DROIT & NOUVELLES TECHNOLOGIES

Présente :

LE SPAM

Par

Julia Morlec

Mémoire préparé dans le cadre de la Maîtrise de droit des affaires
de la Faculté de droit de Nantes

– programme d'échange avec l'Université d'Ottawa –

Date de mise en ligne : 03 février 2004

LE

Mémoire préparé dans le cadre de la Maîtrise de droit des affaires de la Faculté de droit de Nantes

- programme d'échange avec l'Université d'Ottawa -

Mai 2003

Plan

Introduction

« Entre le fort et le faible, c'est la liberté qui opprime et la loi qui affranchit ». Cette phrase de Lacordaire illustre assez bien la situation engendrée par le spam : d'une part on remarque un déséquilibre entre une partie forte (le spammeur) et une partie faible (l'internaute), et d'autre part on constate que jusqu'à récemment, la liberté qui a prévalu en matière de publipostage a donné lieu à de nombreux excès. Et c'est en réaction à ces abus que des législations récentes ont vu le jour, pour faire cesser les atteintes causées par la pratique du multipostage électronique.

Le terme "SPAM" est à l'origine une marque déposée de la compagnie Hormel, et n'est autre que l'acronyme de « Spiced Pork and Meat », une sorte de corned-beef qui accompagnait les soldats américains durant la dernière guerre mondiale. Il semble que les Monty Python[1] aient inspiré l'association de cet aliment avec la pratique d'envoi de courriels non sollicités. Ceux-ci, dans un de leurs célèbres sketches, se mettent à chanter "Spam Spam Spam Spam..." pour vanter les mérites du produit, de façon très répétitive et si fort que cela couvre les propos des autres protagonistes. De là donc, l'origine de l'expression " spamming " employée depuis 1993 environ pour définir l'action d'inonder les réseaux Internet avec un même message, provoquant ainsi une véritable pollution.

Aujourd'hui, de nombreuses expressions circulent sur la toile pour désigner le spam (publipostage électronique ou multipostage excessif non sollicités, spamming, pollupostage, pourriels, *junk mails* sont les plus courants), mais elles réfèrent toutes à la pratique d'envoi en masse de courriers électroniques non sollicités.

Malgré l'apparition de réglementations et d'initiatives destinées à limiter le spamming, le plus récent rapport de la CNIL concernant les communications électroniques non sollicitées[2] a montré qu'il était loin d'être en recul et que la forte mobilisation des internautes était caractéristique de la gêne causée par cette pratique :

> "[Après 3 mois de fonctionnement de la "boîte à spams" à compter du 10 juillet 2002], environ **325 000** spams ont été reçus.
> Ce chiffre démontre la mobilisation qu'a suscitée l'opération [...], les internautes trouvant enfin un relais institutionnel au problème du 'spamming' face auquel ils sont, le plus souvent, désarmés, tant d'un point de vue technique que juridique."

[1] Un groupe de 6 humoristes anglais

[2] « Opération 'boîte à spams' : les enseignements et les actions de la CNIL en matière de communications non sollicitées », rapport de la CNIL adopté le 24 Octobre 2002, disponible sur http://www.cnil.fr/thematic/docs/internet/boite_a_spam.pdf

Au vu des mesures prises dans différents pays à travers le monde et notamment en Europe, on peut se demander pourquoi le spamming perdure et n'est toujours pas neutralisé de façon efficace. L'intérêt étant de pouvoir déterminer, sur le plan juridique, quels seraient les éléments d'une réglementation vraiment efficace qui viserait à éliminer les spams.

En fait, les sociétés pratiquant le publipostage électronique trouvent beaucoup d'avantages à ce mode de prospection, et notamment un avantage économique, dans le sens où la constitution et l'envoi d'e-mails ne coûte pratiquement rien. Si les coûts de prospection sont faibles, les préjudices subis par les internautes sont substantiels lorsque les courriels en question n'ont pas été sollicités (I). C'est l'importance de ces atteintes -qui touchent notamment la vie privée des internautes et se répercutent, de façon plus pragmatique, sur le prix de leur abonnement- qui impose aujourd'hui que des garanties solides soient mises en place (II), afin de restaurer une confiance indispensable à l'épanouissement du commerce électronique, et plus largement du cyberespace.

I – Des coûts de prospection faibles contre des abus réels

Pour reprendre les mots de Lacordaire, le publipostage électronique témoigne d'une situation de déséquilibre entre un fort (le spammeur) et un faible (l'internaute qui subit le flot de courriels non sollicités). Alors que le premier peut difficilement justifier son attitude de façon légitime (A), le second est indéniablement victime de diverses atteintes à ses droits (B).

A) L'argument des « forts » : la liberté d'entreprendre

Bien que les différentes acceptions du spam varient selon les acteurs interrogés sur cette pratique, le but recherché par de tels courriels ne fait par contre aucun doute : il s'agit à l'évidence d'un moyen de prospection (1). Quant à la justification de la pratique, il semble que la liberté d'entreprendre ne soit qu'un prétexte pour masquer un mobile beaucoup plus matériel, à savoir des coûts de prospection quasi-nuls (2).

1) Le spam, différentes définitions mais un but unique de prospection

Avant d'aborder la question de la justification du spamming, celle de sa définition doit être examinée de façon liminaire car elle est en elle-même problématique.

En effet, on peut d'abord constater une **divergence entre la définition officielle et celle qu'en donnent les internautes**. Selon la Commission Nationale Informatique et Libertés (CNIL), le spam est défini par « l'envoi massif, et parfois répété, de courriers électroniques non sollicités, à des personnes avec lesquelles l'expéditeur n'a jamais eu de contact et dont il a capté l'adresse électronique de façon irrégulière ». Les critères posés pour qualifier un e-mail de spam sont donc au nombre de quatre : caractère massif, non sollicité, absence de contact antérieur avec l'expéditeur et déloyauté de la collecte. Sur ce dernier point, la collecte est qualifiée de déloyale lorsqu'elle se fait « soit au moyen de moteurs de recherche dans les espaces publics d'Internet (sites web, forums de discussion, listes de diffusion, chat…), soit que les adresses aient été cédées sans que les personnes n'en aient été informées et sans qu'elles aient été mises en mesure de s'y opposer ou d'y consentir. Une telle collecte est alors déloyale et illicite au sens de l'article 25 de la loi du 6 janvier 1978. »[3]
Les internautes quant à eux qualifient de spam tout courrier électronique non sollicité, générant des charges au détriment du destinataire et du fournisseur (cost-shifting)[4].

[3] Cf note 1

4 « Le spamming », par Me Muriel Cahen, http://www.droit-ntic.com/news/afficher.php?id=60

D'autres personnes ne considèrent que le caractère massif ou répété, sans porter attention au contenu[5]. Mais ne serait-ce que sur ce point, il est difficile de définir un seuil à partir duquel l'envoi serait considéré comme massif ; la communauté Usenet ne considère pas qu'un seul message envoyé à 20 groupes de discussion constitue un spam, alors que d'autres utilisateurs estiment même que l'envoi minimum de 5 messages comportant un contenu semblable durant une période de dix jours en constitue un. Certains auteurs ont même été jusqu'à proposer une formule de calcul permettant de qualifier un envoi de massif[6].

On trouve également **des divergences au niveau international** : alors que l'Europe par exemple, et notamment dans la directive du 12 juillet 2002, l'emphase est mise sur le caractère non sollicité (dans la directive, cela suffit à caractériser un spam[7]), aux Etats-Unis c'est le caractère déloyal ou trompeur de certaines pratiques (comme le détournement d'un filtre devant réduire les courriels non sollicités afin d'en faire un instrument destiné à collecter les adresses électroniques à l'insu des personnes) qui fonde les poursuites engagées contre les spammeurs[8]. La simple collecte, à l'insu de la personne, de son adresse électronique est légale et n'est pas considérée comme une entorse au 'fair practice principle' (sorte de principe général de loyauté)[9].

