Combattre le pourriel

Rapport final du projet de recherche
présenté au Bureau de la consommation
d'Industrie Canada

par

juillet 2005

Rapport de recherche publié par :

l'union des consommateurs

1000 rue Amherst, bureau 300
Montréal (Québec) H2L 3K5

Téléphone : (514) 521-6820
Sans frais : 1 888 521-6820
Télécopieur : (514) 521-0736

union@consommateur.qc.ca
www.consommateur.qc.ca/union

Membres de l'Union des consommateurs

- ACEF Abitibi-Témiscamingue
- ACEF Estrie
- ACEF de l'Est de Montréal
- ACEF de l'Île-Jésus
- ACEF du Nord de Montréal
- ACEF du Grand-Portage
- ACEF de Lanaudière
- ACEF Montérégie-est
- ACEF Rive-Sud de Québec
- Membres individuels

L'Union des consommateurs est membre de l'Internationale des consommateurs (IC), une fédération regroupant 250 membres en provenance de 115 pays.

Prérecherche et rapport préliminaire

- Me Philippe Mercorio

Recherche et rédaction

- Me Marcel Boucher

ISBN : 2-923405-03-X

Cette recherche a été rendue possible grâce au soutien financier d'Industrie Canada.

Pour faciliter la lecture du texte et éviter la redondance systématique, nous avons choisi d'utiliser le masculin générique pour désigner les deux genres.

© **Union des consommateurs**

TABLE DES MATIÈRES

L'UNION DES CONSOMMATEURS, *la force d'un réseau*

L'Union des consommateurs est un organisme sans but lucratif qui regroupe neuf (9) ACEF, le Regroupement des consommateurs d'assurances ainsi que des membres individuels.

La mission de l'Union des consommateurs est de représenter et défendre les consommateurs, en prenant en compte de façon particulière les intérêts des ménages à revenu modeste. Les interventions de l'Union des consommateurs s'articulent autour des valeurs chères à ses membres soit, la solidarité, l'équité et la justice sociale, ainsi que l'amélioration des conditions de vie des consommateurs aux plans économique, social, politique et environnemental.

La structure de l'Union des consommateurs lui permet de maintenir une vision large des enjeux de consommation tout en développant une expertise pointue dans certains secteurs d'intervention, notamment par ses travaux de recherche sur les nouvelles problématiques auxquelles les consommateurs doivent faire face ; ses actions, de portée nationale, sont alimentées et légitimées par le travail sur le terrain et l'enracinement des associations membres dans leur communauté.

L'Union des consommateurs agit principalement sur la scène nationale, en représentant les intérêts des consommateurs auprès de diverses instances, politiques, réglementaires et judiciaires, et sur la place publique. Parmi ses dossiers privilégiés de recherche, d'action et de représentation, mentionnons le budget familial et l'endettement ; l'énergie ; les questions liées à la téléphonie, la radiodiffusion, la télédistribution et l'inforoute ; la santé, l'alimentation et les biotechnologies ; les produits et services financiers ainsi que les politiques sociales et fiscales.

Finalement, dans le contexte de la globalisation des marchés, l'Union des consommateurs travaille en collaboration avec plusieurs groupes de consommateurs du Canada-anglais et de l'étranger. Elle est membre de l'Organisation internationale des consommateurs (OIC) organisme reconnu notamment par les Nations-Unies.

- Ses principaux domaines d'expertise sont :
- Agroalimentaire
- Budget, crédit et endettement
- Énergie
- Produits et services financiers
- Politiques sociales et fiscales
- Santé
- Télécommunications, radiodiffusion et inforoute

INTRODUCTION

Le pourriel (maintenant aussi connu sous le vocable « polluriel » ou « pourriel ») désigne tout message commercial non sollicité reçu par voie de courrier électronique. Ces messages commerciaux, visant à attirer l'attention sur certains services ou produits, plutôt que de s'adresser à un destinataire d'une manière spécifique, font l'objet d'envois massifs automatisés. Les « pourrielleurs » offrent des pilules miracles qui mettront du piquant dans votre vie sexuelle ou réduiront votre tour de taille, des médicaments de toutes sortes, et même des diplômes : quelques clics et un numéro de carte de crédit et vous voilà détenteur d'un doctorat en droit d'une université virtuelle du Costa Rica !

Bien que l'on ait tendance à penser que, quantitativement, les messages à caractère sexuel viennent en tête de liste, dans les faits, il n'en est rien. « Le pourriel pornographique continue à décroître, atteignant son plus bas niveau depuis la création du premier Spam Index Clearswift en juin 2003. Il comptait à l'époque pour 22% du total, mais n'a cessé de décliner depuis, ne représentant plus que 5% en avril 2004. Le pourriel pharmaceutique a lui aussi chuté de 57% des messages non sollicités en mars à 40% en avril, alors que le pourriel financier passait dans le même temps de 26% à 38%. » [1]. Certains facteurs économiques ont fait en sorte que le pourriel soit devenu une véritable industrie. L'investissement initial et les frais d'opération d'un « pourrielleur » sont relativement faibles, se limitant à l'achat d'un matériel informatique relativement performant, et le retour rapide sur l'investissement est presque garanti. Selon le Wall Street Journal, un « pourrielleur » peut rentabiliser ses opérations dès qu'il reçoit plus de 0.001% de réponses sur les courriels expédiés[2]. Cela explique en grande partie la croissance exceptionnelle de cette industrie sur Internet; selon les études sur le sujet, le pourriel représentait, en janvier 2004, 60% de l'ensemble des courriels envoyés[3], comparativement à 36% en août 2002 et 8% seulement en août 2001[4].

Le pourriel a dépassé le stade de " simple nuisance " pour devenir un problème majeur, et ce à plusieurs niveaux: les particuliers se plaignent auprès de leurs fournisseurs d'accès à Internet de l'encombrement par le pourriel de leur messagerie électronique et les entreprises constatent les coûts énormes qu'ils entraînent tant en perte de productivité qu'en coûts financiers (achat d'équipement et de logiciels anti-pourriel, embauche d'employés spécialisés en sécurité informatique). Une firme américaine de consultants spécialisés, Ferris Research Inc., estimait que le pourriel pourrait entraîner à l'ensemble des entreprises américaines des dépenses supplémentaires de 10 milliards de dollars pour la seule année 2003[5], et ce sans compter les pertes de productivité; certains centres de recherches estiment à 1.4% le coût du pourriel sur la productivité des employés, soit 874$ par employé par année[6]. Une étude québécoise va plus

[1] Statistiques établies par ***Clearswift, l'éditeur de MIMEsweeper, couvrant le mois d'avril 2004.*** ~~In Brightmail .Site de Brightmail http://www.brightmail.com/Spamstats.html (page consultée en décembre 2004)~~ Rapportées par Mag-Securs, magazine européen de la sécurité informatique. Disponible sur le site Internet de Mag-Securs http://www.mag-securs.com/article.php3?id_article=868 (page visitée le 5 juillet 2005)

[2] Cité par Roose, Dave « Spam Queen : just trying to make a living » sur le Site de G4; ~~In G4. Site de G4~~ http://www.techtv.com/screensavers/showtell/story/0,24330,3407919,00.html (page consultée en décembre 2004)

[3] Ward, Mark « How to make spam unstoppable » In BBC News Worl Edition. Site de BBC News http://news.bbc.co.uk/2/hi/technology/3458457.stm (page consultée en février 2005)

[4] op. cit. note 2

[5] Krim, Jonathan « Spam's costs to business escalates » In Washi~~e~~ngton Post.com. Site du Washington Post http://www.washingtonpost.com/ac2/wp-dyn/A17754-2003Mar12 (page consultée en décembre 2004)

[6] Nucleus Research : Spam : the silent ROI killer. http://www.nucleusresearch.com/research/d59.pdf (document consulté le 11 mai 2005)

loin, elle estime à 1,2 milliard $ par année pour le Québec seulement la perte de productivité reliée à la gestion des messages de courriel indésirables, soit 1000$ par employé par année[7].

