

(2) "Unsolicited electronic mail advertisement" means any electronic mail advertisement that meets both of the following requirements:

(A)It is addressed to a recipient with whom the initiator does not have an existing business or personal relationship.

(B) It is not sent at the request of or with the express consent of the recipient.

(3) "Electronic mail service provider" means any business or organization qualified to do business in California that provides registered users the ability to send or receive electronic mail through equipment located in this state and that is an intermediary in sending or receiving electronic mail.

(4) "Initiation" of an unsolicited electronic mail advertisement refers to the action by the initial sender of the electronic mail advertisement. It does not refer to the actions of any intervening electronic mail service provider that may handle or retransmit the electronic message.

(5) "Registered user" means any individual, corporation, or other entity that maintains an electronic mail address with an electronic mail service provider.[164]

Il continue en prohibant aux usagers et à toute entreprise l'emploi non autorisé de serveurs de courrier électronique situés en Californie :

(b) No registered user of an electronic mail service provider shall use or cause to be used that electronic mail service provider's equipment located in this state in violation of that electronic mail service provider's policy prohibiting or restricting the use of its service or equipment for the initiation of unsolicited electronic mail advertisements.

(c) No individual, corporation, or other entity shall use or cause to be used, by initiating an unsolicited electronic mail advertisement, an electronic mail service provider's equipment located in this state in violation of that electronic mail service

---

[164] *An act to amend Section 17511.1 of, and to add Section 17538.45 to, the Business and Professions Code, and to amend Section 502 of the Penal Code, relating to advertising*, précitée, note 13.

> *provider's policy prohibiting or restricting the use of its equipment to deliver unsolicited electronic mail advertisements to its registered users.*[165]

Cette loi indique la volonté de son auteur d'interdire, dans certaines conditions, l'une des manifestations du *spamming*. Pourtant, le texte ne fait aucune référence à cette expression. Le législateur californien a préféré se servir de termes comportant moins de connotations. Le système réglementaire *opt-out* de l'État de Washington adopte la même technique :

> *Sec. 2. The definitions in this section apply throughout this chapter unless the context clearly requires otherwise.*
>
> *(1) "Commercial electronic mail message" means an electronic mail message sent for the purpose of promoting real property, goods, or services for sale or lease.*
>
> *(2) "Electronic mail address" means a destination, commonly expressed as a string of characters, to which electronic mail may be sent or delivered.*
>
> *(3) "Initiate the transmission" refers to the action by the original sender of an electronic mail message, not to the action by any intervening interactive computer service that may handle or retransmit the message.*
>
> *(4)* [...][166]

Préférant l'approche du droit de propriété, le projet de loi HB 1037 de cet État précise ce que l'on doit entendre par courrier électronique commercial non sollicité :

> *(8) "Unsolicited commercial electronic mail message" means a commercial electronic mail message:*
> *(a) Sent without a recipient's prior consent;*
> *(b) Sent to a recipient with whom the sender does not have a preexisting and ongoing business or personal relationship; or*
> *(c) Sent for a purpose other than collecting an existing obligation.*[167]

---

[165] *An act to amend Section 17511.1 of, and to add Section 17538.45 to, the Business and Professions Code, and to amend Section 502 of the Penal Code, relating to advertising*, précitée, note 13.

[166] *Prohibited unsolicited electronic mail*, précitée, note 13.

[167] Washington House Bill 1037 (1999).

La précision des textes législatifs et l'application de stratégies normatives efficaces révèlent une opération de prédétermination très satisfaisante à l'égard du courrier électronique non sollicité, seule manifestation du *spamming* que les États ont cru bon de réglementer. Rappelons toutefois que les limites territoriales constituent un frein à l'application des lois et à la compétence de l'État.

Sous-section II - L'inscription de la puissance

Ce que Timsit nomme la « puissance du Sujet » réfère très certainement au champ de compétence de l'auteur. Si les stratégies normatives des législateurs s'avèrent plus que suffisantes, l'indication claire de leur compétence[168] dépend, à l'instar des autres acteurs, de l'ordre normatif en cause[169]. En effet, l'inscription de la puissance est un processus visant à indiquer au lecteur l'autorité de l'auteur de la norme et la place de cet auteur dans la hiérarchie à laquelle il appartient[170]. À ce sujet, Gérard Timsit pose la question suivante :

> [L]es manifestations objectives de la puissance du sujet permettent-elles de conclure à l'existence effective d'une - et une seule - hiérarchie continue et intégrale de l'ensemble des normes d'un ordre juridique déterminé ?[171]

---

[168] L'inscription de la puissance s'effectue par les « formes de l'actes », c'est-à-dire par les indications objectives que la norme est bien le fait d'un acteur, qu'un code de conduite ou une Foire Aux Question est bien le fait d'un FAI ou d'un administrateurs de systèmes. Voir : G. TIMSIT, *op. cit.*, note 5, p. 86.

[169] « On peut définir l'On [ordre normatif] comme un système de normes - des normes relatives à d'autres normes à l'édiction desquelles elles commandent : des archi-normes - : un système de normes définissant les modalités d'engendrement des normes et de leur articulation entre elles et les instances qui les engendrent » . G. TIMSIT, *op. cit.*, note 103, p. 96.

[170] G. TIMSIT, *op. cit.*, note 5, p. 90.

[171] *Id.*

L'inscription du Sujet comme puissance conduit donc à s'interroger sur les expressions du pouvoir de l'auteur. Se rapportant à l'existence d'une hiérarchie de normes, l'inscription de la puissance a pour principal corollaire le contrôle hiérarchique du décodage de la norme, c'est-à-dire le contrôle effectué par les différents organes chargés de cette tâche[172]. En effet, il ne peut exister de hiérarchie effective si aucune institution n'a le pouvoir de s'assurer que l'interprétation et l'application des règles s'effectuent selon la volonté de leur auteur.

Or, il faut admettre que les caractéristiques décentralisées et transnationales d'Internet posent de sérieux obstacles à l'exercice du contrôle hiérarchique du décodage. Nul protagoniste ne possède de véritable ascendant sur l'ensemble du réseau. En conséquence, il est difficile d'envisager qu'une norme puisse bénéficier d'une seule interprétation et d'une application unique alors qu'aucune autorité n'exerce un contrôle hiérarchique sur son décodage.

Par exemple, un administrateur de serveur de courrier électronique ne peut s'assurer que sa politique contre les messages non sollicités sera appliquée et interprétée comme il l'entend par le FAI d'un expéditeur de pourriels. De plus, le fait que l'administrateur choisisse de sanctionner le FAI en interrompant tout message qui provient de son serveur n'équivaut pas à un contrôle hiérarchique. Il s'agit simplement d'une lutte de pouvoir entre deux acteurs de même niveau. Laquelle se distingue d'une « hiérarchie continue et intégrale ». Seule l'État dispose, dans les limites territoriales où sa compétence s'applique, d'une maîtrise sur l'interprétation et l'application de ses lois, et cela même pour des ressources décentralisées.

Il s'en suit qu'aucune ressource Internet décentralisée ne conduit à la mise en œuvre, en contexte transnational, d'un contrôle hiérarchique. Suivant cette perspective, seuls les auteurs disposant d'une ressource centralisée peuvent s'en prévaloir. En effet, l'interprétation et l'application de la politique d'un outil de recherche demeurent, en

---

[172] *Id.*, p. 92.

dernier lieu, celles du propriétaire de l'engin. La centralisation du pouvoir lui permet de « réformer » toute autre interprétation ou application de son code d'utilisation.