Par ailleurs, on peut encore **distinguer selon les ressources atteintes par le spam**. Dans une acception large du terme, elles sont au nombre de trois : le courrier électronique, les forums de discussion (Usenet), et les moteurs de recherche (*spamdexing*, selon l'expression du professeur E. Sorkin, auteur d'une compilation sur le droit du Cyberespace).
Dans le cas des forums, on peut encore distinguer l'Excessive Multi-posting (ou EMP : « les articles sont diffusés simultanément dans de nombreux groupes de discussion, une copie de l'article étant envoyée dans chaque groupe. Souvent, les en-têtes et les sujets de chaque article sont volontairement

---

[5] Greg BYSHENK,«I've been spammed! What do I do?» et J. D. FALKet S. SOUTHWICK, cités dans l'article d'Eric Labbé, "le spamming et son contrôle" [disponible sur http://www2.droit.umontreal.ca/~labbee/ :

« The defining characteristic of spam is volume, and volume only. The content is irrelevant ».

[6] Breidbartidex (BI) : racine carrée du nombre de groupes de discussion auxquels le message a été expédié multiplié par le nombre de messages identiques ou comportant essentiellement le même message (ibid.) :

$$\sqrt{\text{nb de newsgroup(s)}} \times \text{nb de message(s)} = \text{indice Breidbart}$$

[7] cf art.13 § 1 de la directive (a contrario) : « L'utilisation de […] courrier électronique à des fins de prospection directe ne peut être autorisée que si elle vise des abonnés ayant donné leur consentement préalable ».

8 « La Federal Trade Commission poursuit les auteurs de 'pourriels' déloyaux » de J. Le Clainche sur http://www.droitntic.com/

[9] « Courriels non sollicités : Enfin vers une application effective des sanctions ? » de J. Le Clainche, disponible sur http://www.droitntic.com/

différents afin de compliquer la tâche des volontaires qui les traquent pour les annuler » [10]), de l'Excessive Cross Posting (ou ECP : « Ce procédé consiste à diffuser un seul article simultanément dans de nombreux groupes de discussion. Cette variété d'abus est techniquement moins nocive qu'un EMP, puisqu'un seul article est diffusé et est indexé de façon à être visible dans l'ensemble des groupes cibles. » [11]).
Quant au *spamdexing*, il consiste en une indexation abusive dans les moteurs de recherche effectuée par des créateurs de sites ; « motivés par la volonté de faire connaître leurs informations, leurs créations, leurs biens ou leurs services, ces créateurs ont réussi à profiter des défaillances des robots pour hisser leurs sites au sommet du classement des moteurs de recherche »[12].

Enfin, on peut encore **différencier ces courriers non sollicités par leur contenu**. Ils peuvent en effet véhiculer des messages politique, religieux, pornographique, commercial, voire même des escroqueries (*scam*). Les contenus commerciaux et pornographiques sont de loin les plus répandus. Cependant, comme le précise Lionel Thoumyre dans son article « Emails publicitaires : tarir à la source », que le contenu du spam soit frauduleux ou pas importe peu : le spam « constitue un abus en-soi »[13].

En tous cas, quels que soient les critères retenus, on doit mettre l'emphase sur le fait que le spam est avant tout un **moyen de prospection**. Dès lors il importe surtout de déterminer les véritables causes de l'engouement pour ce media publicitaire, qui feront apparaître ou non le besoin d'une réglementation.

2) Le faux prétexte de la liberté d'entreprendre comme justification

L'entrée en vigueur de la directive du 12 juillet 2002 sur la protection des données personnelles dans le secteur des télécommunications électroniques a soulevé de vives réactions quant au système d'opt-in (voir I) B)), c'est-à-dire à l'obligation pour le prospecteur d'obtenir le consentement préalable de l'internaute avant de lui envoyer un quelconque courriel de sollicitation (par opposition à l'opt-out qui permet aux annonceurs d'expédier leur publicité jusqu'à ce que les destinataires retirent leur nom des listes de distribution).
En effet, les entreprises trouvent ce système trop exigeant, dans le sens où il ne permet plus de pondérer justement les intérêts des utilisateurs et ceux

---

[10] « La Lutte anti-spam », Eric Demeester, http://www.sasi.fr/ungi/spam.htm

[11] (id.)

[12] « Les techniques de SPAMDEXING », sur le site de l'AUDEL, société spécialisée dans le référencement, http://www.audel.fr/referencement_article_3.html

13 Lionel THOUMYRE, "Emails publicitaires : tarir à la source", Juriscom.net, décembre 1998, sur http://www.juriscom.net/int/dpt/dpt10.htm

des annonceurs[14]. C'est ainsi par exemple que Bernard Siouffi, délégué général de la Fédération des Entreprises de Vente à Distance (FEVAD), a déclaré que cette disposition « frise l'atteinte à la liberté de communiquer et à la liberté d'entreprendre [...]. Nous ne pourrons plus recruter de clients. La société de l'information et le commerce électronique en Europe vont reculer »[15]. D'autres sociétés, dont Suniles et ABS, épinglées par la CNIL en novembre 2002, invoquent une législation imprécise pour justifier leur démarche commerciale : « il n'y a pas de loi réelle sur le sujet » plaide par exemple le gérant de Suniles[16]. Enfin, d'après certaines sociétés, le spam serait un moyen écologique (car il évite l'utilisation de papier) de faire de la publicité !

En fait, il semblerait plutôt que le réel problème posé par l'opt-in pour les spammeurs est qu'il limiterait considérablement le recours à un moyen de prospection très économique (pour eux en tous cas ! voir B)) en comparaison avec les moyens traditionnels. Comme l'expliquait Jérôme Stioui dans son article "L'opt-in ? Incontournable"[17], "les modes de communication que vous citez [journaux, télévision, prospection téléphonique, etc...] n'ont pas besoin d'une réglementation aussi forte que l'e-mailing. En effet, là où les annonceurs sont naturellement limités par la barrière à l'entrée financière que représentent les coûts de création, de production, d'achat d'espace pour les grands médias, l'e-mailing [...] représente un coût quasi nul et laisse la place à tous les excès". Et en effet, alors que certaines entreprises s'imposaient, avant l'entrée en vigueur de la directive, des chartes d'opt-out exigeantes, force est de constater que la grande majorité des expéditeurs méconnaît les droits des internautes. Dans son rapport du 14 octobre 1999, « le publipostage électronique et la protection des données personnelles »[18], la CNIL décrit la forme la plus contestée de spamming comme celle qui consiste pour l'expéditeur à « falsifier ou à masquer son identité ou encore à usurper l'adresse électronique d'un tiers, afin de ne pas être identifié». Corrolaire de cette falsification : le plus souvent, ces messages n'ont pas d'adresse valide de réponse (« reply to »), et l'adresse de désinscription est inexistante ou invalide.

De plus, comme le note S. H. MUELLER, les spams sont généralement des publicités commerciales aux produits ambigus et aux services à la limite de la légalité. Par exemple, les spams sont souvent, selon lui, des publicités proposant des cures miracles ou des solutions pour devenir riche rapidement[19].