Tout le monde s'entend sur l'ampleur du problème et rien ne laisse croire que ce phénomène tire à sa fin, au contraire. La lutte au pourriel va bon train, mais elle entraîne certains effets secondaires indésirables. Les filtres anti-pourriel, qui sont, à ce jour, le moyen de prédilection pour lutter contre l'envahissement, ne sont pas aussi raffinés qu'il le faudrait : outre le fait qu'ils laissent passer des messages indésirables, ils rejettent aussi parfois des courriels légitimes qu'ils identifient par erreur comme du pourriel.

L'avalanche de plaintes des particuliers, des milieux d'affaires et des fournisseurs d'accès à Internet a amené de nombreux législateurs à rechercher la manière de solutionner cette problématique. Il appert toutefois que la définition à donner au pourriel pose problème; de nombreuses entreprises faisant affaire principalement sur Internet appuient par contre l'industrie du marketing direct dans son opposition aux législations anti-pourriel[8], de crainte qu'une définition trop large leur rende impossible, ou beaucoup plus difficile, la prospection commerciale via Internet.

Après une étude des moyens mis en place pour combattre le pourriel, au Canada, aux États-Unis et ailleurs (recours légaux, registres anti-pourriel, campagnes de conscientisation à l'endroit des consommateurs), nous tenterons d'évaluer les voies de solutions les plus efficaces, selon les approches utilisées et au vu des expériences passées. À notre étude de la législation existante s'ajoutera l'examen de quelques autres initiatives visant à réduire le pourriel: projets de Loi, dispositions contractuelles, codes de conduite.

Après un bref survol des premières expériences de coopération internationale, nous jetterons un coup d'œil sur le Plan d'action canadien dans la lutte au pourriel mis sur pied en 2004 par le ministre de l'Industrie, avant de soumettre nos conclusions et recommandations.

[7] Lacroix, Eric, directeur de la veille stratégique et des enquêtes au cefrio cité par charles poulain in « les pourriels coûtent plus d'un milliard au québec », un article du journal de montréal, 7 novembre 2003, disponible sur le site de canoë, au http://www2.canoe.com/techno/nouvelles/archives/2003/11/20031107-062614.html (page consultée le 11 mai 2005)

[8] ~~Krim, Jonathan « Spam's costs to business escalates » In Washiongton Post.com. Site du Washington Post http://www.washingtonpost.com/ac2/wp-dyn/A17754-2003Mar12 (page consultée en décembre 2004)id.~~ Krim, Jonathan « Spam's costs to business escalates » In Washington Post.com. Site du Washington Post http://www.washingtonpost.com/ac2/wp-dyn/A17754-2003Mar12 (page consultée en décembre 2004)

1. LA SITUATION AUX ÉTATS-UNIS

Les législateurs et les tribunaux américains, tant à l'échelle des États qu'au niveau fédéral, ont tenté de maîtriser l'invasion du pourriel tant par le biais des lois existantes que par l'élaboration de nouveaux instruments de régulation, quitte à ce que le manque de coordination enraye les efforts entrepris. Dans cette section, nous présentons un survol de ces instruments et, le cas échéant, de leur application par les tribunaux.

Les lois fédérales

CAN-Spam Act
En 2003, le Congrès américain a adopté le Controlling the Assault of Non-Solicited Pornography and Marketing Act (Public Law 108-187), plus communément appelé le « CAN-Spam Act », entré en vigueur le 1er janvier 2004[9]. Les Attorney General des États ainsi que la Federal Trade Commission (FTC), l'agence fédérale qui régit le commerce, sont chargés de surveiller l'application de cette Loi.

Il est important de préciser de prime abord que le CAN-Spam Act n'interdit pas l'envoi de pourriel mais ne fait que réglementer les envois de courriers électroniques. Le texte précise d'ailleurs qu'il ne vise qu'à imposer des limitations (et des pénalités) relativement à la transmission par Internet de courriers électroniques commerciaux non sollicités[10].

Cette loi impose donc à tous ceux qui désirent envoyer des courriels de nature commerciale trois obligations principales :
1) Identification : tout courriel non sollicité doit clairement être identifié, de manière à ce que son destinataire puisse savoir qu'il s'agit d'une publicité ou d'une sollicitation en vue de vendre des produits ou services;
2) « Opting out » : les courriels doivent comporter une option, facilement visible et accessible, permettant de signifier à l'expéditeur le refus de recevoir à l'avenir tout courriel émanant de cette source;
3) Adresses : les courriels doivent comporter une adresse électronique de retour valide et indiquer l'adresse postale de l'expéditeur.

Deux obligations additionnelles sont imposées aux expéditeurs de courriels non sollicités qui auraient obtenu la permission (ou qui n'auraient pas reçu d'interdiction) de certains destinataires de leur faire parvenir d'autres courriels de nature commerciale :
1) Interdiction de tromper le destinataire sur l'objet du courriel (en usant, par exemple, d'indications trompeuses sur l'objet ou le contenu du courriel afin d'amener son destinataire à ouvrir le message) et
2) Obligation de se conformer à la politique du registre national « Do not E-mail List », qui interdit l'envoi de courriels de sollicitation commerciale à tous ceux qui s'y sont inscrits; ce

[9] Sorkin David E. "Spam Laws" In Spam Laws United States. Site de Spam Laws http://www.spamlaws.com/federal/108s877.shtmlhttp://www.Spamlaws.com/federal/108s877.html (page consultée le 11 mai ~~en décembre~~ 2004) Le texte est aussi disponible en format Pdf à l'adresse suivante : http://www.spamlaws.com/pdf/pl108-187.pdf

[10] Le préambule du CAN-SPAM Act se lit comme suit: Begun and held at the City of Washington on Tuesday, the seventh day of January, two thousand and three An Act To regulate interstate commerce by imposing limitations and penalties on the transmission of unsolicited commercial electronic mail via the Internet.

registre est le pendant des listes du même genre qui ont été instaurées dans le domaine du télémarketing.

Le FTC a toutefois émis l'avis que la création d'un tel registre serait non seulement très complexe au plan logistique, mais que les résultats anticipés seraient difficiles à atteindre. De l'opinion du FTC, un tel registre pourrait même avoir pour effet de générer un flot encore plus grand de pourriel, dans l'hypothèse où certains pourrielleurs délinquants pourraient être portés à consulter cette liste afin d'inclure ces adresses supplémentaires à leurs listes d'envois[11]. L'idée d'instaurer un registre national semble donc pour l'instant abandonnée, malgré la popularité et le succès d'un registre semblable dans le domaine du télémarketing (le Do-not call Registry, administré par une autre agence fédérale : la Federal Communication Commission (FCC)[12]). La deuxième obligation additionnelle imposée aux expéditeurs de courriels commerciaux, soit l'inscription dans le registre national, reste donc pour le moment lettre morte.

Le CAN-Spam Act est une loi fédérale; le législateur a prévu que sa loi transcende les lois anti-pourriel qu'avaient adoptées plusieurs États (ex. Californie, Virginie). La section 8 b) prévoit que le CAN-Spam Act remplace et annule les lois étatiques qui régissent spécifiquement l'usage d'Internet pour l'envoi de courriels de nature commerciale, à l'exception des dispositions traitant des fausses représentations dans quelque portion des courriels de nature commerciale ou dans les pièces attachées qui y sont jointes, laissant toutefois le champ libre à l'application des lois qui ne seraient pas spécifiques aux courriers électroniques (trespass, contract, tort law, fraud or computer crime). Par conséquent, les lois étatiques ne trouveront plus leur application que dans certains cas types et dans les matières qui ne sont pas couvertes par le CAN-Spam Act, soit par exemple en matière de fausse représentation ou de crimes informatiques[13].

Le CAN-Spam Act précise, dans les définitions qui apparaissent à sa section 3, que le consentement à recevoir des courriels non sollicités de nature commerciale (affirmative consent), doit être donné suite à une demande non équivoque et surtout clairement visible (clear and conspicuous request), afin d'éviter que ne soit interprété comme un consentement un accord qui aurait été donné par inadvertance ou suite à de fausses représentations. Ce consentement, plutôt que d'être exigé avant tout envoi de pourriel, ne constitue toutefois, dans le cadre du CAN-Spam Act, qu'un moyen de défense à l'usage des expéditeurs.