Chapitre II - Analyse systémale d'un pouvoir diffus

L'inexistante, sur une ressource décentralisée, de pouvoir de réformation ou de tout procédé ayant pour effet de contrôler le décodage d'une norme suppose que la solution autoréglementaire relative au courrier électronique non sollicité et au pollupostage procède d'une normativité moins prévisible que les règles élaborées par les opérateurs d'outil de recherche. Une étude en profondeur des conséquences de la diffusion du pouvoir s'impose donc.

L'analyse du système de contrôle du décodage des normes repose sur les mécanismes d'accession des normes à leur signification. Elle ne se préoccupe pas des institutions ou des personnes chargées du décodage mais plutôt de la manière dont il s'effectue[173]. L'intéressement à un pouvoir diffus, à l'absence de monopole normatif sur Internet, nécessite donc une justification. La remarque suivante précède notre raisonnement :

> [...] la signification de la norme dépend au moins autant d'institutions « officielles » - hiérarchiques ou juridictionnelles - que « non officielles » - à la limite, de chacun des membres du groupe social qui, procédant à la lecture de la norme, en donne sa propre interprétation et conformant sa pratique et son comportement à son interprétation, fait produire à la norme des effets qui peuvent être très éloignés de ceux qu'en avait prévus ou conçus son auteur. [174]

En minimisant le rôle des institutions chargées du décodage, le professeur Timsit admet l'avènement, dans un cas extrême, d'un lien de dépendance entre la signification et l'interprétation des membres d'un groupe social.

Or, créant une double concurrence des normes et des champs de valeurs, les contextes des ressources « décentralisées » et « individuelles » d'Internet poussent justement cette

---

[173] *Id.*, p. 181.

[174] *Id.*, p. 180.

relation à la limite. Ces ressources accordent à chaque « membre », à chaque internaute, un choix normatif exempt de toutes interprétations, applications et valeurs autres que celles dont il fait siennes. En conséquence, chaque norme choisie accède à la signification voulue par son auteur. La décentralisation (section I) et l'individualisation (section II) engendrent donc des systèmes ponctuels à forte intégration, des systèmes dans lesquels le contrôle du décodage est assuré.

Dans une perspective autoréglementaire, ces effets contextuels emportent comme séquelle l'entrave à l'adhésion des différents protagonistes à une solution normative commune. Celle-ci risque, en présence de plusieurs champs de valeurs, d'acquérir une toute autre signification que celle léguée par les internautes de la vieille génération. La voie autorèglementaire dépendrait donc d'un système à faible intégration.

Section I - L'effet de décentralisation : la concurrence des normes

La concurrence des normes est encouragée par les ressources décentralisées (sous-section I) et favorise l'internaute comme seul Lecteur de la norme (sous-section II).

Sous-section I - Les ressources favorables à la concurrence

Excluant toute concentration du pouvoir, une ressource Internet décentralisée implique l'existence d'une multitude de serveurs disposant d'un ascendant technique sur leurs usagers. Chaque protagoniste peut aménager librement l'utilisation de ses services. Ainsi, un administrateur de serveur SMTP ou NNTP peut interdire le *spamming*, réglementer le courrier électronique non sollicité et le pollupostage, ou *a contrario*, autoriser expressément ou tacitement l'exercice de ces activités. La diffusion du pouvoir se manifeste par une prolifération de normes destinées à encadrer la pratique d'une

même activité[175]. À cette distribution du pouvoir, se joignent les normes des acteurs politiques.

En raison de l'effet de décentralisation, une foule de règles différentes, tant par leur objet que par les stratégies normatives qu'elles comportent, s'offrent aux utilisateurs. Les internautes disposent donc d'un libre choix. Ils ont l'opportunité d'adopter la règle qui leur convient ou celle qui les convainc.

Dans la plupart des cas, le choix de l'internaute est certainement inconscient. Il devient volontaire lorsque l'utilisateur opte, dans son intérêt, pour l'une ou l'autre des normes proposées. À cet égard, sa préférence sera conditionnée par le « marché normatif »[176].

À l'inverse du courrier électronique et des groupes de discussion Usenet, les ressources centralisées se caractérisent par un monopole technique et normatif. Ainsi, les règles énoncées par l'opérateur d'un outil de recherche bénéficient d'un système à forte intégration. Celles-ci, tatouées de la substance et de la puissance de leur auteur, sont destinées à être interprétées et appliquées par lui, garantissant le contrôle du décodage de la norme.

Sous-section II - Le Lecteur de la norme en contexte de concurrence

Comme l'expose le professeur Timsit, le Lecteur de la norme est, à la limite, chaque membre d'un groupe social. Dans le cadre du modèle étatique, où prime la conception positive du droit, cette limite se voit repoussée par des systèmes hiérarchiques.

---

[175] À cet égard, l'organisation Usenet II tente d'instaurer un réseau hiérarchique de groupes de discussion parallèle à la ressource Usenet. Ce nouveau modèle a pour effet de centraliser l'exercice du pouvoir. Cependant, il s'agit d'un regroupement volontaire de serveurs Usenet. Voir Usenet II : http://www.usenet2.org/usenet/.

[176] « A kind of competition between individual networks to design and implement rule-sets compatible with the preferences of individual internetwork users will thus marerialize in a new and largely unregulated, because largely unregatable, market for rules. » D. POST, « Anarchy, State, and the Internet : An Essay on Law-Making in Cyberspace », (1995) *J. Online L.*, http://warthog.cc.wm.edu/law/publications/jol/post.html.

En effet, de tels systèmes favorisent un haut degré du contrôle du décodage et restreignent la place laissée à la codétermination, l'auteur de la norme profitant à souhait de ses pouvoirs de prédétermination (pouvoir de disposer des stratégies normatives) et de surdétermination (pouvoir d'imposer le champs interprétatif du décodage).

Il peut s'agir de ces systèmes juridictionnels où le contrôle du décodage s'effectue par référence à des éléments internes de la norme. Distingués par un contrôle autoréférenciel, ces systèmes ne concèdent aucun pouvoir de surdétermination à l'autorité chargée du décodage, le juge. Sa fonction de magistrat l'oblige, lorsqu'il procède au décodage, à se référer uniquement à la norme, c'est-à-dire aux valeurs imposées par son auteur[177]. Le caractère hiérarchique de ce système s'estompe donc à chaque fois que le juge renvoie à un code différent de celui de la norme, pavant ainsi la voie au gouvernement des juges.

Il peut aussi s'agir d'un système administratif où le contrôle du décodage de la norme est mené par référence à des éléments externes de la norme, c'est-à-dire selon un contrôle hétéroréférentiel. Dans ce cas, l'autorité chargée du décodage de la norme, l'agent administratif, dispose d'un pouvoir de surdétermination. Le système devient hiérarchique lorsque cette compétence est contrôlée par l'auteur de la norme en vertu de ses divers pouvoirs d'instruction et de réformation.

Au regard des protagonistes techniques du réseau, le système de type administratif détermine le contrôle du décodage des normes élaborées par les propriétaires de ressources et les « représentants ». En effet, l'interprétation et l'application « officielles »

---

[177] G. TIMSIT, *op. cit.*, note 5, pp. 184-185. Bien qu'il qualifie les systèmes juridictionnels à forte intégration de systèmes hiérarchiques, le professeur Timsit explique que le principe de séparation des pouvoirs exclut toute subordination hiérarchique du juge au législateur (pp. 189-190). Le caractère hiérarchique du système s'expliquerait plutôt par la mission exigeante mais originelle dont est investi le juge, celle de déclarer le droit (p. 184).

des règles sont accomplies par référence à un élément externe de la norme, l'auteur : le FAI, l'administrateur du serveur ou l'opérateur de l'outil.