De plus, la méthode de collecte des adresses électronique montre elle aussi un manque d'égard vis-à-vis des droits des internautes : souvent celle-ci

---

14 Cf Eric Labbé, la spamming et son contrôle, id.

15 Solveig GODELUCK, " L'Europe interdit le spam ", disponible sur http://www.lageopolitiquedinternet.com/e-books/pages/e-articles_europeinterdit.htm

16 « le spam mis en examen », Estelle Dumont, disponible sur http://news.zdnet.fr/story/0,,t118-s2126800,00.html

17 Article de Jérôme Stioui, PDG de DirectiNet, disponible sur http://www.journaldunet.com/tribune/011214tribune.shtml

18 disponible sur http://www.cnil.fr/thematic/docs/publpost.pdf

19 S. H. Mueller «Fight Spam on the Internet», http://spam.abuse.net ; voir également le rapport « Boîte à spam » de la CNIL, précité, qui confirme cet état de fait.

est irrégulière, c'est-à-dire qu'elle se fait soit « au moyen de moteurs de recherche dans les espaces publics d'Internet (sites web, forums de discussion, listes de diffusion, chat, …) ; soit que les adresses [ont] été cédées sans que les personnes n'en aient été informées et sans qu'elles aient été mises en mesure de s'y opposer ou d'y consentir »[20] (ce qui est contraire, comme nous allons le voir tout de suite, à l'art. 25 de la loi du 6 janvier 1978).

Les inconvénients juridiques et techniques posés par le spam semblent donc peser plus lourd dans la balance que la liberté d'entreprendre, qui, au demeurant, n'apparaît pas être la réelle justification des spammeurs.

B) le déséquilibre initial ou la pléthore d'atteintes aux droits des « faibles »

La pratique du spamming est abusive de deux façons : d'abord sur le plan technique, principalement en ce qu'elle obstrue le réseau (a), et surtout sur le plan juridique en ce qu'elle porte atteinte à de nombreux droits des internautes (2).

1) Survol des abus techniques

Nous n'entreront pas dans le détail des répercussions techniques néfastes du spam sur le réseau, ceux-ci étant d'ailleurs bien résumés par Eric Labbée dans son article sur le spamming (précité). Principalement, la quantité de spams expédiés engorge le réseau et rend les transmissions Internet moins rapides. Un autre inconvénient est celui du coût généré par cette pratique ; s'il est quasi-nul pour les spammeurs, il en va autrement pour les fournisseurs d'accès et les utilisateurs. Les FAI doivent notamment investir dans l'augmentation de la largeur de bande afin de contrer l'augmentation de trafic sur Internet, ce qui se répercute sur le prix payé par les usagers au titre de leur abonnement. De plus, ceux-ci doivent rallonger leur temps de connexion pour lire ou à tout le moins supprimer ces messages indésirables.

En ce qui nous concerne, il nous faut surtout étudier les problèmes juridiques posés par cette pratique.

2) Les abus juridiques

Les abus juridiques sont nombreux, et c'est l'un des aspects problématiques dans la lutte contre le spamming. En effet, ce phénomène touche divers pans du droit assez disparates, ce qui ne crée qu'une complication supplémentaire lorsqu'il faut aborder la question de la réglementation du phénomène (a). Malgré tout, le terrain de la protection de la vie privée paraît émerger comme étant le plus apte à prémunir les internautes des inconvénients de cette pratique (b).

a) Une législation éclatée

[20] Rapport de la CNIL opération « Boîte à spams » précité.

Le premier problème posé lorsqu'on cherche un recours juridique pour contrer le spam n'est pas tant l'absence de texte spécifique (ce qui est le cas au Canada, mais plus en Europe depuis la directive du 12 juillet 2002), mais surtout la multitude de régimes juridiques possiblement applicables.

Ainsi, les jurisprudences française et canadienne ont fait référence à la responsabilité contractuelle pour condamner des spammeurs[21]. Plus précisément, les tribunaux ont validé la décision de fournisseurs d'accès de résilier les abonnements de personnes se connectant à Internet par leur service pour envoyer massivement du spam, en faisant entrer la netiquette dans le champ contractuel. En France, c'est sur le fondement des articles 1135 et 1184 du code civil que le TGI de Rochefort sur mer a affirmé que la netiquette constitue un usage source du droit, et ainsi « s'impose à celui qui se livre à une activité entrant dans son champ d'application ». C'est sur des principes similaires que la Cour Supérieure Ontarienne a tranché dans l'affaire Nexx.

D'autres régmes, bien qu'ils n'aient pas été consacrés par la jurisprudence, sont potentiellement applicables à la lutte contre le spam. En France comme au Canada par exemple, le droit de la protection du consommateur et de la concurrence s'appliquent dans une certaine mesure au spam, si celui-ci contient de la publicité trompeuse[22].

Toujours au Canada, le CRTC (Conseil de la radiodiffusion et de la télécommunication canadienne) dispose, en vertu de la loi sur les télécommunications, de nombreux pouvoirs qu'il pourrait exercer pour encadrer le spam. Le plus évident est celui qui lui est conféré par l'article 41 de cette loi, qui lui permet d'interdire ou de réglementer par ordonnance, « dans la mesure qu'il juge nécessaire -- compte tenu de la liberté d'expression -- pour prévenir tous inconvénients anormaux, l'utilisation par qui que ce soit des installations de télécommunication de l'entreprise canadienne en vue de la fourniture de télécommunications non sollicitées ».

Egalement, les dispositions sur la fraude pourraient être invoquées. En France, c'est la Loi du 5 Janvier 1988 dite loi Godefrain, concernant la sécurité des systèmes de traitement automatisés de données (STAD), condamne le fait d'accéder et de se maintenir frauduleusement dans un STAD. Ce régime, codifié aux articles 323-1 à 323-7 du Code Pénal, recouvre deux hypothèses lorsqu'on l'applique au spam. Soit l'envoi d'un ombre excessif de courriels finit par saturer la messagerie électronique qui se bloque : l'entrave au fonctionnement d'un STAD est alors caractérisée ; soit le spammeur prend le contrôle de l'ordinateur d'un tiers, ce qui lui permet d'envoyer des courriels sans être identifié. Cette deuxième possibilité a été évoquée, mais non retenue en l'espèce, dans l'affaire kitetoa.com contre Tati[23]. Cela est

---

[21] TGI Rochefort sur mer , 28 février 2001, disponible sur http://www.juriscom.net/txt/jurisfr/cti/tgirochefortsurmer20010228.pdf ; TGI de Paris, ord réf 15 janvier 2002, disponible sur http://www.juriscom.net/txt/jurisfr/cti/tgiparis20020115.pdf ; au Canada : « affaire Nexx », 1267623 Ontario Inc. et al. v. **NEXX** Online, Inc. (1999), 45 OR (3d) 40.

[22] on se reportera aux articles L.121-1 et s. du code de la consommation en France, aux articles 52 et 74.01 de la loi canadienne sur la concurrence et aux articles 218 et 219 de la loi québécoise sur la protection du consommateur.

[23] CA Paris, 30 oct 2002, disponible sur http://www.kitetoa.com/Pages/Textes/Les_Dossiers/Tati_versus_Kitetoa/arret-cour-appel.shtml

notamment rendu possible par l'utilisation d'un petit logiciel appelé « Cheval de Troie » : celui-ci s'installe automatiquement dans le système d'exploitation de la victime et permet au pirate de le retrouver à chaque connexion afin de prendre le contrôle de son ordinateur. Des dispositions similaires sur la fraude existent au Canada : est qualifié de vol le fait qu'une personne, frauduleusement, malicieusement ou sans apparence de droit, soit se serve d'installations, soit obtienne un service en matière de télécommunication (art. 326 (1) du code criminel) ; le fait d'accéder ou d'utiliser un ordinateur de façon non autorisée est puni à l'art. 342.1 (1) de ce même code.

D'autres dispositions pénales peuvent aussi être invoquées dans le cas de mails pornographiques. En France il s'agira de l'article L.227-24 du code pénal sur la protection des mineurs[24], et au Canada les art. 163 (1) et (8) du code criminel sur le contenu obscène, et 163.1 (2) et (3) sur la pornographie juvénile.