La définition du pourriel que donne la Loi n'inclut pas les courriels qui sont de nature transactionnelle ou informationnelle et qui font suite à une relation d'affaires déjà initiée; ainsi un courriel informant un consommateur du rappel concernant un produit acheté ou donnant des informations sur l'utilisation sécuritaire du produit acheté ne tomberait pas sous le coup de la définition du pourriel. De même, un courriel envoyé pour informer un client d'une mise à jour disponible (ex. sur un logiciel acheté) ne serait pas non plus du pourriel. Il reste à voir si la jurisprudence donnera à la définition statutaire un sens large ou restrictif.

[11] "Keep your email address unlisted : there is no national do not email registry" . in FTC Consumer Alert. Site du Federal Trade Commission http://www.ftc.gov/bcp/conline/pubs/alerts/dnealrt.pdf (~~page~~ document consulté en août 2004)

[12] Cette liste aurait enregistré plus de 50 millions de numéros de téléphone en moins d'un an. Olsen, S. Do Not Call List Tops 50 Million Phones, CNet (17 septembre 2003), cité par Michael Geist in: Untouchable: a Canadian perspective on the anti-spam battle" In Michael Geist.ca. Site de Michael Geist http://www.michaelgeist.ca/geistSpam~~/~~.pdf, p.30-31 (~~page~~document consulté~~e~~ en décembre 2004)

[13] "CAN-SPAM : Unwanted text messages and e-mail on wireless phones and other mobile devices" In FCC Consumer Facts. Site du Federal Communications Commission Consumer and Governmental Affairs Bureau. http://ftp.fcc.gov/cgb/consumerfacts/canspam.html (page consultée en novemvre 2004)

En ce qui a trait aux pratiques sanctionnées, la Loi prévoit que l'utilisation d'adresses électroniques obtenues sciemment par le biais de moyens automatisés (section 5 b)) constitue une aggravation dans le cas des infractions listées à la section 5 (courriel sans identification de l'objet du message, envoi en l'absence d'autorisation de la part du destinataire) qui permettrait au Tribunal, en vertu de la section 7 (Enforcement Generally) de tripler les montants prévus à titre de dommages. L'utilisation des logiciels spécialisés qui génèrent des combinaisons de chiffres et de lettres pouvant constituer des adresses électroniques ou qui balayent les sites Internet pour repérer toutes les adresses électroniques qui y sont affichées ne constituerait donc pas à elle seule une infraction.

Le CAN-Spam Act, jugé trop favorable à l'industrie par nombre d'intervenants, a fait l'objet de plusieurs critiques qui visent notamment à dénoncer l'approche « opt out » adoptée par le législateur, qui fait porter sur la personne qui reçoit les messages la tâche de faire stopper les envois[14]. Une approche qui n'aurait permis l'envoi de pourriel qu'à ceux qui se déclareraient prêts à en recevoir (« affirmative consent » ou « opt in ») semblerait préférable à celle qui permet l'envoi jusqu'à ce qu'un avis clair soit envoyé pour signaler le désir de ne plus en recevoir (opt out).

L'interdiction faite par le CAN-Spam Act aux particuliers d'entamer des poursuites judiciaires au civil contre les pourrielleurs a elle aussi été l'objet de plusieurs critiques. Outre les recours qui sont réservés aux autorités ou agences étatiques (prévus à la section 7), le législateur a jugé bon de limiter aux fournisseurs de services Internet l'accès aux recours civils visant à faire cesser certaines pratiques ou à obtenir compensation pour des dommages encourus (section 7 g).

Le « super statut » de cette loi fédérale a aussi soulevé plusieurs critiques. Les critiques sont d'autant plus virulentes de la part des groupes de défense des intérêts des consommateurs qu'ils voyaient dans certaines lois étatiques, telles la loi anti-pourriel californienne, des modèles en matière de répression du «Spamming» (voir plus loin à la section sur le California Business and Professions Code). La loi californienne anti-pourriel a été adoptée en 2003 pour se voir immédiatement couper l'herbe sous le pied par le CAN-Spam Act dès son entrée en vigueur. Cette loi californienne prévoyait entre autres la possibilité pour les particuliers d'intenter au civil des poursuites contre les pourrielleurs pour obtenir des dommages et des dommages exemplaires allant jusqu'à 1000$ par courriel reçu. Du fait qu'elle néglige d'inclure cette possibilité de recours directs et qu'elle retire aux États le loisir de légiférer à cet effet, plusieurs praticiens et théoriciens considèrent qu'il y a dans la loi fédérale un manque de synergie entre les intentions avouées et les mesures qu'elle prévoit pour tenter d'en arriver à ses fins. Ray Everett-Church, un expert en sécurité et vie privée, commentait ainsi le CAN-Spam Act : « I think the reality is that most companies who are engaged in e-mail marketing are not going to be deeply affected by (CAN-Spam), because that law is geared towards dealing with abusive and deceptive practices, most of which legitimate companies are wise enough to avoid»[15].

[14] D'autant plus que les campagnes anti-Spam mettent en garde contre ces fausses options qui, plutôt que d'être respectées par l'expéditeur, confirme la validité de l'adresse à laquelle le Spam a été expédié. Microsoft, par exemple, donne le conseil suivant : « **Ne répondez à un message non sollicité** que si vous êtes certain qu'il provient d'une source légitime. Cela implique également de ne pas répondre aux messages vous proposant de vous désabonner d'une liste de publipostage. » (nos soulignés) - À faire et à ne pas faire avec le spam : comportement à adopter vis-à-vis du spam, in Site Microsoft Sécurité. Sur le site Internet de Microsoft France http://www.microsoft.com/france/securite/gpublic/email/options.mspx (page consultée le 18 juillet 2005); voir aussi Combattre le pourriel : trois conseils clés; in arrêtezlepourrielici.ca, disponible au http://arretezlepourrielici.ca/ (page consultée le 12 juillet 2005)

[15] Ulbrich Chris « Spam law generates confusion ». In Wired News. Site de Wired News. http://www.wired.com/news/business/0,1367,62031,00.html (page consultée en décembre 2004)

En fait, les fournisseurs d'accès à Internet, auxquels le CAN-Spam Act permet les recours légaux, avaient déjà, avant son adoption, la possibilité de poursuivre en justice les pourrielleurs, que ce soit en vertu des dispositions de lois fédérales comme le Computer Fraud and Abuse Act ou en vertu des « torts » de Common Law, soit les dommages résultant d'actions intentionnelles ou négligentes commises hors d'un cadre contractuel, comme le « trespassing », ou encore pour violation de contrat, les fournisseurs d'accès à Internet limitant généralement par contrat l'usage qui peut être fait par leurs clients des systèmes de courrier électronique qu'ils leur fournissent[16].

Une loi fédérale qui, plutôt que de rendre inopérantes les dispositions des lois des États, aurait veillé à imposer quant aux courriers électroniques commerciaux non sollicités des normes minimales et un encadrement obligatoire, tout en laissant les États préciser dans leurs propres lois le niveau de tolérance ou le degré de contrôle applicable, nous eût semblé beaucoup plus efficace. Ainsi, les États qui auraient négligé d'adopter des lois spécifiques auraient eu un cadre national auquel se référer et les États plus progressistes ou plus soucieux du problème auraient pu apporter les précisions qu'ils jugeaient nécessaires et tenter même d'enrayer le pourriel plutôt que de l'encadrer.

Les rédacteurs et les promoteurs du CAN-Spam Act clamaient que sa conception était, justement, de nature à enrayer le pourriel. Les critiques doutent au contraire de son efficacité, puisque le cadre qu'il impose ne fera, selon plusieurs, dans le meilleur des cas qu'inciter les pourrielleurs à pratiquer un « Spamming légal ». Neil Schwartzman, de la branche canadienne de la Coalition Against Unsolicited Commercial Email (CAUCE) mentionne que le CAN-Spam Act, tel que rédigé, "means that every company has the right to send you at least one Spam e-mail. And there are tens of millions of small- and medium-sized enterprises in the U.S. alone."[17]

Mise application du CAN-Spam Act

En mars 2004 le CAN-Spam Act a enfin été invoqué devant les tribunaux: 4 des plus grands fournisseurs d'accès à Internet et de services de messageries électroniques, soit AOL, Microsoft, EarthLink et Yahoo, ont décidé de coordonner leurs efforts dans leur lutte au pourriel en poursuivant plusieurs pourrielleurs en vertu du CAN-Spam Act[18].