De même, le décodage des normes émises par les différents « représentants » est réalisée par référence aux membres des regroupements à l'origine de la norme[178]. Dans ce cas, le pouvoir de surdétermination dépend de la subordination volontaire des membres et des tiers affectés. Ces normes sont donc sujettes à un cas limite, à cette situation exceptionnelle dont parle Timsit, ne pouvant être repoussé par un système hiérarchique.

Ce cas extraordinaire devient une situation banale dans un contexte de décentralisation et de concurrence des normes. Chaque utilisateur se voit libre de choisir les règles de conduite que les acteurs, en fait, « proposent ». En d'autres termes, il peut « contracter » avec l'un ou l'autre des propriétaires de ressources, c'est-à-dire changer de fournisseur d'accès Internet, de serveur de courrier électronique ou s'adresser à un serveur Usenet public. Il devient, par sa capacité de changer de « cocontractant », le Lecteur volage s'appropriant la norme défendue par d'autres[179]. Mais au même titre que l'or, il sait que les normes sont rares…

De nouvelles normes, élaborées par quelques propriétaires et « représentants », émergent. Elles sont destinées à interdire aux autres protagonistes, propriétaires et usagers, l'exercice du *spamming*[180]. Ces règles révèlent, par l'inexistence du contrôle du décodage, un faible degré de juridicité. En effet, le possible refus des destinataires d'adopter le code de l'auteur et d'admettre son « champ de compétence » empêche tout contrôle ultérieur du décodage de la norme. À ce sujet, le professeur Timsit remarque :

---

[178] En effet, les dénonciateurs, les internautes disposant de listes noires, les « suppresseurs de pollupostages » et autres interprètes et applicateurs des règles des « représentants » sont généralement leurs auteurs.

[179] À cet effet, « […] what emerges represents the rules that people have voluntary chosen to adopt rather than rules that have been imposed by others upon them ». D. POST, *loc. cit.*, note 176.

[180] À titre d'exemple, voir la politique du FAI AOL. *AOL's Unsolicited Bulk E-mail Policy* : http://www.aol.com/info/bulkemail.html.

> Il existe en fait tout un système de contrôle du décodage des normes dont le degré d'intégration est évidemment, pour partie, lié au degré de centralisation et de hiérarchisation de l'ordre juridique.[181]

Caractérisé par un faible degré de hiérarchisation, les ressources décentralisées favorisent, au regard d'une solution normative commune, un système à faible intégration, un système dialogique. Celui-ci se présente comme un « marché normatif » où chaque autorité tente d'imposer sa loi.

Mais dans une perspective systémale, cette relation dialogique n'existe pas seulement en raison de l'effet de décentralisation et de concurrence des normes. À cet égard, Gérard Timsit observe que le système de contrôle du décodage ne saurait être réduit à la centralisation et à la hiérarchisation, puisque :

> [...] l'y réduire serait commettre de nouveau l'erreur consistant à limiter la signification de la norme à son seul mécanisme de prédétermination, alors qu'existent également une co- et une surdétermination.[182]

En conséquence, le contrôle du décodage d'une solution autoréglementaire est également fonction de la concurrence des champs de valeurs.

Section II - L'effet d'individualisation : la concurrence des champs de valeurs

Sans prédétermination satisfaisante, la solution autorèglementaire du *spamming* obtient, en présence d'un seul champ de décodage, un degré intermédiaire de juridicité. En effet, la concurrence des auteurs et des normes empêche toute prédétermination efficace relativement à une solution globale du *spamming*, mais ne compromet pas

---

[181] G. TIMSIT, *op. cit.*, note 5, p. 183.

[182] *Id.*

nécessairement l'unicité du champ de valeurs. Il existe des situations où les traces matérielles laissées par les normes concurrentes souffrent entre elles de légères contradictions alors que le code utilisé pour les déchiffrer demeure le même[183].

Ainsi, dans un contexte de concurrence des normes, peut intervenir une seconde joute, celle des champs de valeurs. Favorisée par le caractère d'individualisation de certaines ressources Internet (I), cette double concurrence met en évidence la nature régulatoire des normes issues de ce réseau (II).

Sous-section I - Les ressources favorables à la concurrence

Environnements électroniques de nature privée, nous avons démontré que les ressources « individuelles » ont pour principale répercussion la création de conditions impropres à l'émergence d'un « sentiment communautaire » propice à la préservation d'une ressource fonctionnelle. Ces ressources engendrent subséquemment un phénomène d'individualisation.

Le courrier électronique illustre cette relation de cause à effet. Isolés les uns des autres par des relations strictement privées[184], les utilisateurs de cette ressource ont moins l'opportunité de développer d'autres intérêts que ceux de leur propre boîte de courriers électroniques. Qualifiable d'espace privé, cette boîte individualise l'usager. Ainsi, les rationalités de la valorisation du droit de propriété et du dénigrement de l'activité promotionnelle ne sont partagées que par les internautes victimes du *spamming*.

Néanmoins, l'individualisation peut être surmontée lorsque les effets importuns s'avèrent considérables. Comme nous l'avons déjà souligné, les utilisateurs ont la possibilité de sortir de leur isolement en s'appropriant une ressource de nature publique

---

[183] Voir : *Id.*, p. 111 et s.

[184] Les messages expédiés par courrier électronique sont essentiellement de nature privée bien qu'il est techniquement possible de les intercepter.

pour dévoiler le caractère abusif du *spamming*. Si un consensus sur le courrier électronique ne s'établit pas par l'utilisation de cette ressource, les débats qui ont cours sur Usenet et le Web risquent de développer un « sentiment communautaire » imprévu.

Consécutif à l'individualisation, la concurrence des champs de valeurs ne semble pas entretenir un effet permanent. Justifiable par une relation d'ordre économique, la gravité des abus se révèle être un facteur déterminant dans le processus d'émergence de l'interdiction du *spamming* sur Internet.

Encore est-il nécessaire, dans le cadre du processus d'émergence des normes en contexte décentralisé, que les principaux intéressés assurent un débat normatif persuasif. À ce titre, la nature régulatoire des règles est représentative de leur volonté.

Sous-section II - La nature régulatoire des normes sur Internet

La nature régulatoire des normes issues du réseau Internet ne saurait être abordée sans renvoi à la double dimension normative (juridicité / normativité ou impérativité). Gérard Timsit expose que chacune de ces dimensions façonne le caractère obligatoire de la norme :

> [L]e caractère obligatoire de la norme ne dépend pas seulement de la contrainte - ce que j'appelle la normativité - qui peut être mise en œuvre pour en faire respecter les termes, mais également de la signification, la juridicité qu'elle revêt et, par conséquent, de la manière et de la mesure dans laquelle le jugement rendu adhère aux valeurs dominantes du groupe social. Pour dire les choses autrement, il apparaît que le caractère obligatoire de la norme ne se situe pas seulement sur le plan de l'impérativité - de la contrainte, de la normativité - mais résulte également de considérations liées à la juridicité, à la signification de la norme...[185]

[185] G. TIMSIT, *loc. cit.*, note 6, 101.

Dans la perspective de cette double dimension, la norme régulatoire se traduit comme l'expression d'une responsabilité collective, comme une loi que le groupe s'impose à lui-même, évacuant le plan de la contrainte[186]. En effet, substituant à la sanction des mécanismes de persuasion, d'incitation et de recommandation, la norme de régulation induit un déclin de la notion d'impérativité[187].