Enfin, deux affaires américaines ont encore utilisé d'autres pans du droit pour condamner le spamming. La première affaire est l'affaire AOL v. CN roductions, Inc.[25], dans laquelle une unité d'AOL Time Warner avait porté plainte contre la société de marketing direct pour envoies massifs de spam sur 25 % de sa base de membre. Un an plus tard, le FAI avait obtenu gain de cause, CN Production ayant reçu une injonction du tribunal de Virginie de cesser ses activités de spamming. Ce tribunal s'est basé pour cela sur le droit des marques de commerce : le fait pour CN Production d'utiliser une adresse AOL créait de la confusion dans le sens où le public aurait pu être porté à croire qu'AOL avait un lien quelconque avec cette société émettrice des spams[26]. L'autre affaire a traité le problème sur le terrain du droit de propriété (notion de « trespass to chattels » : violation du droit de propriété sur un bien meuble)[27]. Cette notion a évolué et inclut aujourd'hui l'utilisation non autorisée de la propriété d'autrui ; si celle-ci cause un dommage matériel, quant à la qualité ou à la valeur du bien, au propriétaire, l'auteur de ce dommage sera responsable pour la perte ainsi causée. En l'espèce, le volume substantiel de courriels reçus par Compuserve lui a causé un tel préjudice puisque leurs serveurs ont été dans l'obligation de stocker des courriels dont la plupart ne pouvaient être distribués et ont du travailler en vain pour les retourner à des expéditeurs dont l'adresse était erronée, les spammeurs ayant

[24] **Article 227-24 :** Le fait soit de fabriquer, de transporter, de diffuser par quelque moyen que ce soit et quel qu'en soit le support un message à caractère violent ou pornographique ou de nature à porter gravement atteinte à la dignité humaine, soit de faire commerce d'un tel message, est puni de trois ans d'emprisonnement et de 75000 euros d'amende lorsque ce message est susceptible d'être vu ou perçu par un mineur.
Lorsque les infractions prévues au présent article sont soumises par la voie de la presse écrite ou audiovisuelle, les dispositions particulières des lois qui régissent ces matières sont applicables en ce qui concerne la détermination des personnes responsables.

[25] Civil Action N°. 98-552-A (E.D. Va. 1998)

[26] « Defendants' use of the aol.com domain name caused AOL Members to believe that AOL was connected to, affiliated with, approved of , or condoned Defendants' transmission of the adult entertainment products and services advertised in their messages ».

[27] Compuserve Incorporated v. Cyber Promotions Inc., 962 F. Supp. 1015 (S.D. Ohio 1997)

dissimulé leur adresse[28]. L'atteinte au droit de propriété sur les serveurs du FAI était ainsi caractérisée.

Bien que tous ces régimes soient potentiellement applicables, le plus efficace et sans doute le plus évident est celui de la protection de la vie privée.

b) La pierre angulaire : la protection de la vie privée

Dans son rapport « opération boîte à spams » de 2002, la CNIL se félicitait de « l'utilisation des dispositions de la loi informatique et libertés du 6 janvier 1978 comme outil de lutte contre le spam. Cette loi, ainsi que les lois canadiennes[29] dont nous parlerons plus loin, concernent la protection des données personnelles ou nominatives, au nombre desquelles figure l'adresse e-mail. Au Québec, l'art. 2 de la loi sur la protection des renseignements personnels dispose qu 'est un renseignement personnel, "tout renseignement qui concerne une personne physique et permet de l'identifier". En France, la CNIL a précisé dans son rapport de 1999[30] qu' une "adresse électronique est évidemment une information nominative : directement lorsque le nom de l'internaute figure dans le libellé de l'adresse ; en tout état de cause, toujours indirectement nominative dans la mesure où toute adresse électronique est associée à un nom et à une adresse physique. De surcroît, à la différence d'autres catégories de données personnelles (numéro de téléphone, plaque minéralogique, etc.), une adresse électronique fournit dans bien des cas de nombreux renseignements sur la personne : son nom, son lieu de travail, son fournisseur de messagerie ou son fournisseur d'accès, son pays d'établissement, etc". Il s'agit donc d'une donnée sensible qu'il faut protéger.

La CNIL a donc mené, sur la base de la loi de 1978, une série de cinq dénonciations au Parquet : selon elle, le spam viole la loi sur au moins trois points. D'abord, il contrevient à son article 25 qui dispose que « la collecte de données opérée par tout moyen frauduleux, déloyal ou illicite est interdite ». La collecte d'adresses e-mail figurant dans les espaces publics d'Internet à l'insu des internautes est donc illicite. Deuxièmement, les entreprises en question ne permettent pas un usage effectif du droit d'opposition, pourtant imposé par l'article 26 de cette même loi. Ces deux pratiques sont visées par l'art. L. 226-18 du Code pénal, qui prévoit que « le fait de collecter des données par un moyen frauduleux, déloyal ou illicite, ou de procéder à un traitement d'informations nominatives malgré l'opposition de la personne,

---

[28] « Handling the enormous volume of mass mailings that Compuserve receives places a tremendous burden on its equipment. Defendants' more recent pratice of evading Compuserve's filters by disguising the origin of their messages commandeers even more computer resources because Compuserve's computers are forced to store undeliverable e-mail messages and labor in vain to return the messages to an address that does not exist. »

[29] Loi fédérale sur la protection des renseignements personnels et les documents électroniques (2000, ch. 5), disponible notamment sur http://lois.justice.gc.ca/fr/P-8.6/texte.html
& Loi québécoise sur la protection des renseignements personnels dans le secteur privé (L.R.Q., c. P-39.1), disponible sur http://www.cai.gouv.qc.ca/fra/docu/loiprive.pdf

[30] précité, voir note 15

lorsque cette opposition est fondée sur des raisons légitimes, est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende ». Enfin, « la constitution et l'utilisation de traitements automatisés d'informations nominatives doivent, préalablement à leur mise en œuvre, faire l'objet d'une déclaration à la Commission nationale de l'informatique et des liberté, conformément à l'article 16 de la loi du 6 janvier 1978. […]Tout manquement à cette obligation est sanctionné par l'article 226-16 du Code pénal ».

Mais la loi de 1978 n'est pas le seul texte auxquels doivent se conformer les entreprises qui désirent faire de la prospection. Ainsi, la directive européenne du 24 octobre 1995 relative à la protection des données personnelles pose cinq principes concernant la collecte de ces données en général (et pas spécifiquement dans le cadre de la prospection électronique). Il s'agit des principes de finalité de la collecte (celles-ci doivent être « déterminées, explicites et légitimes » et ceci est valable pour un traitement ultérieur des données), de légitimité du traitement (la personne a indubitablement consenti au traitement), de loyauté de la collecte (les données doivent être traitées loyalement et licitement), d'information des personnes (en cas de collecte directe : les personnes doivent être informées de la finalité de celle-ci, des destinataires des informations, de l'existence d'un droit d'accès et de rectification, etc… et en cas de collecte indirecte : la personne doit être informée de la collecte dès l'enregistrement des données par le responsable du traitement), et enfin du droit d'opposition (au traitement des données et à leur utilisation par des tiers).

On le voit, la loi de 1978 et la directive de 1995 règlent les cas de prospection dans lesquels la collecte des adresses de courriel a eu lieu directement (c'est-à-dire que la personne est cliente ou visiteur du site qui collecte ses données) ou indirectement (à partir de listes d'e-mails fournies par des tiers à la société de prospection). Dans ces deux cas, si la société est déclarée auprès de la CNIL et qu'elle permet un droit d'opposition effectif (cela permet notamment aux annonceurs d'expédier leur publicité jusqu'à ce que les destinataires retirent leur nom des listes de distribution), la garantie d'une information préalable de la personne concernée, lors de la collecte *initiale* des données, la mettant en mesure de s'opposer dès la collecte et en ligne, par l'intermédiaire d'une case à cocher, à la réception de tout message commercial, est jugée suffisante. Dans ces deux cas donc, l'internaute, "informé de son droit d'opposition et qui ne l'a pas exercé, est *présumé* avoir consenti à recevoir des communications commerciales de la part de l'organisme auquel il avait fourni son e-mail"[31]. La seule question restée en ouverte était celle de la collecte « sauvage » des adresses e-mails, dans les espaces publics d'internet. Le mécanisme de droit d'opposition (« opt-out ») était-il suffisant ou un mécanisme renforcé (« opt-in ») devait-il être prévu ?