Les sénateurs Burns et Wyden, les promoteurs du CAN-Spam Act au Sénat, ont réagi à l'annonce des poursuites entreprises par les 4 grands de l'industrie informatique en déclarant que les beaux jours des pourrielleurs allaient bientôt prendre fin et que ceux-ci devraient rendre compte de leurs actions. De dire le sénateur Wyden: « Today's filing proves that the days of spamming with impunity are finally over, and all those who abuse e-mail and threaten its viability as the Internet's most popular and useful application should take notice. These suits will have to

[16] Ainsi, dans l'affaire America Online Inc.v. LCGM Inc., le tribunal a donné raison au fournisseur d'accès à Internet qui poursuivait un pourrielleur, en se basant entre autres sur la doctrine de « trespassing » : la cour a considéré que l'envoi massif de courriels non sollicités pouvait constituer un « trespass of chattels », soit : le fait pour une partie d'abuser (ce qui comprend « l'immixtion » dans un système) de manière intentionnelle du bien d'autrui. *America On-Line, Inc. v. LCGM, Inc.*, 46 F. Supp.2d 444 (E.D. Va. 1998)

[17] Chezzi, Derek "You've got Spam" In Macleans.ca. Technology . Site de Macleans. http://www.macleans.ca/topstories/technology/article.jsp?content=20040223_75808_75808 (page consultée en décembre 2004)

[18] Gross Grant « Update : majors ISPs sue hundred of spammers » In The Standard.com. site de The Standard http://www.thestandard.com/article.php?story=20040310183418590& (page consultée en janvier 2004)

be settled in a court of law, but I believe this action marks the dawn of a new day for spammers -- one in which they face real accountability.»[19].

Dans l'affaire AOL. c. Davis Wolfgang Hawke et al., la requête de la demanderesse allègue que: *« Defendant's messages are characterized by a variety of deceptive and fraudulent techniques calculated to camouflage their true identities… »* [20]. La demanderesse reproche aux défendeurs les infractions suivantes au CAN-Spam Act: usage de tiers pour l'envoi massif de pourriel par la technique du « cheval de Troie »[21]; dissimulation du véritable expéditeur de courriels non sollicités (le « spoofing »); défaut d'indiquer l'adresse physique de l'expéditeur des courriels; défaut d'offrir dans les courriels envoyés une option demandant de ne plus en recevoir; promotion de services ou produits de nature frauduleuse[22]. Il appert de la requête que les actions des défendeurs auraient provoqué des plaintes auprès de la demanderesse de la part de plus de 100 000 de ses clients. AOL invoque de plus la violation de dispositions contractuelles, soit la politique anti-pourriel de la compagnie, qui fait partie intégrante des modalités de services auxquelles les clients adhèrent en s'abonnant. Enfin, AOL demande à la Cour de lui accorder, en plus des dommages, y compris les dommages punitifs, une injonction permanente visant à interdire aux défendeurs de poursuivre les actions qui leur sont reprochées.

Le résultat des actions en justice entreprises contre les pourrielleurs par ces géants de l'informatique permettra certainement d'évaluer l'importance que les tribunaux américains accorderont au pourriel et à cette loi fédérale qui devrait viser à mater les pourrielleurs. Les suites de ces procès mériteront aussi une attention soutenue. La publicité qui sera certainement faite autour des jugements pourrait jouer un rôle important dans la sensibilisation aux pourriels et aux armes qui sont mises à la disposition du public pour lutter contre son envahissement.

Pour ce qui est des défendeurs dans ces affaires, par contre, ces causes ne sauraient être déterminantes, puisque seuls sept des 220 défendeurs sont identifiés[23]. D'autre part, la facilité pour les entreprises de faire faillite ou de fermer leurs portes suite à une condamnation, pour poursuivre par la suite autrement leurs activités étant un secret de polichinelle, on peut douter de l'efficacité d'éventuelles condamnations contre des entreprises délinquantes ou de leur effet de dissuasion sur un marché aussi rentable.

---

[19] Gross Grant « Update : majors ISPs sue hundred of spammers » In The Standard.com. site de The Standard. http://www.thestandard.com/article.php?story=20040310183418590& (page consultée en janvier 2004)

[20] ~~(nom de la cause)~~America Online v. David Wolfgang Hawke et al. - In Findlaw.com Site de Findlaw : http://news.findlaw.com/hdocs/docs/cyberlaw/aolhawke30904cmp.pdf, Complaint and Exhibits p.6 ~~jugement~~ ((document consulté~~e~~ en janvier 2005)

[21] Le pourrielleur infecte discrètement un ordinateur, souvent sans que son propriétaire ne s'en rende compte; l'ordinateur infecté se chargera à partir de ce moment d'expédier le Spam vers sa propre liste d'adresse.

[22] La requête, qui invoque la violation du CAN-SPAM Act, et plus particulièrement des articles de la section 5, qui indique les prérequis nécessaires à l'envoi de courriel non sollicité, soulève aussi la violation de certaines dispositions de la loi anti-Spam de la Virginie, où se trouve le siège social de la demanderesse.

[23] AOL a deposé deux poursuites, contre l'ancien néo-Nazi Davis Wolfgang Hawke et al. Ainsi que contre 40 inconnus ("John Does"). La poursuite de EarthLink est dirigée contre 75 défendeurs inconnus. Celles de Microsoft visent JDO Media et autres, puis 50 inconnus ("John Does") faisant affaire sous le nom de "Super Viagra Group". Yahoo dirige pour sa part sa poursuite contre Eric Head, Matthew Head and Barry Head et leurs compagnies Gold Disk Canada Inc, Head Programming Inc and Infinite Technologies Worldwide Inc, connues collectivement sous le nom de The Head Operation. THE online REPORTER, March 13-19, 2004 - Issue 387. In Online Reporter http://www.onlinereporter.com/TORbackissues/TOR387.htm (page consultée le 5 juillet 2005)

Lanham (Trademark) Act
Le Lanham (Trademark) Act [24], qui contient les dispositions fédérales sur les marques de commerce, comprend une section sur les désignations trompeuses de biens et la fausse représentation. Ces dispositions ont déjà été invoquées contre des expéditeurs de courriers électroniques commerciaux.

C'est en effet en vertu du Lanham Act que, dans l'affaire Register.com Inc. v. Verio[25], le tribunal accorda au demandeur, registraire de noms de domaines, l'injonction demandée contre un concurrent qui communiquait par courriels avec des clients du demandeur dans un but de démarchage. Le tribunal a conclu que les moyens utilisés violaient le Lanham Act, puisque l'usage par le défendeur d'un nom similaire à la marque de commerce employée par un concurrent, soit le demandeur, ainsi que celui d'un slogan semblable, étaient de nature à créer de la confusion auprès des clients du demandeur.

De même dans l'affaire Classified Ventures L.L.C., v. Softcell Mktg, Inc.[26], le demandeur qui poursuivait Softcell, un pourrielleur qui s'était servi du nom de domaine du demandeur comme adresse de retour dans sa campagne d'envoi massif de pourriel à caractère pornographique, s'est vu confirmer par la cour que les agissements de Softcell violaient le Lanham Act, parce qu'il entraînait un risque de confusion dans l'esprit des clients du demandeur.

L'utilisation des lois visant la protection des marques de commerce pourrait donc, dans des cas bien particuliers, entraîner pour certains pourrielleurs des ennuis dans la poursuite de leurs activités. Le cadre très restrictif et la possibilité pour le pourrielleur de corriger ce qui a entraîné l'infraction font toutefois en sorte que ces lois ne peuvent être considérées comme une arme efficace pour lutter, à grande échelle, contre le pourriel ou les pourrielleurs.

Computer Fraud and Abuse Act
Le Computer Fraud and Abuse Act (CFAA)[27] fait d'actes, comme l'accès non autorisée à des ordinateurs, ou le fait de les altérer ou de les endommager, des infractions. Ses dispositions se sont à quelques reprises avérées utiles lors de poursuites contre des pourrielleurs.