Dans un contexte électronique décentralisé et « anarchique », où les mécanismes de la contrainte s'effacent au profit d'un pouvoir diffus, les différentes autorités sont amenées à promouvoir les valeurs conformes aux intérêts qu'elles défendent et, par conséquent, des normes qu'elles édictent. Ce faisant, elles portent une attention particulière à l'inscription du code dans le texte - ou dans le *contexte* - de la norme. Par le biais de textes persuasifs, de statistiques et d'arguments économiques, elles façonnent le code auquel chaque utilisateur, acteur et communauté adhère, soit en raison des préoccupations qui le rendent soucieux, réfractaire ou furieux, soit, simplement, en raison de son échelle de valeurs.

À titre d'illustration, rappelons quelques textes de nature régulatoire : les RFC sur l'utilisation du courrier électronique et des groupes de discussion, les FAQ des groupes de discussion *news.admin.net-abuse*, les campagnes d'internautes contre le courrier électronique non sollicité (*Don't Spam!!!*, *Combattez le Spamming*, etc.), les chartes de groupe de discussion, la campagne de sensibilisation parallèle à la législation de l'État de Washington, etc.

Se rapportant à des environnements décentralisés, ces règles privilégient le plan de la juridicité et l'une de ses principales composantes, la surdétermination. Souffrant à la fois des imprécisions des différentes règles et de l'ambiguïté que leur lecture parallèle emporte, la prédétermination de la solution normative commune est quasi-nulle. Dans

---

[186] G. TIMSIT, *op. cit.*, note 8, pp. 198 et 202.

[187] *Id.*, p. 202.

cette perspective, la portée de cette solution est réduite à la surdétermination qu'elle renferme. Ainsi Timsit expose la caractéristique fondamentale de la norme régulatoire :

> La norme de régulation comporte, par définition, l'indication des valeurs au nom desquelles les décisions individuelles doivent être adoptées. Elle ne comporte même que cette indication. C'est justement ce qui en fait l'originalité - c'est une norme d'orientation.[188]

Or, lorsque les orientations des normes concurrentes entrent en conflit, une porte s'ouvre au dialogisme et le sens de l'interdiction du *spamming* se retrouve forcément disséminé.

Néanmoins, cette ouverture semble, dans les faits, se refermer progressivement au profit d'une solution autorèglementaire. En effet, les rationalités avancées par les détenteurs du pouvoir s'avèrent identiques et majoritaires. À ce titre, le pullulement des détracteurs du réseau ne doit pas être perçu comme un problème affectant la juridicité de l'interdiction du *spamming* mais plutôt comme une difficulté liée à l'effectivité de la norme d'autoréglementation que seule la technique semble pouvoir surmonter.

En somme, il est impensable d'interpréter le pollupostage et le courrier électronique non sollicité comme des activités parfaitement « licites » du réseau. Elles sont actuellement encadrées par une proscription généralisée[189] mais imprécise, révélant un degré intermédiaire de juridicité.

---

[188] *Id.*, p. 211.

[189] À cet égard, même les lois réglementant le courrier électronique non sollicité se voient tranquillement remplacer par une législation moins permissive octroyant aux propriétaires de ressources la possibilité d'interdire légalement cette activité sur leur serveur. Voir : Washington House Bill 1037 (1999). La première jurisprudence canadienne sur le courrier électronique non sollicité est au même diapason. Voir : Sophie BERNARD, « Victoire contre un polluposteur », (1999) *Branchez-Vous!*, http://www.branchez-vous.com/actu/99-04/03-191901.html.

Conclusion

La mise en rapport de la norme avec l'environnement dans lequel elle s'intègre introduit une nouvelle approche plus à même de rendre compte des différentes formes que revêt la normativité. En cela, cette manière d'étudier les phénomènes normatifs assure une appréciation rigoureuse des qualités d'une solution normative telle que l'autoréglementation. Dans le cas particulier du *spamming*, cet exercice nous a d'abord conduit aux raisons pour lesquelles un besoin normatif s'est créé. La nécessité d'interdire cette activité résulte d'un simple rapport économique inéquitable et de l'influence d'une tradition universitaire et scientifique sur un réseau dont l'avenir est assurément commercial.

L'étude de l'environnement nous a ensuite renseigné sur les rapports sociaux qu'emporte la structure des ressources Internet. Certaines se sont révélées défavorables à la mise en commun d'intérêts entre les utilisateurs. D'autres ont témoigné d'une organisation et d'un fonctionnement opposés à une hiérarchisation des relations entre protagonistes de même acabit. Aussi, les contraintes exercées par la structure d'Internet et par ses possibilités techniques se sont avérées une source importante de normativité.

L'influence de l'environnement s'est également concrétisé par l'existence, dans le cas de ressources décentralisées et privées, d'un marché de règles sujet aux fluctuations et aux divergences des valeurs, idéologies et intérêts. Nous avons donc reconnu que le caractère obligatoire de la solution autoréglementaire était, dans ces cas particuliers, passablement diminué. Néanmoins, une certaine intensité du caractère obligatoire a pu être préservée par l'élaboration de règles destinées à convaincre les destinataires.

Nous avons donc conclu que la voie autoréglementaire, dans le cas des ressources décentralisées, disposait d'un degré intermédiaire de juridicité puisqu'elle ne bénéficiait d'aucun contrôle hiérarchique. L'observation des carences normatives des contextes

électroniques décentralisés et privés rendent maintenant possible une classification plus précise du degré de juridicité de l'interdiction du *spamming*.

En effet, une nouvelle gradation peut être effectuée. Celle-ci est déterminée par l'évaluation quantitative de la prédétermination et de la surdétermination. La quantification de ces éléments repose sur l'appréciation de leurs principales composantes.

L'opération de prédétermination est susceptible de varier en fonction des stratégies normatives appliquées aux textes et de la puissance de l'auteur. À cet égard, nous avons établi que l'autorité était dépendante du degré de centralisation du pouvoir. La prédétermination est donc le fruit des procédés normatifs et de la concentration du pouvoir. Si nous attribuons trois différents degrés à ces deux facteurs, il est possible d'évaluer le degré de prédétermination d'une solution normative commune. Celui-ci résulte du produit des degrés attribués aux facteurs. Une prédétermination parfaite équivaut donc à un produit de 9.

L'estimation de la surdétermination s'avère plus complexe. Sujette au contrôle hiérarchique de l'auteur, elle dépend également de l'unicité du champ de valeurs. Nous avons démontré que le caractère unique du champ interprétatif était fonction de la nature du contexte de la norme. Par conséquent, la surdétermination résulte du contrôle hiérarchique et du caractère communautaire de la ressource. L'allocation de trois niveaux à chacun de ces éléments permet, lorsque le produit atteint le chiffre 9, d'apprécier l'idéal de surdétermination.

Cependant, nous avons remarqué que l'unicité du champ de valeurs peut être engendré autrement que par la nature communautaire d'une ressource. La gravité des effets du *spamming* risque également, sinon plus, de favoriser le partage d'intérêts et de valeurs. Il faut en effet restorer l'importance, même dans un contexte électronique, des facteurs

traditionnels de l'émergence des normes : les intérêts en cause, les motivations des acteurs, les rapports de force, etc[190].

Ces différents éléments nécessitent sans doute une analyse plus poussée. En outre, la dimension économique du *spamming* n'est qu'un résumé conceptuel des diverses relations qui sont à l'origine d'un code majoritaire.