C'est cette question qu'a tranchée la directive vie privée et communications électroniques du 12 juillet 2002, en imposant à son article 13 que l'utilisation de « courrier électronique à des fins de prospection directe ne peut être autorisée que si elle vise des abonnés ayant donné leur

[31] rapport CNIL "boîte à spams" précité.

consentement préalable ». Il s'agit donc ici d'un mécanisme d'opt-in (voir définition plus haut). Comme nous l'avons dit, cette décision d'imposer l'opt-in n'a pas été accueillie favorablement par certains commerçants. Pourtant, l'imposition d'obtenir un consentement *a priori* pour recevoir des courriels de sollicitation ne concerne que les collectes dans les espaces publics, ce qui se comprend puisque le destinataire du courrier n'a strictement aucune relation avec l'expéditeur, (contrairement aux deux autres cas mentionnés au-dessus). Il s'agit donc d'un régime mixte, parfois appelé "soft opt-in", qui constitue, selon nous, un bon compromis entre les intérêts des acteurs du commerce électronique. Cette directive devrait être transposée en droit français avant le 31 octobre 2003, et on peut d'ailleurs d'ores et déjà constater l'adoption de ce régime de soft "opt-in" dans l'art. 12[32] du projet de loi pour la confiance dans l'économie numérique [33].

Au Canada, la question du consentement à l'envoi de courriels de prospection électronique n'est abordée dans aucun texte. Cependant, on retrouve des dispositions similaires à la directive de 1995 quant à la protection des renseignements personnels et plus particulièrement quant à la collecte de données nominatives dans une loi fédérale et une loi québécoise[34] (pour le secteur privé)[35]. On y retrouve notamment les principes de finalité[36], de consentement à la collecte de données et à la transmission de ces données à des tiers[37], de licéité dans les moyens utilisés pour la collecte[38] ; des mesures de sécurité doivent être prises pour protéger les renseignements et empêcher

---

[32] **Article 12** du projet de loi pour la confiance dans l'économie numérique :
I. - L'article L. 33-4-1 du code des postes et télécommunications est remplacé par les dispositions suivantes : (voir page suivante)
« *Art. L. 33-4-1*. - Est interdite la prospection directe, au moyen d'automates d'appel, télécopieurs et courriers électroniques, de toute personne qui n'a pas exprimé son consentement préalable à recevoir de tels appels ou courriers électroniques.

« Par dérogation aux dispositions du premier alinéa, la prospection directe par courrier électronique est autorisée si les coordonnées électroniques du destinataire ont été recueillies directement auprès de lui, dans le respect des dispositions de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, à l'occasion d'une vente ou d'une prestation de service, si la prospection directe concerne des produits ou services analogues à ceux antérieurement fournis par la même personne, et si le destinataire se voit offrir, de manière expresse et dénuée d'ambiguïté, la possibilité de s'opposer, sans frais et de manière simple, à l'utilisation de ses coordonnées électroniques lorsque celles-ci sont recueillies et chaque fois qu'un courrier électronique de prospection lui est adressé."

[33] Le projet de loi est disponible sur http://www.telecom.gouv.fr/internet/index_len.htm
[34] Précitées, voir note 25
[35] En effet il existe aussi des lois spécifiques à la protection des renseignements personnels dans le secteur public.
[36] art. 4.2 de l'annexe 1 de la loi fédérale, art 5 de la loi québécoise
[37] art. 4.3 de l'annexe 1 de la loi fédérale, art 6 et surtout 12 à 15 de la loi québécoise
[38] art. 4.4 de l'annexe 1 de la loi fédérale, art 5 al. 2 de la loi québécoise

toute utilisation ou communication non autorisée[39], un droit d'accès et de rectification est également prévu[40], etc…

Ainsi, les normes sur la protection des renseignements personnels semblent constituer une arme efficace contre les atteintes à la vie privée et plus largement aux droits des internautes. Cependant, cette solution est en fait loin d'être satisfaisante, notamment en raison du caractère étatique des lois en question ; une réponse forte et surtout adaptée au cyberespace serait donc la seule garantie des internautes face à l'abus réel que constitue cette pratique.

[39] art. 4.7 de l'annexe 1 de la loi fédérale, art 10 de la loi québécoise
[40] art. 4.9 de l'annexe 1 de la loi fédérale, art 29 et 30 notamment de la loi québécoise

II – Des abus nécessitant de fortes garanties

En réaction aux nombreuses atteintes portées aux droits des internautes, diverses initiatives ont été prises pour tenter de contrebalancer ces abus par de fortes garanties. Les solutions actuelles ne semblent malheureusement pas très adaptées aux contraintes imposées par le spamming (A). Face à ce constat, une solution à deux volets semble aujourd'hui s'imposer comme la meilleure arme contre le phénomène (B).

A) Les limites posées par les solutions actuelles

Les limites posées par les solutions actuelles sont de deux ordre : d'une part, les législations actuelles sont nationales, ce qui apparaît rapidement problématique lorsqu'un litige présente un élément d'extranéité (1) ; d'autre part, bien que nombreuses initiatives aient été prises par les internautes eux-mêmes, celles-ci souffrent d'un manque de légitimité et sont donc peu effectives pour réduire le spam (2).

1) L'inadaptation des normes actuelles, réactions étatiques à un problème international

Malgré l'apparente efficacité des réglementations en matière de renseignements personnels, le problème du spamming reste en grande partie irrésolu (du moins en Europe) du fait qu'une majorité des courriels non sollicités vient de pays de langue anglaise (84.8% d'après les chiffres de la CNIL), et notamment des Etats-Unis. Or il n'existe aujourd'hui aucune réglementation internationale permettant de contrer ce phénomène par nature supranational. On pourrait donc penser que le recours aux règles du droit international privé pallierait cette inadaptation des normes au cyberespace, par nature international. Pourtant, les règles régissant la compétence des tribunaux ainsi que l'exécution des jugements étrangers, et surtout leur application ont montré que même à ce niveau, une grande incertitude règne encore. L'affaire Yahoo! en est l'exemple le plus représentatif.

En l'espèce, des objets nazis avaient été mis en vente sur le site de vente aux enchères , hébergé aux Etats-Unis, "yahoo.com". Trois associations[41], ont alors demandé à *Yahoo! Inc.* de faire cesser toute mise à disposition sur le territoire français à partir de son site « Yahoo.com » de ces objets. Les tribunaux français, après avoir relevé « *que l'exposition en vue de leur vente d'objets nazis constitue une contravention à la loi française (article R 645-2 du Code pénal) mais plus encore une offense à la mémoire collective du pays* », ont considéré que leur juridiction était compétente pour connaître du litige. Il ont donc ordonné à Yahoo! Inc. de rendre impossible l'accès aux pages où

[41] la LICRA (Ligue Internationale contre le Racisme et l'Antisémitisme) et l'UEJF (Union des Etudiants Juifs de France), rejoints par la suite par le MRAP (Mouvement contre le Racisme, l'Antisémitisme et pour la paix)

figuraient les objets en question. Peu de temps après, Yahoo! décidait de retirer volontairement ces objets de son site d'enchères en ligne, mais s'adressait à un tribunal californien pour déterminer si un jugement prononcé par un tribunal français avait force de loi aux États-Unis. Celui-ci décida que le jugement français ne pouvait être exécuté, au motif que si l'affaire avait été jugée aux Etats-Unis, des principes de droit différents auraient été appliqués, et plus précisément la vente de tels objets aurait été tolérée car protégée par le premier amendement, qui garantit la liberté d'expression :

> "Bien que la France ait le droit souverain de réglementer le discours permissible en France, ce tribunal ne peut faire appliquer une ordonnance venant de l'étranger qui viole les garanties constitutionnelles des États-Unis en tentant de bâillonner la liberté d'expression à l'intérieur de nos frontières."