Dans l'affaire Hotmail c.Van$ Money Pie[28], le demandeur alléguait une violation du Computer Fraud and Abuse Act. Le défendeur, un pourrielleur, avait créé de multiples comptes de courriers Hotmail afin, notamment de rediriger les plaintes de ceux qui recevaient du pourriel vers ces adresses. Hotmail soutenait que ces agissements lui avaient entraîné des dommages, dont : perte de réputation, risques de dommages au système informatique de Hotmail, délais dans le service aux abonnés légitimes occasionné par l'engorgement du réseau, etc. S'appuyant sur une disposition du CFAA, la cour condamne la transmission volontaire d'informations à des ordinateurs protégés en sachant que cela causera des dommages, le tribunal a donné raison au demandeur.

Les amendements apportés en 2002 ont clairement indiqué la volonté d'étendre à tout ordinateur connecté à Internet et qui sert au commerce la protection offerte par le CFAA, plutôt que de la limiter à ceux qui sont la propriété de l'État. Les ordinateurs protégés en vertu du CFAA comprennent donc maintenant, outre ceux des agences gouvernementales et des

[24] Lanham Trademark Law (15 U.S.C.S.)
[25] Register.com, Inc. v. Verio, Inc., 126 F. Supp. 2d 238 (SDNY 2000)
[26] Classified Ventures L.L.C., v. Softcell Mktg, Inc, 109 F. Supp. 2nd 898 (N.D. Ill.2000)
[27] Computer Fraud and Abuse Act (18 U.S.C.S.1030)
[28] 47 U.S.P.Q.2d (BNA) 1020, 1998 US Dist. LEXIS 10729, 1998 WL 388389 (N.D. Cal. Apr. 16, 1998).

systèmes médicaux et financiers, tout ceux qui servent au commerce domestique ou international ou aux communications qui y sont reliées[29].

Les tribunaux américains ont donc considéré que la terminologie employée (« accès non-autorisé » et « ordinateur protégé ») est suffisamment inclusive pour permettre de s'attaquer à nombre de pourrielleurs. Ainsi dans l'affaire Shurgard Storage Centers v. Safeguard Self Storage Inc.[30], la Cour, en faisant l'historique législatif de la CFAA, souligne le fait que les termes « without autorization » et « protected computer » doivent recevoir une interprétation très libérale. Le juge exprime en ces termes la portée du CFAA:

> « the CFAA was intended to control interstate computer crime, and since the advent of the Internet, almost all computer use has become interstate in nature. »[31]

Cependant, la jurisprudence souligne aussi les limites du CFAA: ainsi dans Chance v. Ave. A. Inc.[32], la Cour rappelle le fait que, pour qu'il y ait une cause d'action en vertu du Computer Fraud and Abuse Act, des dommages d'au moins 5000.00$ doivent pouvoir être prouvés, comme le précisait l'arrêt Theofel v. Farey-Jones[33]. L'accès non autorisé à un ordinateur protégé et un dommage matériel ne suffisent pas à invoquer l'application de la loi; à défaut d'un dommage qui s'élève au moins à 5000.00$, il n'y aura tout simplement pas de cause d'action.

Le CFAA prévoit à son article 1030 a) 5) b) d'autres dommages qui pourraient résulter du pourriel et qui pourraient être considérés par les tribunaux, notamment : les menaces à la santé ou à la sécurité publique, l'atteinte à l'intégrité physique d'un particulier, etc. Le pourriel pharmaceutique étant parmi les plus présents, il ne serait pas étonnant de voir plaidées un jour devant les tribunaux américains ces dispositions à l'encontre de certains pourrielleurs.

Modèles de lois étatiques

Nous examinons ici brièvement 2 des lois étatiques anti-pourriel qui avaient fait l'objet d'une importante attention médiatique. Bien que ces lois aient été, en grande partie, rendues inopérantes par l'adoption du CAN-Spam Act[34], elles comportent certaines dispositions et certaines approches dont l'étude, ne serait-ce qu'à des fins pédagogiques, reste pertinente, et dont l'approche utilisée pourrait servir de modèle pour de futures législations.

---

[29] Fraud and Related activity in connection with computers. In US Code Collection. Site du Legal Information Institute http://www4.law.cornell.edu/uscode/18/1030.html (page consultée en décembre 2004) "tThe term "protected computer" means a computer - exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or which is used in interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States". Notons que le CAN-SPAM Act reprend à son compte cette notion de « protected computers ».;

[30] Shurgard Storage Centers v. Safeguard Self Storage Inc ,119 F. Supp. 2d 1121 (W.D. Washington, 2000)

[31] Shurgard Storage Centers v. Safeguard Self Storage Inc ,119 F. Supp. 2d 1121 (W.D. Washington, 2000)id., section E par. 5

[32] Chance v. Avenue A Inc., 165 F.Supp.2d 1153 (W.D. Wash. 2001).

[33] Theofel v. Farey-Jones, 341 F.3d 978 (9th Cir. 2003)

[34] Rappelons que le CAN-SPAM Act rend inopérante toute Loi qui réglemente expressément l'utilisation du courrier électronique pour l'expédition de messages commerciaux, sauf dans la mesure où les prohibitions qui y sont prévues portent sur les déclarations mensongères ou trompeuses incluses ans quelque portion du message ou des pièces qui y sont jointes. CAN-SPAM Act of 2003, Sec.8 (2)(b)(1)

California Business and Professions Code

Le Code des professions et des affaires californien[35] (CBPC) est une loi gigantesque, comprenant 25 762 articles qui visent entre autres les professions (champs de compétences, permis, discipline, etc.) mais aussi les règles concernant la concurrence, applicables aux commerces opérant dans une multitude de champs d'activités.

La partie 3 (Representations to The Public) de la Division 7 (General Business Regulations) comprend, à son Chapitre 1 (articles 17 500 à 17 594), qui porte sur la publicité, des dispositions qui réglementent des sujets aussi variés que la publicité trompeuse, la sollicitation pour des fins charitables, la vente par téléphone, l'étiquetage des produits destinés aux non voyants, jusqu'à la vente de voyages, en passant par les produits de fabrication autochtone, les machines distributrices, les appareils de traitement de l'eau, le Cyber-piratage et les sollicitations téléphoniques non sollicitées et non désirées.

On y trouve au passage des dispositions qui prévoient les Restrictions applicables aux courriers électroniques commerciaux non sollicités (articles 17529-17529.9)[36] ainsi que certaines infractions particulières (17538.45).

La définition adoptée par le CBPC à l'article 17 529.1 o) pour le courriel non-sollicité est particulièrement inclusive :

> "Unsolicited commercial e-mail advertisement" means a commercial e-mail advertisement sent to a recipient who meets both of the following criteria:
> (1) The recipient has not provided direct consent to receive advertisements from the advertiser.
> (2) The recipient does not have a preexisting or current business relationship, as defined in subdivision (l), with the advertiser promoting the lease, sale, rental, gift offer, or other disposition of any property, goods, services, or extension of credit."

Contrairement à celui que prévoit maintenant le CAN-Spam Act, le choix d'un régime « d'opting-in », soit l'exigence d'un consentement direct préalable à l'envoi du courriel publicitaire, donne son sens véritable à l'expression « courrier non-sollicité ». Toutes les communications qui n'ont pas été expressément sollicitées, sauf celles qui sont faites dans le cadre d'une relation d'affaire préexistante, sont visées par la loi californienne, qui en interdit tout simplement, à son article 17529.2, l'envoi.