L'acceptation des idéologies, valeurs et croyances implique toutefois un exercice de persuasion. Les facteurs traditionnels de l'émergence du droit requièrent, sur un média électronique décentralisé, un passeport susceptible d'être visé par les destinataires. À cet égard, la norme régulatoire fait office de laissez-passer. La présence de telles règles vient donc modifier la donne.

Pour synthétiser l'ensemble de ces relations normatives, il est possible de s'en remettre à quelques graphiques. Ces derniers ont pour objectif d'indiquer, pour chaque ressource, l'espace occupé par la prédétermination et par la surdétermination.

Résultant de l'addition de l'intensité respective de ces éléments, le degré de juridicité a pour limite et idéal la somme de 18. Débutant à un plancher de 2, la mesure médiane est fixée à 10. Le tableau suivant récapitule cette nouvelle gradation de la juridicité :

Tableau 1. Récapitulatif d'une nouvelle gradation de la jutidicité (Source : l'auteur)

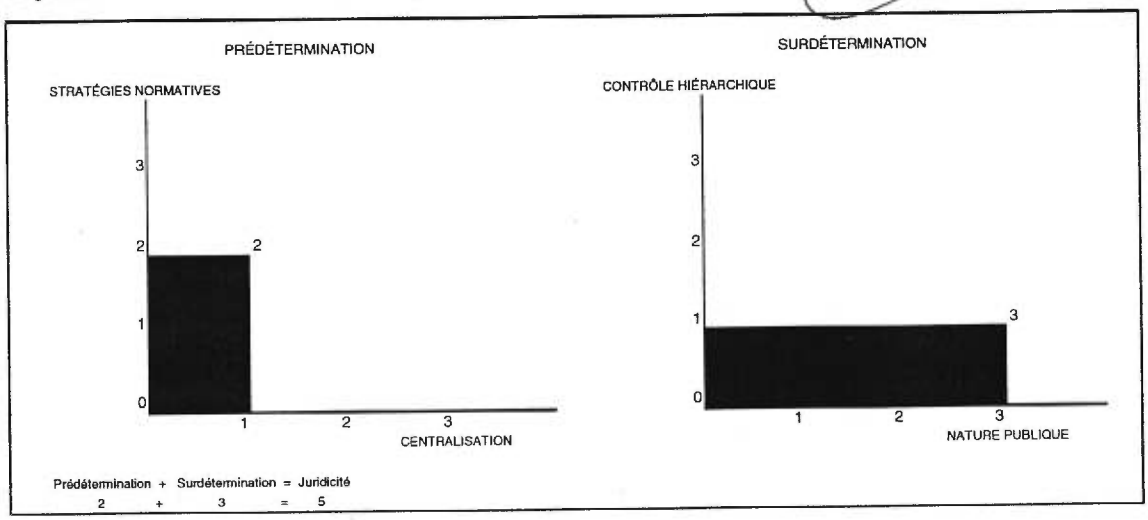
	Occupation				Degré de juridicité
Degré minimal de juridicité	Degré de prédétermination = 1		Degré de surdétermination =1		2
	SN = 1	CE = 1	CH = 1	NP = 1	
Degré intermédiaire de juridicité	Degré de prédétermination = 5		Degré de surdétermination = 5		10
	SN ˜ 2,25	CE ˜ 2,25	CH ˜ 2,25	NP ˜ 2,25	
Degré maximal de juridicité	Degré de prédétermination = 9		Degré de surdétermination = 9		18
	SN = 3	CE = 3	CH = 3	NP = 3	
Où SN = stratégies normatives, CE = centralisation, CH = contrôle hiérarchique et NP = nature publique.					

[190] R. CÔTÉ, P. MACKAY, G. ROCHER et P. TRUDEL, *op. cit.*, note 16, p. 11.

Ainsi, la proscription du pollupostage sur la ressource Usenet atteint un degré faible de 5, attestant du peu d'espace occupé par la prédétermination et par la surdétermination (voir figure 1). Les indéterminations laissées par les stratégies normatives, le caractère décentralisé de la ressource, l'absence de contrôle hiérarchique et la nature publique du contexte expliquent ce résultat.

Figure 3 (Source : l'auteur)

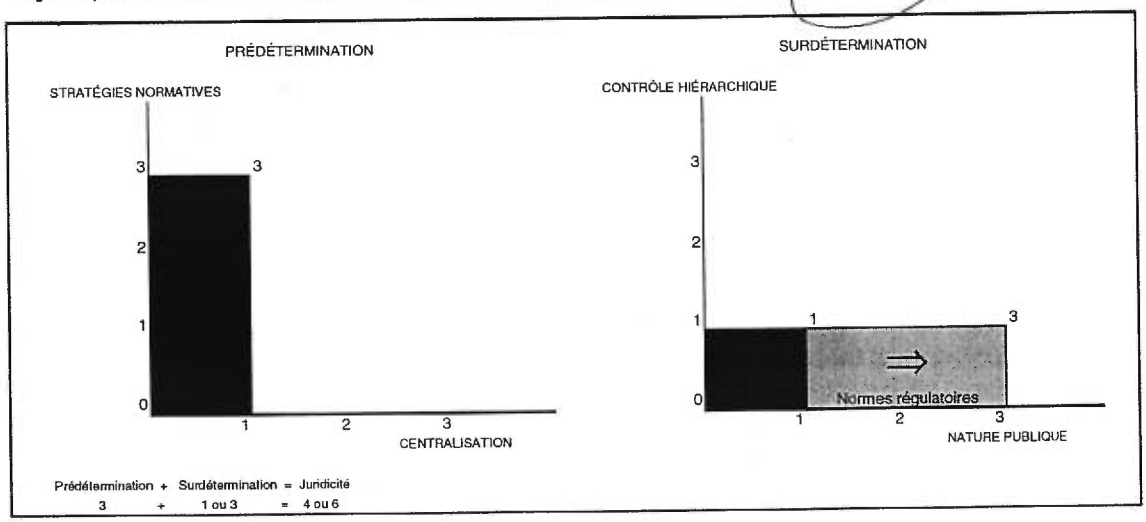
Degré de juridicité de l'interdiction du *spamming* - Usenet



La normativité afférente au courrier électronique non sollicité obtient un degré inférieur de 4 (voir figure 2). Confrontée à une structure décentralisée, l'opération de prédétermination bénéficie toutefois de règles claires de la part des législateurs et des fournisseurs d'accès Internet. À ce titre, un degré de 3 lui est attribuable.

La surdétermination souffre, quant à elle, de l'absence de contrôle hiérarchique et d'un contexte privé. Elle mérite donc une note de 1 sur 9. Cependant, l'existence de règles régulatoires dénotant la gravité des effets du pourriel a pour effet de stimuler l'univocité du champ de valeurs. Par conséquent, la surdétermination acquiert un degré de 3, et la juridicité se voit augmenter à 6.