Dès lors, on peut s'interroger sur l'effectivité des décisions concernant le cyberespace qui comportent un élément d'extranéité, et qui font appel à des réglementations juridiques très variables selon les pays, comme en l'espèce. Cela est d'autant plus vrai en ce qui concerne le spam, car les réponses des Etats varient énormément dans le monde. Ainsi, aux Etats-Unis, certains Etats ont adopté des lois anti-spam qui sanctionnent pénalement la communication de courriels non sollicités par leur destinataires[42], alors qu'au Canada, il n'existe comme nous l'avons dit aucune loi spécifique, et la seule sanction ayant jamais été prise est celle de l'affaire NEXX, et était une sanction civile. De plus, alors qu'aux Etats-Unis la plupart des législations s'orientent vers un système d'opt-out[43], la directive européenne de juillet 2002 posait le principe de l'opt-in. Dans ces conditions, on peut donc douter, si les principes de l'affaire Yahoo! sont appliqués, que des litiges comportant un élément d'extranéité soient rendus exécutoires dans les pays d'origine du spammeur. Il serait donc souhaitable, comme nous le verrons plus tard, que le spam soit réglementé de façon internationale qu'un contrôle réel et efficace du phénomène puisse être exercé.

Malheureusement, la grande disparité des législations étatiques actuelles, en plus d'empêcher l'exécution des décisions comportant un élément d'extranéité, ne faciliterait pas une harmonisation des normes en matière de spamming, dans le cas où elle serait décidée.

Face à ce constat, les internautes ont réagi, notamment par le biais des codes de conduite, pour tenter de résoudre par eux-mêmes ce problème.

2) L'absence de force obligatoire des codes de conduite

L'un des premiers types d'action des acteurs d'Internet (Internautes, associations de professionnels, fournisseurs de services Internet, etc…) contre le

---

[42] notamment les lois des Etats de Washington, de Californie et du Nevada. Cf rapport CNIL sur le publipostage électronique, précité.

[43] Thibault Verbiest, "*Spamming : les Etats-Unis se dirigent vers l'opt-out*", 2 Janvier 2002, disponible sur http://www.droit-technologie.org/1_2.asp?actu_id=500

spam, a été l'édiction de codes de déontologies (ou codes de conduite) : il s'agit d'un ensemble de règles juridiques et morales auxquelles des personnes exerçant certaines activités publiques ou privées s'imposent entre elles. De tels codes paraissent avantageux, puisqu'ils permettent de passer outre les problèmes d'extranéité dont nous avons parlé plus haut, mais aussi parce qu'en théorie, ils empêchent l'action du législateur, dans les cas où celle-ci n'est pas absolument nécessaire[44]. Au Canada par exemple, l'Association canadienne de marketing (ACM) a établi pour ses membres un code de déontologie et des normes de pratique[45] pour la distribution de matériel promotionel par Internet. En vertu de ce code, les agents de marketing doivent offrir aux destinataires de matériel le choix d'indiquer qu'ils ne veulent plus recevoir d'autres communications de ces agents. En cas de non respect du code, l'agent de marketing est expulsé de l'Association. Un autre exemple est celui de l'association canadienne des fournisseurs Internet (ACFI), qui a également élaboré un code de conduite volontaire[46], fondé sur les meilleures pratiques de ses membres. Les FAI sont libres d'établir leurs propres contraintes d'usage et de les faire appliquer par des contrats. Selon l'ACFI, la vaste majorité des FAI membres de l'association interdisent déjà l'utilisation de leur réseau pour l'envoi de courrier électronique en vrac et se réservent le droit de fermer le compte des abonnés qui se livrent à cette activité.

En Europe, il existe également de telles initiatives ; par exemple, le Syndicat national de la communication directe (SNCD), qui regroupe en son sein soixante-dix acteurs du marketing direct, dont plusieurs sociétés Internet (AOL, Wanadoo Data, Maximiles, Pointop, Net2One, …) a adopté un code déontologie[47] de l'e-mailing[48]. La Ligue Internationale pour le droit de la concurrence (LIDC)[49] a elle aussi adopté un code de conduite pour une saine concurrence dans le commerce électronique[50], dans lequel elle condamne l'envoi de courriels de prospection sans le consentement du destinataire[51].

---

[44] Au Canada cependant, cet incitatif s'est retourné contre l'Association Canadienne de Normalisation qui avait édicté un *Code type sur la protection des renseignements personnels*, puisque celui-ci a été intégralement repris dans la loi fédérale sur la protection des renseignements personnels et les documents électroniques, précitée (voir son annexe 1).

[45] disponible sur http://www.the-cma.org/french/ethics_1.cfm

[46] disponible sur http://www.caip.ca/issues/images/FairPra-FR-p.pdf

[47] disponible sur http://www.sncd.org/deontologie/docs/deontologie-emailing.pdf

[48] voir l'article " Un code de bonne conduite contre le spam" de Karine Solovieff, du 05/12/2001 disponible sur http://www.01net.com/article/170135.html

[49] la LIDC est une association scientifique internationale indépendante, qui a notamment pour but de "de promouvoir la concurrence libre, saine et honnête […], d'étudier les législations, de les comparer et de faire toutes propositions sur les problèmes de concurrence qui se posent tant dans les relations internationales que sur le plan strictement national […] et de défendre et de rechercher les moyens d'assurer la liberté de l'entreprise et du commerce".
Pour plus d'informations voir leur site : http://www.ligue.org

[50] "Code of conduct in regard to fair competition in electronic commerce", disponible sur http://www.uni-muenster.de/Jura.itm/netlaw/itmccode.html

[51] voir l'article II)1. : "No person should initiate the transmission, conspire with another to initiate the transmission or assist the transmission of a commercial electronic mail message unless the sender knows or has substantial reason to know that he uses the addressee's electronic mail address with the permission of the addressee."

Mais les associations d'internautes proposent aussi d'autres moyens de lutte contre le spam. C'est ainsi que le livre blanc de l'Observatoire du mail[52] préconise la mise en place d'un système de marquage électronique des e-mails envoyés en nombre qui permettra la mise en place d'un filtrage légal. Ce dispositif prévoit l'identification de l'expéditeur et de l'objet des messages envoyés en nombre. "Les critères d'identification et de tri seraient d'ordre technique et formel : adresse valide d'expédition, identité de l'annonceur, présentation de l'objet du message, poids du message et, le cas échéant, des pièces jointes, […] etc. Les messages respectant ces critères seraient réputés " distribuables ". Ils pourraient être marqués électroniquement pour permettre un traitement automatisé par les fournisseurs d'accès et de messageries"[53]. L'Observatoire propose aussi l'application aux spammeurs du fameux principe "pollueur-payeur", qui consisterait à faire supporter les coûts techniques du spam à leurs expéditeurs, ce qui leur rendrait la pratique beaucoup moins rentable[54].

