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

Éric LABBÉ(*)

Mémoire de Maîtrise réalisé par Éric Labbé dans le cadre de la Maîtrise "Droit des technologies de l'information" (Université de Montréal), déposé en automne 1999.

Partie II - Les prescriptions des acteurs du réseau

213. 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.

214. 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).

215. 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

216. 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.

217. 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.

218. 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

219. 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]

220. 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.

221. 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.

222. 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.

223. 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].

224. 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

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

226. 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.

227. 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].

228. 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.

229. 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 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.

230. 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.

231. 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 oeuvre d'une solution technique à une norme supplétive.

232. 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.

233. 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 oeuvre d'un système de sécurité, bien que très efficace, échappe à la définition d'une norme.

234. 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.

235. 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.

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

237. Se rapportant aux moyens mis en oeuvre 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.

238. 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.

239. 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

240. 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.

A. Le pollupostage

241. 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.

242. 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.

243. 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].

B. Le pourriel

244.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.

245. 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.

246. 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.

247. 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.

248. 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.

249. 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'oeuf 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 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

250. 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 manoeuvre assez large aux Webmestres.

251. 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].

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

253. 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.

254. 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

255. 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.

256. 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.

257. 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).

258. 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

259. 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).

A. Les stratégies des propriétaires de ressources

260. 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

261. 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.

262. 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]

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]

263. 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]

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]

264. 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 :

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.

265. 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.

266. 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.

267. 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].

268. 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 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] ».

269. 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].

270. 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

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

272. 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

273. 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.

274. 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].

275. 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.

276. 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).

277. 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

278. 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]

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

280. 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]

281. 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]

282. 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

283. 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]

284. 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.

285. 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.

286. 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.

287. Il s'en suit qu'aucune ressource Internet décentralisée ne conduit à la mise en oeuvre, 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 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

288. 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.

289. 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]

290. 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.

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

292. 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

293. 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

294. 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.

295. 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.

296. 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].

297. 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

298. 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.

299. 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).

300. 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.

301. 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.

302. 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 » 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.

303. 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.

304. 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...

305. 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 :

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]

306. 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.

307. 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]

308. 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

309. 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 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].

310. 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

311. 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.

312. 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.

313. 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 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.

314. 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 duspamming sur Internet.

315. 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

316. 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 oeuvre 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]

317. 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].

318. 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.

319. 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.

320. 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 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]

321. 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.

322. 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.

323. 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.

Conclusion

324. 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.

325. 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.

326. 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.

327. 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.

328. 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.

329. 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.

330. 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.

331. 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].

332. 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.

333. 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.

334. 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.

335. 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)

[…]

336. 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)

[…]

337. 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.

338. 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)

[…]

339. 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.

340. 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 oeuvre 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)

[…]

341. 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.

342. 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.

343. 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.

344. 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.

345. 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.

346. 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.

Notes

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

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

[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.

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

[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.

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

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

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

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

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

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

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

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

[145] Id., p. 77.

[146] Id., p. 80.

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

[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.

[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.

[156] Id., p. 85.

[157] Id., p. 87.

[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.

[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.

[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.

[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).

[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.

[172] Id., p. 92.

[173] Id., p. 181.

[174] Id., p. 180.

[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.

[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).

[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.

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

[182] Id.

[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.

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

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

[187] Id., p. 202.

[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.

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

© copyright 1995-2008 Lex Electronica Tous droits réservés / All Rights Reserved ISSN 1480-1787