Figure 4 (Source : l'auteur)

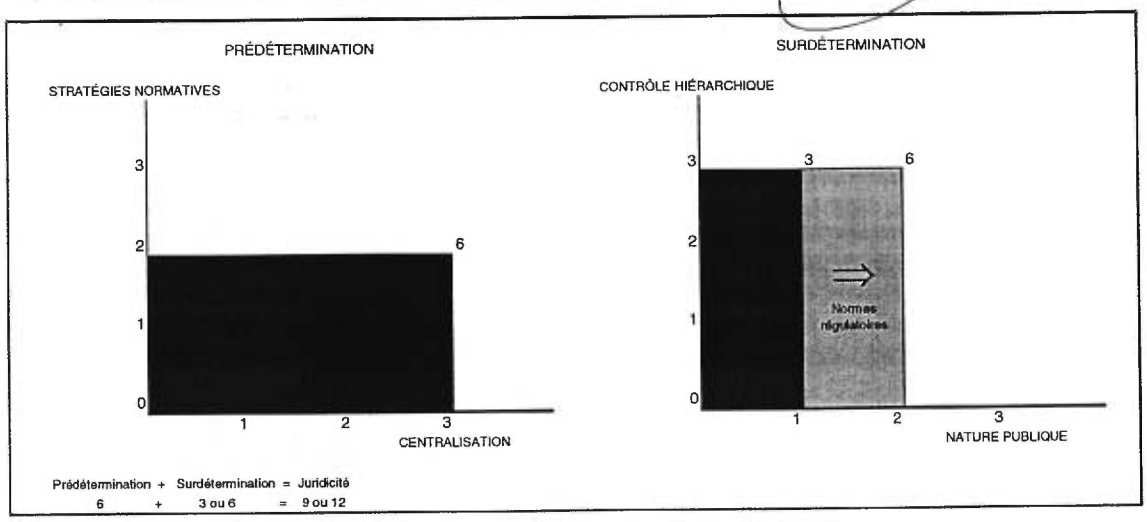


Les ressources centralisées offrent un degré de juridicité plus remarquable. Le caractère obligatoire de l'interdiction du *spamming* par un opérateur d'outil de recherche est évalué à 9. Ce calcul s'explique par la centralisation d'un outil de recherche et le pouvoir de surdétermination que son administrateur détient. Toutefois, pour des raisons que nous avons déjà expliquées, les opérateurs d'outils de recherche n'ont pas inscrit adéquatement le contenu de leur proscription, laissant quelques imprécisions. L'opération de prédétermination obtient donc un degré de 6.

De nature privée, la normativité destinée à enrayer le référencement abusif pose une limite au développement d'un champ interprétatif unique. Cet obstacle est susceptible d'être contourné par la mise en œuvre de normes persuasives. Dans cette éventualité, la surdétermination risque d'obtenir un produit de 6 (éventuellement de 9), et la juridicité, un degré supérieur de 12 (ou de 15).

Figure 5 (Source : l'auteur)

Degré de juridicité de l'interdiction du *spamming* - Outil de recherche



Ces résultats emportent certaines considérations à l'égard de la solution autoréglementaire. La première se rapporte à l'importance du contrôle hiérarchique de l'ordre juridique dans l'attribution du degré de juridicidé. La mise à profit de cet élément a pour conséquence d'établir la limite du caractère obligatoire de l'autoréglementation. Cette frontière est déterminée, au regard de l'acceptation volontaire des normes, par l'impossibilité d'imposer une application et une interprétation voulues par l'auteur. La solution autoréglementaire ne peut donc obtenir un degré de juridicité supérieur à 12.

Ne s'adressant qu'aux ressources décentralisées, la solution autoréglementaire est affectée par une seconde limite. En effet, l'autoréglementation n'est envisagée que lorsque chaque membre participe volontairement au développement des règles de l'activité à laquelle il participe. Or, seuls les contextes décentralisés présente cette faculté puisque chaque internaute dispose d'un libre choix normatif.

Par le jeu de la concurrence des normes, ces contextes ont pour effet de diminuer le plafond de juridicité attribuable à la « solution du marché ». Le caractère obligatoire de l'autoréglementation est donc confiné à une limite de 6 sur l'échelle de la qualité juridique d'une norme.

Témoignant d'un degré de juridicité maximal de 6, la prohibition généralisée du courrier électronique non sollicité atteint le plafond de l'autoréglementation. Sans disposer d'un caractère obligatoire supérieur, cette règle peut néanmoins être interprétée et appliquée conformément à son sens initial. Il existe donc des circonstances dans lesquelles se préserve la signification d'une norme malgré le faible contrôle du décodage.

L'autoréglementation est donc une solution normative imprévisible au regard du caractère obligatoire qui en résulte. Elle suit pas à pas les changements de valeurs et repose substantiellement sur l'unicité du champ interprétatif du décodage. Elle constitue un marché de valeurs et de normes sujet aux fluctuations des intérêts des différents protagonistes. En cela, l'autoréglementation reflète de manière quasi-immédiate les rapports socio-économiques.

Seuls les moyens techniques restent disposés à rendre la « solution du marché » encore plus prévisible et obligatoire. Susceptible de pallier à un système « anarchique » et à un pouvoir diffus, la technique s'assure une place de choix dans l'engendrement du droit en contexte décentralisé.

Tables bibliographiques

A. Monographies

BERGERON, M., KEMPA, C., et PERRON, Y., *Vocabulaire d'Internet : vocabulaire anglais/français*, 2e éd., Ste-Foy, Publication du Québec, 1997.

CÔTÉ, R., MACKAY, P., ROCHER, G., et TRUDEL, P., *Bilan et perspectives. Cadre conceptuel et propositions sur l'émergence des normes dans l'univers technologique*, Montréal, Édition conjointe des Cahiers du Centre de recherche en droit public et *Recherche*, 1992.

KATSH, E. M., *The Electronic Media and the Transformation of Law*, Oxford, Oxford University Press, 1989.

OSMAN, F., *Les principes généraux de la Lex Mercatoria : contribution à l'étude d'un ordre juridique anational*, Paris, L.G.D.J., 1992.

RHEINGOLD, H., *Les communautés virtuelles*, (trad. Lionel Lumbroso), Paris, Éditions Addison-Wesley France, SA, coll. Mutations Technologiques, 1995.

TIMSIT, G., *Archipel de la norme*, Paris, Presses Universitaires de France, 1991.

TIMSIT, G., *Les noms de la loi*, Paris, Presses Universitaires de France, 1997.

TIMSIT, G., *Thèmes et systèmes de droit*, Paris, Presses Universitaires de France, 1986.

TRUDEL, P., ABRAN, F., BENYEKHLEF, K., et HEIN, S., *Droit du cyberespace*, Montréal, Éditions Thémis, 1997.

B. Articles de revue, publications électroniques ou recueils d'études

ANONYME, «NoCeM FAQ. VO. 93», http://www.cm.org/faq.html.

ANONYME, «The What is Scientology? (ARSBOMB) Spam Team FAQ for Los Angeles Area ISPs », (22 décembre 1996), http://www.panix.com/~tbetz/WIS_Spam _Team_FAQ.shtml.

ANDREWS, W., «Beating (Up) the System», (1997), 22 sept., *Web Week* 38, 41, http://www.internetworld.com/print/1997/09/22/industry/19970922-beating.html.

BASELEY, W. D., « The Email Abuse FAQ », (25 juin 1998), http://members.aol.com/ emailfaq/emailfaq.html.

BEAULIEU, J., « Les muds ou l'art de réussir le renouveau communautaire par la Coopération », (1997) *Espace Droit*, http://www.droit.umontreal.ca/espacedroit/fr/crdp/1997/beauliej.html.

BELL, J., « News.newusers.questions : What newsgroups are and how they work? », (1999), http://www.geocities.com/ResearchTriangle/Lab/6882/how-it-works.html.

BELLEY, J.-G., « L'État et la régulation juridique des sociétés globales: pour une problématique du pluralisme juridique », (1986) 18.1 *Sociologie et sociétés* 11.