Parmi les moyens visant à limiter le déferlement de courriels non sollicités, l'article 17529.4 interdisait diverses pratiques qui sont monnaie courante dans l'industrie du «Spamming», notamment la collecte d'adresses électroniques affichées sur Internet, l'usage de logiciels qui génèrent des adresses électroniques par combinaisons aléatoires de chiffres, lettres et autres caractères, l'ouverture de multiples comptes de messagerie électronique dans le but de s'en servir comme plate-forme d'envoi de pourriel, etc.[37]

---

[35] California Business and Professions Code, disponible en ligne sur le site de **Find**Law, au http://caselaw.lp.findlaw.com/cacodes/bpc.html (page consultée le 6 juillet 2005)~~California Business and Professions Code~~
~~Division 7, Part 3, Chapter 1, Article 1.8. Restrictions On Unsolicited Commercial E-mail Advertisers~~

[36] California Business and Professions Code Division 7, Part 3, Chapter 1, Article 1.8. Restrictions On Unsolicited Commercial E-mail Advertisers (added by Stats. 2003 ch. 487 (S.B. 186), approved September 23, 2003; amended by Stats. 2004 ch. 183 (A.B. 3082), approved July 19, 2004; and Stats. 2004 ch. 571 (S.B. 1457), approved Sept. 17, 2004)

[37] Le CAN-SPAM Act a jusqu'à un certain point repris à son compte ces restrictions par l'interdiction d'obtenir ou de générer des listes par des moyens automatisés. CAN-SPAM Act, section 5 b)

Au chapitre des recours, le CBPC prévoyait à l'article 17529.8. la possibilité pour les particuliers aussi bien que pour les fournisseurs d'accès ou le gouvernement de poursuivre en justice les pourrielleurs qui auraient violé des dispositions de la Loi. Les demandeurs, en plus de réclamer les dommages directs qu'auraient pu leur causer les pourrielleurs, pouvaient obtenir, à titre de dommages exemplaires, une somme de 1000.00$ par courriel publicitaire non sollicité reçu, jusqu'à concurrence de 1 million de dollars et pouvaient demander le remboursement d'honoraires raisonnables engagés dans le cadre du recours. Les poursuites contre le fournisseur d'accès n'étaient toutefois pas permises lorsque ce dernier n'est qu'un tiers passif qui ne fait que véhiculer sur son réseau des messages expédiés par des tiers, sans exercer de surveillance sur leur contenu. Le CBPC prévoyait toutefois que si un expéditeur de courriels publicitaires non sollicités présentait une défense de diligence raisonnable, démontrant qu'il avait pris des moyens adéquats pour tenter de prévenir l'expédition de tels courriels, les sanctions prévues diminuaient dans un ordre de grandeur de 10 (ainsi un particulier verrait les dommages exemplaires maximum qui pouvaient lui être attribués plafonner à 100 000$).

L'article 17529.2 précisait qu'étaient interdits aussi bien les envois de courriels publicitaires non sollicités effectués *à partir* de la Californie que ceux qui étaient *destinés à* une adresse électronique de Californie.

La Loi de 2003 reflétait un durcissement important de la position législative californienne, puisque les dispositions antérieures du CBPC[38] qui visaient la publicité non sollicitée, telles qu'amendées en 1998 (Assembly Bills 1629 et 1676) pour inclure les courriels à titre de mode de transmission, ne prévoyaient qu'une simple obligation de transparence, soit l'indication dans le texte de l'objet véritable du courriel, ainsi que l'indication des coordonnées de l'expéditeur et un régime « d'opting-out »[39]. Une telle relation présuppose, selon les termes de la Loi, qu'il y ait eu une démarche active de la part du consommateur auprès de l'expéditeur de courriels publicitaires (achat ou transaction, demande de renseignements au sujet de produits et services), accompagnée de la transmission au commerçant de l'adresse électronique pour la réception des publicités par courriel.

Les dispositions prévues par le CBPC se révélaient donc à plus d'un titre idéales en vue d'une lutte efficace contre le pourriel : définition inclusive, obligation de consentement positif préalable à tout envoi, possibilités de poursuites par les destinataires (plus susceptibles de nettoyer le marché que les recours réservés aux fournisseurs d'accès), domicile des émetteurs et des récepteurs susceptible d'entraîner l'application des dispositions anti-pourriel, importance des dommages punitifs prévus, illégalité des outils servant à générer des adresses, etc. Cette approche, qui démontrait une véritable intention de provoquer des résultats tangibles, pourrait certes servir d'inspiration à un législateur qui partagerait cette volonté.

[38] Reid, Thelen "California Enacts Two "Anti-Spam" Bills Targeting Unsolicited E-mail"; disponible sur le site de Construction WebLink, au http://www.constructionweblinks.com/Resources/Industry_Reports__Newsletters/Oct_2_1998/oct_2_1998.htm; le texte de AB 1676 est disponible sur le site de CyberspaceLaw, au : http://www.cyberspacelaw.org/loren/ca17538-4.html . Les texte du California Business and Professions Code tels qu'amendés par les AB 1676 et 1629 sont disponibles sur le site de Hostworks International, au http://www.hostwork.com/info/spam.html (pages consultées le 5 juillet 2005)

[39] Business and Professions Code §17538.4 (1998); Les dispositions pertinentes du CPBC prévoit encore un régime « d'opting-out » qui ne s'applique toutefois qu'alternativement, dans le cadre de relations d'affaires préexistantes ou courantes.Sorkin David E. "Spam Laws" In Spam Laws United States. Site de Spam Laws http://www.Spamlaws.com/state/ca1.html (page consultée en décembre 2004)

Virginia Computer Crimes Act

Les dispositions anti-pourriel de la Virginie[40] ont souvent été invoquées devant les tribunaux américains, du fait que le siège social de AOL, l'un des plus grands fournisseurs d'accès à Internet aux États-Unis, se trouve dans cet État. Ces dispositions ont, sur plusieurs aspects, servi d'inspiration au CAN-Spam Act.

Le Virginia Computer Crimes Act (VCCA) définit quantitativement ce qui peut constituer, au sens de la Loi, un « envoi massif de courriels non sollicités », ou UBE (unsolicited bulk electronic mail). Pour répondre à la définition :

a) plus de 10 000 courriels non sollicités doivent avoir été transmis dans les 24 heures, ou
b) 100 000 courriels non sollicités doivent avoir été transmis sur une période de 30 jours, ou
c) 1 million de courriels non sollicités doivent avoir été transmis sur une période de 1 an, ou
d) les revenus générés pour une transmission de courriels non sollicités doivent être de plus de 1000$ ou
e) les revenus générés pour une transmission de courriels non sollicités doivent être de plus de 50 000$ pour l'ensemble des transmissions à un fournisseur de messagerie électronique, ou EMSP (electronic mail service provider).

Sera coupable d'infraction quiconque utilise un ordinateur ou un réseau avec l'intention de forger ou de falsifier des informations de transmission de courrier électronique en lien avec la transmission d'envois massifs ou qui vend, donne, possède ou distribue des logiciels pouvant servir à ces fins.

Le VCCA prévoit que le moindre des montants suivants peut être accordé à une personne (autre qu'un fournisseur de messagerie électronique) à titre de dommages punitifs: 10$ par courriel non sollicité expédié dans le cadre d'un envoi massif ou 25 000$ par jour de transmission de UBE. Les fournisseurs de messageries électroniques peuvent aussi réclamer des dommages de l'ordre de 25 000$ par jour de transmission de UBE ou encore 1$ par courriel non sollicité expédié à chaque abonné du fournisseur de messagerie électronique[41].

La législation de Virginie, qui vise à contrer les crimes informatiques plutôt qu'à enrayer le pourriel, exige donc une preuve très complexe qui doit faire état à la fois de la quantité de messages envoyés et de l'intention de falsifier ou de forger, ou de le permettre par voie logicielle.

La définition de pourriel par voie de qualification quantitative répond clairement aux préoccupations principales que suscite le pourriel. La preuve de la quantité d'envoi, qui est à la charge du plaignant, peut par contre être difficile à établir, sauf bien entendu pour le fournisseur d'accès par lequel transitent ces envois. Une définition du pourriel qui tiendrait compte de la quantité d'envois ou de la nature des envois ou encore du mode d'envoi pourrait certainement faciliter pour les particuliers la preuve contre les pourrielleurs, quitte à prévoir des moyens de défense qui permettent d'écarter les recours non fondés.