Enfin, dans le même ordre d'idées, on doit citer l'action d'Euro-CAUCE (branche européenne de l'association américaine "Coalition Against Unsolicited Commercial E-mail"), une organisation non gouvernementale regroupant des associations représentatives d'internautes, qui avait lancé une pétition contre le spamming. Celle-ci était destinée à être adressée aux députés des Parlements européen et allemand, afin de préciser la directive de 1995 sur la protection des données personnelles. Car d'après leurs constatations, ni les solutions techniques (celles dont nous parlerons plus loin – voir B)), ni les tentatives d'auto-régulation du publipostage électronique n'ont réussi à enrayer le spam. Et c'est bien là mettre l'accent sur l'inconvénient majeur des codes de conduite et autres propositions faites par les acteurs de l'Internet : aucune de ces normes n'a de force obligatoire, et celles-ci ne contraignent que ceux qui veulent bien s'y soumettre. Ce n'est bien évidemment pas le cas des spammeurs, qui font bien peu de cas de tels codes d'éthiques, et qui altèrent ainsi la confiance des internautes pourtant nécessaire à l'épanouissement du commerce électronique. L'auto-régulation n'est donc pas suffisante, au vu de ces considérations, à enrayer le phénomène.

Les solutions actuelles en matière de réglementation du spam apparaissent donc comme insuffisantes pour enrayer efficacement le phénomène. C'est en se basant sur ce constat que la CNIL, dans son rapport le plus récent sur le spam, a suggéré une "double réponse" au spam, à la fois technique et juridique, pour donner le moins de chances possibles aux spammeurs d'arriver à leurs fins.

---

[52] fondé par deux associations : l'ACSEL (Association pour le Commerce et les Service en Ligne) et l'IREPP (Institut de Recherches et Prospective Postales) ; le livre blanc est intitulé "Mille milliards d'e-mails" ; voir le site http://www.observatoiredumail.com

[53] voir le communiqué de presse de l'ACSEL de septembre 2002 disponible sur http://www.acsel.asso.fr/acsel/actions/communiques/2002_septembre.htm

[54] voir également à ce sujet l'article "L'opt-in ? Incontournable", de Jérôme Stioui, PDG de DirectiNet, disponible sur précité note 15.

B) Vers une solution à deux volets

1) Le volet technique et pédagogique

Selon la CNIL, la volet pédagogique devrait permettre aux internautes "de saisir les principales caractéristiques du phénomène du "spamming" et leur fournir les moyens de s'en protéger". Ce volet comprend donc des éléments d'information du public à la fois pratiques (définition du spam, les méthodes de collecte, etc…), juridiques (son caractère illégal et les armes juridiques disponibles pour s'en prémunir) et technique (les moyens technologiques de s'en protéger). Nous ne nous étendrons pas sur cet aspect qui n'entre pas précisément dans l'objet de notre étude.

Pour résumer, les solutions techniques consistent en des logiciels de filtrage (à installer par l'internaute ou inclus dans son logiciel de courrier faire son fournisseur de services Internet, comme c'est la cas pour Yahoo! ou Hotmail par exemple ; on peut par exemple mettre en place un système de "white list", c'est-à-dire n'accepter que les courriels dont l'adresse de l'expéditeur nous est connue), la possibilité de bloquer certaines adresses (comme cela est possible sur AOL notamment), voire d'inscrire l'adresse d'un spammeur notoire à une "black list" sur Internet, comme celle tenue par CASPAM[55], afin d'enclencher de la part de la communauté des internautes un effet de "boycott[…] des commerces et services des entreprises ou organismes qui font du mass mailing (envoi d'e-mails non sollicités en masse)", comme le précise cette association. Il est également possible de déjouer la plupart des logiciels "extracteurs" d'adresses mél lors de la participation à des groupes de discussion "en remplaçant l'arobase (@) de l'adresse mél par "at" dans la mesure où la plupart des "extracteurs" de mél ne sont pas en mesure de les repérer. Une autre méthode consiste à écrire son adresse mél de la manière suivante : nom@domaine.fr-enlevercette partie"[56]. Enfin il est également possible de crypter[57] l'adresse mél de notre page personnelle, afin que les spammeurs ne puissent plus la détecter grâce à leurs logiciels "aspirateurs", mais que les internautes qui voudront nous écrire pourront toujours voir[58].

2) Le volet juridique : éléments pour des normes efficaces

Nous l'avons vu, les solutions actuelles présentent toutes des caractéristiques qui freinent l'efficacité de la lutte contre le spamming. Nous proposons donc ici d'établir les éléments qui permettraient, sur le plan juridique, une réglementation adaptée au phénomène.

---

[55] Collectif Anti SPAM, dont le site web est à l'adresse suivante : http://caspam.org/
[56] recommandations de la CNIL sur sa page "les solutions techniques" : http://www.cnil.fr/thematic/internet/spam/lacnil_aide4.htm
[57] un guide d'encryption est fourni par la CNIL à l'adresse http://www.cnil.fr/thematic/internet/spam/lacnil_aide4_3.htm
[58] cf note 51

D'abord, la réglementation devrait être internationale, ou à tout le moins permettre une application effective des jugements comportant un élément d'extranéité. Pour cela, une harmonisation des normes en matière de spamming serait, comme nous l'avons montré, nécessaire. Ou alors on pourrait penser à mettre en place, comme c'est le cas actuellement pour les prolbèmes de cybersquatting, des modes de règlement alternatifs des différends. En l'espèce, les centres d'arbitrage en question appliquent un texte spécifique, l'UDRP (Uniform Dispute Resolution Policy ou "Principes directeurs régissant le règlement uniforme des litiges relatifs aux noms de domaine"), qui définit précisément quand un cas de cybersquatting est caractérisé, et les sanctions qui peuvent être prises par la juridiction alternative lorsqu'un tel cas est constaté[59], ce qui résout les problèmes de loi applicable, de compétence de juridiction et d'exécution du jugement habituellement posés. De plus, de tels systèmes ont d'autres avantages comme la rapidité de la procédure, des coûts peu élevés, et paraissent donc de ce fait plus adaptés aux cyberespace.

Une réglementation efficace du cybersquatting devrait également être, comme nous l'avons dit aussi, de force obligatoire, au vu des atteintes constantes portées aux droits des internautes. Malgré l'existence de la Netiquette et de nombreux codes de conduite, le spam continue toujours, et même de plus en plus à encombrer les boîtes aux lettres des internautes. Il faudrait donc une réglementation plus contraignante vis à vis des spammeurs pour observer une quelconque amélioration. Ce caractère obligatoire pourrait être obtenu soit par jugement (comme ceux basés sur la Netiquette par exemple), soit par un traité international, soit par un mécanisme "d'arbitrage obligatoire" comme celui qui existe pour le cybersquatting. En effet là encore, le mécanisme prévu paraît judicieux et adapté à l'Internet. D'une part, cette procédure d'arbitrage est rendue obligatoire à tous les déposants de noms de domaines génériques par la présence d'une clause d'acceptation dans le contrat d'enregistrement[60]. Une clause similaire pourrait être insérée par les fournisseurs de service Internet dans les contrats d'abonnement qu'ils offrent à leurs clients, de sorte que tout spammeur se verrait automatiquement soumis à une procédure d'arbitrage. D'autre part, dans la procédure UDRP, la procédure arbitrale n'est pas exclusive de recours devant les tribunaux classiques : appliqué au spamming, ce principe donnerait une garantie supplémentaire quant à la force exécutoire de la décision.