BERNARD, S., « Victoire contre un polluposteur », (1999) *Branchez-Vous!*, http://www. branchez-vous.com/actu/99-04/03-191901.html

BOWEN, B. D., « Controlling unsolicited bulk e-mail (Who's taking action? What's being done?) », (1997), http://www.sun.com/sunworldonline/swol-08-1997/swol-08-junkemail.html.

BRANSCOMB, A. W., « Cyberspaces: Familiar Territory or Lawless Frontiers », (1996) 2 *Journal of Computer-Mediated Communication*, http://jcmc.mscc.huji.ac.il/vol2/issue1 /intro.html.

BURK, D. L., « Jurisdiction in a World Without Borders », (1997) 1 *VA. J.L. & TECH.* 3, http://www.student.virginia.edu/~vjolt/vol1/BURK.htm.

BYRNE, J., « Squeezing Spam Off the Net: Federal Regulation of Unsolicited Commercial E-mail », (1998) 2 *W. Va. J. L. & Tech.* 4, http://www.wvjolt.wvu.edu/v2i1/byrne.htm.

BYSHENK, G., «I've been spammed! What do I do?», http://www.tezcat.com/~gbyshenk/ive.been.spammed.html.

CARROLL, M. W., « Garbage In: Emerging Media and Regulation of Unsolicited Commercial Solicitations », (1996) 11 *Berkeley Tech. L.J.* 233, http://www.law.berkeley.edu/journals/btlj/articles/11-2/carroll.html.

CRANOR, L. F. et LAMACCHIA, B. A., « Spam! », (1998) 41 *Communications of the ACM* 74 (version définitive : http://www.acm.org/pubs/citations/journals/cacm/1998-41-8/p74-cranor/).

CURTIS, P., « Mudding : Social Phenomena in Text-Based Virtual Realities », (1992), ftp://parcftp.xerox.com/pub/MOO/papers/DIAC92.

DEUTSCH, P., « Preserving and Promoting the "Internet Culture" », (mars 1994), http://www.eff.org/papers/eegtti/eeg_268.html.

FALK, J. D. et SOUTHWICK, S., «The Net-Abuse FAQ», (23 décembre 1998), http://www.cybernothing.org/faqs/net-abuse-faq.html.

FURR, J. K., « Advertising on Usenet: How To Do It, How Not To Do It », ftp://rtfm.mit.edu/pub/ faqs/usenet/advertising/how-to/part1.

GAUTRAIS, G., LEFEBVRE, G. et BENYEKHLEF, K., « Droit du commerce électronique et normes applicables : l'émergence de la *lex mercatoria* », (1997) 5 *RDAI/IBLJ* 547.

HAMBRIDGE, S., « RFC 1855 : Netiquette Guidelines » (Octobre 1995), http://www.sri. ucl.ac.be/SRI/frfc/rfc1855.fr.html.

HAMBRIDGE, S et LUNDE, A., « IETF RUN Working Group draft-ietf-run-spew-08 : DON'T SPEW. A Set of Guidelines for Mass Unsolicited Mailings and Postings (spam*) », (avril 1999), http://search.ietf.org/internet-drafts/draft-ietf-run-spew-06.txt (expire le 21 octobre 1999).

HAMBRIDGE, S. et EASTLAKE 3rd, D., « IETF RUN Working Group draft-ietf-run-adverts-00.txt : $$$$$ MAKE ENEMIES FAST $$$$$ or How to Advertise Responsibly Using the Internet », (Mars 1998), http://search.ietf.org/internet-drafts/draft-ietf-run-adverts-00.txt (expiré depuis le 9 septembre 1998).

JOHNSON, D. R., « Due Process and Cyberjurisdiction », (1996) 2 *Journal of Computer-Mediated Communication*, http://www.usc.edu/dept/annenberg/vol2/issue1 /due.html.

JOHNSON, D. R., « Lawmaking And Law Enforcement in Cyberspace », http://www.cli. org/DRJ/make.html.

LAJOIE, A., « La normativité professionnelle dans le droit: trajets et spécificité formelle », dans BELLEY, J.-G., (dir.), *Le droit soluble; Contribution québécoise à l'étude de l'internormativité*, Paris, L.G.D.J., 1996, p. 150.

LEMOS, A., « Les Communautés virtuelles », (1994) in Société, Paris: Dunod, 1994, no 45.

LOSCHAK, D., « Droit, normalité et normalisation », dans Jacques CHEVALIER, *Le droit en procès*, Paris, Presses universitaires de France, 1983.

MACDONALD, R. A., « Les Vieilles Gardes. Hypothèse sur l'émergence des normes, l'internormativité et le désordre à travers une typologie des institutions normatives », dans BELLEY, J.-G., (dir.), *Le droit soluble; Contribution québécoise à l'étude de l'internormativité*, Paris, L.G.D.J., 1996, p. 233.

MARYIN, L.-E., « Spoof, Spam, Lurk and Lag: the Aesthetics of Text-based Virtual Realities », (1996) *Journal of Computer-Mediated Communication*, http://209.130.1.169/jcmc /vol1/issue2/marvin.html.

MALTZ, T., « Customary Law & Power in Internet Communities », (1996) *Journal of Computer-Mediated Communication*, http://www.ascusc.org/jcmc/vol2/issue2/.

MUELLER, S. H., «Fight Spam on the Internet», http://spam.abuse.net.

OBERDING, J. M., et NORDERHAUG, T., « A Separate Jurisdiction For Cyberspace? », (1996) 2 *Journal of Computer-Mediated Communication*, http://www.usc.edu/dept/annenberg/vol2/issue1 /juris.html.

PINARD, D., « Le droit et les faits dans l'application des standards et la clause limitative de la Charte canadienne des droits et libertés », (1989) 30 *Cahiers de droit* 137.

PIQUET, L., « Search Engines Battle the New Spam », (1998) *ZDNet*, http://www.zdnet. com/devhead/stories/articles/0,4413,1600389,00.html.

POST, D. G., « Anarchy, State, and the Internet : An Essay on Law-Making in Cyberspace », (1995) *J. Online L.*, http://warthog.cc.wm.edu/law/publications/jol/post.html.

POST, D. G., et JOHNSON, D. R., « And How Shall the Net Be Governed? A Meditation on the Relative Virtues of Decentralized, Emergent Law », (1996), http://www.cli.org/emdraft.html.

POST, D. G., et JOHNSON, D. R., « Law And Borders - The Rise of Law in Cyberspace », (1996) *Stanford Law Review*, http://www.cli.org/X0025_LBFIN.html.

POST, D. G., et JOHNSON, D. R., « The New 'Civic Virtue' of the Internet », http://www.cli.org/paper4.htm.

REID, E., « Cultural Formations in Text-Based Virtual Realities », (1994), ftp://ftp.lambda. moo.mud.org/pub/MOO/papers/CulturalFormations.txt.

REIDENBERG, J., « *Lex Informatica* : The Formulation of Information Policy Rules Throught Technology », (1998) 76 *Tex. L. Rev.* 553.

ROCHER, G., « L'effectivité du droit », dans LAJOIE, A., MACDONALD, R. A., JANDA, R. et ROCHER, G., *Théories et émergence du droit : pluralisme, surdétermination et effectivité*, Montréal, Les Éditions Thémis, 1998, p. 134.

SKIRVIN, T., « The Cancel FAQ », (1997), http://www.ews.uiuc.edu/~tskirvin/faqs/cancel.html.