Si on les compare aux montants des dommages punitifs qui étaient prévus dans les dispositions californiennes (dommages exemplaires de 1000.00$ par courriel publicitaire non sollicité), le 10$ par courriel non sollicité reçu lors d'un envoi massif de la législation de Virginie, vu le degré

[40] Virginia Computer Crimes Act (Va. Code Ann. § 18.2-152.2 et seq.) (amended effective July 1, 1999) In Legislative Information System, sur le site Internet de Virginia General Assembly, au : http://leg1.state.va.us/cgi-bin/legp504.exe?991+ful+CHAP0886 (page consultée le18 juillet 005)

[41] Sorkin, David E. "Spam Laws" In Spam Laws United States; Virginia. Site de Spam Laws. http://www.Spamlaws.com/state/va.html (page consultée en janvier 2005)~~id.~~

de preuve nécessaire, semble bien conservateur et n'apparaît pas comme une menace aussi sérieuse. Il n'en demeure pas moins que ces deux États avaient tout de même sur le CAN-Spam Act l'avantage d'autoriser les poursuites entreprises par des particuliers.

2. LA SITUATION AU CANADA

Au cours des dernières années, des projets de Loi anti-pourriel spécifiques ont été déposés devant le parlement du Canada, l'un au Sénat, l'autre à la chambre des communes par un sénateur et un député qui croient fermement que le gouvernement doit légiférer en vue de contrôler l'envahissante pratique du pourriel. L'opinion généralement émise à ce sujet laisse au contraire entendre que le Canada disposerait déjà des lois nécessaires pour s'attaquer adéquatement à ce problème.

Dans les pages qui suivent, nous nous pencherons sur ces projets de Loi et sur les lois d'application générale afin de tenter de déterminer les outils qui pourraient sembler les plus propices à la lutte contre les courriels non sollicités.

Nous analyserons ensuite brièvement quelques outils supplémentaires afin de voir s'ils sont susceptibles de trouver application efficace dans la lutte au pourriel.

Les projets de Loi

Soulignons de prime abord que l'adoption d'une législation spécifiquement anti-pourriel ne figure pas dans les priorités de l'agenda du gouvernement canadien, qui entend, à ce jour, lutter contre ce problème avec les lois canadiennes existantes, notamment les lois visant la protection de la vie privée[42]. L'existence de ces projets de Loi nous donne néanmoins des indications sur les voies que pourraient emprunter une législation canadienne visant spécifiquement à contrer le pourriel; c'est à ce titre que nous les examinons.

Projet de Loi C-460 : Loi modifiant le Code criminel (courriel non sollicité) 43
Un projet de Loi privé a été déposé en première lecture le 22 octobre 2003 par le député Dan McTeague, qui visait à faire modifier le Code criminel dans le but d'y ajouter une section (PARTIE VI.I) portant spécifiquement sur le courriel non sollicité (articles 196.1 à 196.5).

Les articles proposés visaient à créer deux nouvelles infractions en rapport avec le pourriel, soit : 1) l'envoi de courriel non sollicité et 2) la vente d'adresses électroniques sans le consentement des personnes touchées. Le projet C-460 prévoyait aussi un régime de sanctions, incluant des amendes et des peines d'emprisonnement.

Le projet de Loi C-460 a franchi l'étape de la première lecture lors de la session parlementaire 2002-2003, mais, comme ce n'était pas un projet de loi du gouvernement, ne disposant pas de ce fait des soutiens nécessaires pour aller au bout du processus d'adoption, le projet est mort au feuilleton et son sponsor a décidé de ne pas le réintroduire lors de la session parlementaire débutant en octobre 2004[44] .

[42] Chezzi, Derek "You've got Spam" In Macleans.ca. Technology . Site de Macleans. http://www.macleans.ca/topstories/technology/article.jsp?content=20040223_75808_75808 (page consultée en décembre 2004)

[43] Le texte du projet de Loi est disponible sur le site Web du Parlement du Canada, in Parlement du Canada. Projets de lois émanant des députés. http://www.parl.gc.ca/37/2/parlbus/chambus/house/bills/private/C-460/C-460_1/C-460_cover-E.html (page consultée le 6 juillet 2005)

[44] 38ème législature, 1ère session

Le projet C-460 définissait (196.1) un « courriel non sollicité » comme étant un message transmis par un expéditeur, à l'exclusion d'un fournisseur d'accès à Internet, à un destinataire, sans relation d'affaires préexistante, et qui a été envoyé sans avoir été demandé et sans le consentement exprès du destinataire. Il visait à faire de la transmission d'un tel courriel non sollicité une infraction et prévoyait les sanctions suivantes: pour une première infraction, une peine d'emprisonnement maximale de 2 ans et/ou une amende de 250 000$, passant à 5 ans d'emprisonnement et/ou une amende de 500 000$ en cas de récidive (196.2).

Le projet C-460 prévoyait des sanctions identiques pour un autre type d'infraction, soit la vente, l'échange ou la transmission sans le consentement de la personne concernée de son adresse électronique (196.3).

Le projet C-460 prévoyait (196.4) une possible défense de diligence raisonnable en vue d'empêcher la commission d'une des infractions mentionnées, sans toutefois en préciser les paramètres ou mentionner ce qui pourrait être invoqué à l'appui d'une telle défense.

Parmi les vides laissés par ce projet, on notera l'absence dans le projet de Loi C-460 d'une définition de ce qui pourrait constituer une « relation d'affaires »; cette lacune est d'autant plus évidente que les versions anglaises et françaises des textes diffèrent. En effet, la version anglaise de la définition de courriel non sollicité faisant référence à une « pre-existing business relationship », alors que la version française parle simplement de relations d'affaires, omettant le qualificatif « préexistante ».

Au vu des autres législations visant à combattre le pourriel, on ne peut s'empêcher de remarquer aussi qu'il manque une définition de la sollicitation, alors que l'absence de sollicitation par le destinataire est l'un des éléments de l'infraction. Le consentement négatif pourrait-il être invoqué à l'encontre d'une infraction ainsi rédigée? Il nous semble qu'une définition du consentement qui, idéalement, ne permettrait que l'usage du consentement positif (opt-in) serait seule susceptible de permettre la mise en application de telles infractions.

D'autre part, on peut s'interroger sur le bien-fondé d'une lutte au pourriel qui passerait par la création d'une nouvelle infraction de responsabilité stricte au cœur du Code criminel. Le pourriel, c'est admis, représente pour le public en général une sérieuse nuisance; la société canadienne est-elle prête à admettre que l'envoi d'un seul courriel non sollicité puisse entraîner pour l'expéditeur un emprisonnement de deux ans ? Nous nous permettrons d'en douter et de croire que les armes envisagées par ce projet sont clairement disproportionnées.

On peut aussi s'interroger sur la pertinence d'inclure au Code criminel un domaine, soit la protection des renseignements personnels, qui fait déjà l'objet de législations spécifiques au fédéral ainsi que dans certaines provinces (Québec, Alberta et Colombie-Britannique) et d'y accoler des peines d'emprisonnement aussi sérieuses, qui ne s'appliqueront, bien entendu qu'aux individus, alors que le pourriel serait principalement le fait d'entreprises commerciales.

Le projet de Loi S-15[45]

Le projet de Loi S-15 n'émane pas non plus du gouvernement; c'est au Sénat qu'il a été déposé. S'il en est présentement au stade de la 2ème lecture au Sénat, il ne faudrait pas présumer trop hâtivement de son adoption prochaine : son sponsor, le sénateur Oliver, a dû réintroduire, pour une troisième fois, ce projet lors de la première session de la 38ème législature (octobre à décembre 2004) puisqu'il n'était pas parvenu à franchir toutes les étapes du processus législatif lors des sessions antérieures[46].

Le projet de Loi S-15, intitulé « *Loi visant à empêcher la diffusion sur Internet de messages non sollicités* », prévoit divers moyens de lutte contre le pourriel (le terme employé dans le texte du projet) qui y est défini comme suit à l'article 2: « un ou plusieurs messages non sollicités envoyés et reçus sur l'Internet, à l'exception des messages qu'une personne envoie à une autre personne avec qui elle a des relations commerciales ou personnelles ».

Le projet de Loi, plutôt que de limiter la définition pour n'inclure que les courriels non sollicités à caractère de promotion ou de vente de produits ou services, inclut tout courriel non sollicité, peu importe sa nature. Le préambule donne toutefois quelques indications sur le problème que vise à corriger la Loi et ne manquerait pas d'être utilisé par les tribunaux pour circonscrire son application[47].