En dernier lieu, nous pensons qu'une bonne réglementation devrait intégrer, d'une façon ou d'une autre, le point de vue des acteurs du cyberespace, à savoir les internautes, les commerçants électroniques, les associations, etc… Cela permettrait de mieux adapter cette réglementation aux réalités du commerce électronique et plus largement du cyberespace, et d'éviter que des décisions contestables ne soient rendues à cause d'une

---

[59] l'UDRP est disponible en français sur http://arbiter.wipo.int/domains/rules/icann/icannpolicy-fr.pdf ; pour plus d'informations, vous pouvez vous reporter à mon mémoire sur le cybersquatting, téléchargeable à l'adresse suivante : http://morzelech.free.fr/droit/Publications%20droit.htm

[60] article 4 de l'UDRP

mauvaise connaissance du média Internet[61]. Si l'on garde l'idée d'une juridiction d'arbitrage spécifique, cela pourrait se faire par l'introduction de l'échevinage dans le panel d'experts chargés de trancher le litige : un juge professionnel serait présent pour s'assurer de l'application rigoureuse des textes et un commerçant ou un représentant d'une association (un membre du CASPAM par exemple ou de l'ACSEL) pour représenter selon les cas les intérêts des internautes et/ou des commerçants. Plus classiquement, le point de vue des acteurs d'Internet pourrait être recueilli par leur consultation avant l'édiction de textes, de rapports, de toute réglementation touchant le spam, comme le font déjà la CNIL (voir dans le rapport sur le publipostage électronique la partie intitulée "les positions des acteurs concernés et des organismes et associations représentatifs"), et le CRTC[62] (comme il l'a fait par exemple pour l'élaboration de son rapport sur les nouveaux médias[63]).

Rappelons pour conclure l'art. 12 de la Déclaration Universelle des Droits de l'Homme :

> "Nul ne sera l'objet d'immixtions dans sa vie privée, sa famille, son domicile ou sa correspondance [...]"

Ainsi sur le plan strictement juridique, une telle réglementation du spamming permettrait de restaurer la confiance des acteurs de l'Internet en un média conçu à l'origine pour être au service des citoyens, et non pour leur porter préjudice par une atteinte injustifiée à leur vie privée et à leurs droits. Cependant, les critères posés pour une cette réglementation paraissent très exigeants, et il y a fort à parier que la technique (par la généralisation des logiciels de filtrage dans les logiciels de courrier notamment, ce qui semble être l'orientation actuelle) supplantera les efforts juridiques en la matière et mettra ainsi fin au débat.

---

[61] voir par exemple l'affaire PEINET au Canada dans laquelle les juges ont rejeté toute possibilité de confusion entre un nom commercial et un nom de domaine au motif que le premier étant constitué de majuscules (PEINET INC.) tandis que le second était constitué de minuscules (pei.net), ce qui n'a pourtant aucune incidence sur Internet ! PEINET INC. v. O'BRIEN (CARRYING ON BUSINESS AS ISLAND SERVICES NETWORK), 61 C.P.R. (3d) 334.

[62] "Le dépôt des commentaires écrits par les parties intéressées s'est déroulé en trois étapes. Avec plus de 1000 réponses à l'appel d'observations, c'est sans aucun doute la première fois qu'une consultation du Conseil a suscité des commentaires de la part d'un aussi large éventail *de particuliers, d'industries et de groupes d'intérêts divers*. Les nombreux intervenants représentaient à la fois de *simples citoyens, des sociétés de multimédia associées à la production et la distribution de nouveaux produits et services ainsi que des industries traditionnellement réglementées et leurs associations*, qui participent toujours activement aux consultations du Conseil."
Extrait du Rapport sur les nouveaux médias, Avis public radiodiffusion CRTC 1999-84, Avis public télécom CRTC 99-14 ; disponible sur http://www.crtc.gc.ca/archive/frn/Notices/1999/PB99-84.htm .

[63] Voir note précédente

Bibliographie

- NOTE IMPORTANTE : dernière date d'accès aux liens proposés dans ce mémoire : 25 mai 2003 -

- Textes et doctrine :

- ✓ **L'internet et le courrier électronique en vrac non sollicité (MULTIPOSTAGE)**, sur le site d'Industrie Canada concernant le commerce électronique au Canada
  http://com-e.ic.gc.ca/francais/strat/multipostage.html
- ✓ **Le contenu illégal et offensant diffusé dans Internet** – sur le site du gouvernement du Canada
  http://cyberwise.gc.ca/french/accueil.html
- ✓ **Rapport de la CNIL du 14 octobre 1999 sur le publipostage électronique et la protection des données personnelles**
  http://www.cnil.fr/thematic/docs/publpost.pdf
- ✓ **Rapport de la CNIL du 24 octobre 2002 sur l'opération "boîte à spams": les enseignements et les actions de la CNIL en matière de communications électroniques non sollicitées**
  http://www.cnil.fr/thematic/docs/internet/boite_a_spam.pdf
- ✓ **Le spamming et son contrôle** – Par Eric Labbée, Agent de recherche au Centre de Recherche en Droit Public, Université de Montréal
  http://www2.droit.umontreal.ca/~labbee/SPAM.HTM
- ✓ **Pourriel, pollupostage et référencement abusif : le spamming dans tous ses états** - Par Eric Labbé
  http://www.juriscom.net/pro/1/cns19990401.htm
- ✓ **Internet et la concurrence déloyale** – Rapport du groupe français sur la question "comment assurer le respect effectif des règles de la concurrence loyale en matière de commerce électronique ; journée d'étude de Venise organisée par la LIDC
  http://www.uni-muenster.de/Jura.itm/lidc/q3fran.doc
- ✓ **Courriels non sollicités : Enfin vers une application effective des sanctions** - par Julien Le Clainche
  http://www.droit-ntic.com/news/afficher.php?id=102
- ✓ **Le spamming** – par Me Murielle-Isabelle Cahen, avocate -
  http://www.droit-ntic.com/news/afficher.php?id=60
- ✓ **"Comment se défendre contre le spam X…**" – Par Me Etienne Drouard, avocat
  http://www.journaldunet.com/itws/it_drouard.shtml
- ✓ **L'opt-in ? Incontournable** – par Jérôme Stioui
  http://www.journaldunet.com/tribune/011214tribune.shtml

- ✓ **Lutte anti-spam : deux sociétés épinglées par la CNIL réagissent** – Par Estelle Dumont
  http://news.zdnet.fr/story/0,,t118-s2126621,00.html?nl=zdnews
- ✓ **La solution logicielle est la plus efficace contre le spam** - Par Thomas Dautieu et Mathias Moulin (CNIL)
  http://www.journaldunet.com/chat/retrans/021204_cnil.shtml
- ✓ **"White lists" emerge as a tool for consumers in fight against spam** – Par Noël C. Paul
  http://news.findlaw.com/csmonitor/s/20021202/02dec2002104017.html
- ✓ **L'Europe interdit le spam** – Par Solveig GODELUCK
  http://www.lageopolitiquedinternet.com/e-books/pages/e-articles_europeinterdit.htm
- ✓ **Envoi d'e-mails en nombre :** l'ACSEL et l'IREPP proposent un marquage électronique pour supprimer le spam
  http://www.acsel.asso.fr/acsel/actions/communiques/2002_septembre.htm

- Sites web :

Portails de droit des nouvelles technologies :

- ✓ Arobase - http://www.arobase.org
- ✓ Droit et Nouvelles technologies - http://www.droit-technologie.org/
- ✓ Droit NTIC - http://www.droitntic.com/
- ✓ Juriscom - http://www.juriscom.net/
- ✓ Legalis - http://www.legalis.net/
- ✓ Njuris - http://www.njuris.com/
- ✓ Juritel - http://www.juritel.com
- ✓ Clic-droit - http://www.clic-droit.com/
- ✓ Legalbiznext - http://www.legalbiznext.com/

Sites institutionnels :

- ✓ Commission nationale informatique et libertés - http://www.cnil.fr/
- ✓ Commission d'accès à l'information du Québec - http://www.cai.gouv.qc.ca/
- ✓ Commission à la protection de la vie privée du Canada - http://www.privcom.gc.ca/index_f.asp
- ✓ Site du gouvernement français sur les technologies et la société de l'information - http://www.telecom.gouv.fr/