SKIRVIN, T et LEWIS, C., «Current Usenet Spam Tresholds and Definitions», (11 octobre 1998) http://www.cen.uiuc.edu/ ~tskirvin/faqs/spam.html.

SORKIN, D. E., « Unsolicited Commercial E-Mail and the Telephone Consumer Protection Act of 1991 », (1997) 45 *Buffalo L. Rev.* 1001, http://www.jmls.edu/faculty/sorkin/tcpa.html.

TIMSIT, G., *La surdétermination de la norme de droit : questions et perspectives*, dans LAJOIE, A., MACDONALD, R. A., JANDA, R. et ROCHER, G., *Théories et émergence du droit : pluralisme, surdétermination et effectivité*, Montréal, Les Éditions Thémis, 1998, p. 99.

TIMSIT, G., « Sept propositions pour une définition systémale du droit », (1989) 10 *Droits. Revue française de théorie juridique* 93.

TIMSIT, G., « Sur l'engendrement du droit », (1988) *Revue de droit public* 39.

TRUDEL, P., « Les effets juridiques de l'autoréglementation », (1989) 19 *Revue de droit de l'Université de Sherbrooke* 251.

WITTES, B., « Witnessing the Birth of a Legal System on the Net », (1995) *American Lawyer Media*, http://www.english.upenn.edu/~afilreis/law-on-net.html.

C. Table législative

Législation

- Lois québécoises

  Code civil du Québec, L. Q. 1991, c. 64.

- Lois américaines

  - Lois fédérales

  Telephone Consumer Protection Act of 1991, Pub. L. No. 102-203, 105 Stat. 2394 (codifié tel qu'amendé à 47 *U.S.C.* § 227 (1994))

  Communications Decency Act of 199, 47 U.S.C. §§ 223.

- Lois étatiques

Californie

An act to amend Section 17538.4 of the Business and Professions Code, relating to advertising chapter 865, Statutes of 1998 (54th Legislatures).

An act to amend Section 17511.1 of, and to add Section 17538.45 to, the Business and Professions Code, and to amend Section 502 of the Penal Code, relating to advertising, chapter 863, Statutes of 1998 (54th Legislatures).

Névada

AN ACT relating to actions concerning persons; providing that a person who transmits certain items of electronic mail is liable to the recipient for civil damages under certain circumstances; providing that the district court may enjoin a person from transmitting certain items of electronic mail under certain circumstances; and providing other matters properly relating theret, chapter 341, Laws of 1997 (69th Legislature).

Virginie

An Act to amend and reenact §§ 8.01-328.1, 18.2-152.2, 18.2-152.4, and 18.2-152.12 of the Code of Virginia, relating to personal jurisdiction, chapter 886, Acts of the General Assembly (1999 Session)

An Act to amend and reenact §§ 8.01-328.1, 18.2-152.2, 18.2-152.4, and 18.2-152.12 of the Code of Virginia, relating to personal jurisdiction, chapter 905, Acts of the General Assembly (1999 Session)

An Act to amend and reenact §§ 8.01-328.1, 18.2-152.2, 18.2-152.4, and 18.2-152.12 of the Code of Virginia, relating to personal jurisdiction, chapter 904, Acts of the General Assembly (1999 Session).

Washington

Prohibited unsolicited electronic mail, chapter 149, Laws of 1998 (55th Legislature).

Propositions législatives

- Propositions européennes

Proposition de directive du Parlement européen et du Conseil relative à certains aspects juridiques du commerce électronique dans le marché intérieur, COM(98) 586, Journal off. 99/C 30 (05/02/1999).

- Projets de loi américains

- Projets fédéraux

Anti-Slamming Amendments Act (S. 1618/H.R. 3888).

Data Privacy Act of 1997 (H.R. 2368).

Digital Jamming Act of 1998 (H.R. 4176).

Electronic Mailbox Protection Act of 1997 (S. 875).

E-Mail User Protection Act of 1998 (H.R. 4124).

Inbox Privacy Act of 1999 (S. 759).

Netizens Protection Act of 1997 (H.R. 1748).

Unsolicited Commercial Electronic Mail Choice Act of 1997 (S. 771).

- Projets étatiques

Alaska House Bill 491 (1997).

California Assembly Bill 1629 (1998).

California Assembly Bill 1676 (1998).

Connecticut House Bill 6558 (1997).

Kentucky Bill Resolution 337/House Bill 41 (1998).

Maryland House Bill 1114 (1998).

Massachusetts House Bill 4581 (1997).

Nevada Senate Bill 13 (1997).

New Hampshire House Bill 1633 (1997).

New Jersey Assembly Bill 295 (1998).

New Jersey Assembly Bill 513 (1998).

New York Senate Bill 3524/Assembly Bill 6805 (1997).

North Carolina House Bill 1744 (1997).

Rhode Island Senate Bill 1073 (1997).

Virginia House Bill 1325 (1998).

Washington House Bill 2752 (1998).

Washington House Bill 1037 (1999).

Wisconsin Senate Bill 283 (1997).

Table de la jurisprudence

Jurisprudence américaine

American Civil Liberties Union c. *Reno*, 929 F. Supp. 824 (E.D. Pa. 1996), http://www.ciec.org/decision_PA/decision_text.html.

Earthlink Network Inc. v. *Cyber Promotions*, Inc. No. BC 167502 (Cal. Super. Ct. L.A. County May 7, 1997).

Reno v. *American Civil Liberties Union*, 117 S. Ct. 2329 (1997).

Ressources pertinentes

AOL's Unsolicited Bulk E-mail Policy : http://www.aol.com/info/bulkemail.html.

Acceptable Use Guidelines for Netcom Services : http://www.netcom.com/netcom/aug.html.

AT&T Web Site Agreement : http://www.att.com/terms.html#exhibit-a.

Blacklist of Internet Advertisers : http://math-www.uni-paderborn.de/~axel/BL/blacklist.html.

Bright Mail Technologies : http://www.brightlight.com/.

CAUSE : http://www.cauce.org/.

Combattez le Spamming sur Internet : http://www.cypango.net/~spam/ et http://spam.abuse.net/.

CompuServe's US and Canada Member Agreement Terms : http://support.csi.com/cshelp%5Fdocs/ sr052.htm.

Cyberspace Law Subject Index : http://host1.jmls.edu/cyber/index/index.html.

Digex Incorporated Acceptable Use Policy : http://www.access.digex.net/~policy/digex-aup.html.

IBM Service Terms : http://www.ibm.net/terms/index.html.

Infoseek (What is spamming?) : http://infoseek.go.com/AddUrl?pg=Spamming.html.

Mail Abuse Prevention System Realtime Blackhole List : http://maps.vix.com/rbl/.

MCI WorldCom Spamming Policy : http://www.wcom.com/legal/spamming/.

MISC : http://pages.hotbot.com/politics/tetsuo/fr_intro.html.

Net Abuse Links , http://www.novia.net/~doumakes/abuse/.

Junk Email Resource Page : http://www.junkemail.org/.

*news.admin.net-abuse.** *Homepage*, en date du 1er juillet 1997 : http://www.ews.uiuc.edu/~tskirvin/nana/.

Règles d'utilisation acceptable du service Sympatico du 27 août 1998 : http://www2.sympatico.ca:80/Aidez/local/bell/aup.bell.html.

Spam Free Washington! : http://www.mcnichol.com/spam.htm.

Spam-L FAQ, en date du 16 mai 1999 : http://oasis.ot.com/~dmuth/spam-l/.

Usenet II : http://www.usenet2.org/usenet/.