Le projet de Loi ne limite pas non plus les courriels visés aux envois massifs, mais à tout courriel, du moment qu'il n'a pas été sollicité. Cette approche distingue ce projet de Loi de la plupart des législations anti-pourriel, qui tendent à inclure cet élément quantitatif dans les définitions ou dans les éléments de l'infraction.

Tel qu'en fait foi son préambule, les problèmes d'application des législations anti-pourriel dus au caractère international d'Internet ont été pris en compte[48] et le projet de Loi tente de mettre en place des outils susceptibles de surmonter ces problèmes. Le projet de Loi S-15 fait donc état d'une série d'obligations dont aurait à s'acquitter le ministre de l'Industrie, soit: procéder à des consultations avec les représentants des gouvernements des autres provinces et d'autres pays en vue de partager des informations sur des moyens de réduire la problématique du pourriel et instaurer des collaborations nationales et internationales à cette fin. Le ministre devrait ensuite faire rapport de ces activités au parlement[49].

---

[45] Présenté sous S-23 à la Deuxième session de la trente-septième législature, 51-52 Elizabeth II, 2002-2003, puis sous S-2 à la 3e session de la 37e législature, 52 Elizabeth II, 2004, puis sous S-15 à la première session de la trente-huitième législature, 53 Elizabeth II, 2004, le projet de « *Loi visant à empêcher la diffusion sur Internet de messages non sollicités* » peut être consulté en ligne . Parlement du Canada. Projets de lois émanant des sénateurs. Site du Parlement du Canada http://www.parl.gc.ca/38/1/parlbus/chambus/senate/bills/public/pdf/s-15_1.pdf (document consulté en janvier 2005)

[46] Pour qu'un projet de loi soit adopté, il doit franchir l'étape des 3 lectures dans chacune des chambres du parlement lors d'une même session, pour ensuite recevoir la sanction royale du gouverneur général, à défaut de quoi le projet de loi est abandonné.

[47] Projet de Loi S-15, « *Loi visant à empêcher la diffusion sur Internet de messages non sollicités* », Préambule : Attendu que bon nombre de ces messages contiennent ou offrent du matériel pornographique, encouragent des activités illégales ou sollicitent ou offrent des biens ou services qui n'intéressent aucunement les destinataires;

[48] Projet de Loi S-15, « *Loi visant à empêcher la diffusion sur Internet de messages non sollicités* », Préambule :Attendu que, vu le caractère international de l'Internet, tant une collaboration internationale que la coopération et la réglementation des fournisseurs de services Internet au Canada sont requises pour contrôler le flux de ces messages;

[49] Projet de Loi S-15, « *Loi visant à empêcher la diffusion sur Internet de messages non sollicités* », Article 3

Le projet de Loi prévoit aussi la création d'un Conseil de la protection des consommateurs sur Internet ou l'attribution à un organisme existant du mandat à être confié à tel Conseil[50].

Malgré ce que pourrait laisser entendre le nom de ce Conseil, son mandat premier viserait à représenter les intérêts de tous les fournisseurs d'accès Internet canadiens et de leurs clients, en favorisant notamment l'auto réglementation des fournisseurs de services internet (FSI ou ISP : Internet Services Provider), pour ensuite susciter une collaboration pour la création de filtres anti-pourriel ou d'autres modes de contrôle des pourriel, en vue de l'utilisation de ces moyens techniques de contrôle par les FSI. En vertu de l'article 7, il serait interdit d'offrir des services Internet à moins d'être membre du Conseil, ou qu'un des administrateurs ou des propriétaires, dans le cas d'entreprises, n'en soit membre.

L'article 8 du projet de Loi S-15 prévoit qu'une liste anti-pourriel doit être mise en place et tenue à jour. Tout propriétaire d'une adresse électronique pourrait demander à figurer sur cette liste et les personnes qui envoient des courriels non sollicités auraient l'obligation aux termes de l'article 8(3) de s'assurer que les adresses électroniques auxquelles sont destinées ces courriels ne sont pas inscrites sur cette liste anti-pourriel. L'envoi de pourriel à une adresse inscrite à la liste constituerait ainsi, en vertu de l'article 11, une infraction, de même qu'un envoi sans vérification préalable de cette liste anti-pourriel. Le projet de Loi prévoit que cette liste ne serait pas un document public et que les informations y apparaissant ne pourraient être divulguées.

Tout comme le CAN-Spam Act, on voit que ce projet de Loi ne vise pas à interdire le pourriel, mais bien à encadrer l'envoi de courriels non sollicités et à mettre en place des moyens coordonnés pour, à plus long terme, parvenir à contrôler l'envahissement du pourriel. Le projet de Loi S-15 envisage ainsi de soumettre les expéditeurs de courriels non sollicités à plusieurs obligations : un courriel non sollicité doit indiquer clairement la nature du courriel envoyé, l'adresse de l'expéditeur et l'identité des personnes offrant des biens ou services (lorsque tel est l'objet du courriel non sollicité) et offrir au destinataire la possibilité d'envoyer un message anti-pourriel. Tout manquement à ces obligations, de même que les fausses représentations au sujet des biens ou services offerts ou de l'identité ou de l'adresse de l'expéditeur de ces courriels constituerait, en vertu de l'article 11, une infraction.

Le projet de Loi prévoit aussi que la vente, l'échange ou l'offre de vendre ou d'échanger des adresses électroniques dans le but de permettre l'envoi de courriels non sollicités constitueraient des infractions. 11(1) (g).

Une amende maximale de 500$ peut être imposée en cas de déclaration de culpabilité à l'une des infractions prévues. Des peines plus sévères sont toutefois prévues dans certaines circonstances : si les courriels non sollicités contiennent de la pornographie juvénile, la représentation d'une activité sexuelle explicite ou une tentative de frauder le destinataire, une amende maximale de 1000$ et/ou une peine de prison de 6 mois pourront être imposées. Enfin, si les courriels non sollicités étaient, au regard de la cour, conçus pour attirer les enfants (ou destinés à une adresse électronique qui pourrait amener l'expéditeur à croire que des enfants y auraient accès) ou visaient un établissement d'enseignement autre qu'un établissement post-secondaire, l'amende pourrait s'élever à 5000$ et la peine d'emprisonnement être doublée, pour atteindre un maximum de 1 an.

[50] Projet de Loi S-15, « *Loi visant à empêcher la diffusion sur Internet de messages non sollicités* », Article 4

Contrairement à ce que prévoit le CAN-Spam Act, les victimes du pourriel pourraient s'adresser directement aux tribunaux en vue de réclamer les dommages que leur aurait causés la réception de messages non sollicités expédiés en contravention à la Loi. En vue de faciliter la preuve, l'article 17 crée une présomption : si une personne reçoit des courriels non sollicités en « quantité excessive », des dommages seront présumés même s'ils ne peuvent être établis de manière spécifique et des dommages-intérêts pourraient être accordés dans le cadre d'un recours civil. Le texte du projet de Loi ne précisant pas ce qui peut constituer une quantité excessive de courriels non sollicités, il reviendrait donc aux tribunaux le soin de déterminer, selon les particularités de chaque dossier, ce qui devrait être considéré comme une quantité excessive.

En vue de contrer toute objection qui pourrait être soulevée quand à l'applicabilité de la Loi aux entreprises étrangères, l'article 14 adopte une solution originale, créant une présomption irréfragable quant à la provenance du pourriel: tout courriel non sollicité reçu au Canada sera réputé avoir été envoyé au Canada.

On constate dans ce projet de Loi des ressemblances avec certaines approches adoptées par le CAN-Spam Act (la volonté, par exemple, d'encadrer plutôt que de bannir les pourriels, mise sur pied d'une liste anti-pourriel) ainsi que certaines dissemblances qui portent principalement sur l'application de ces lois et sur les moyens mis en œuvre en vue d'apporter au problème une solution à long terme.

Il nous semble indispensable que les recours prévus dans le cadre d'une législation anti-pourriel soient accessibles à toutes les victimes de ces envois non sollicités. L'approche adoptée par le projet de Loi S-15 a donc sur le CAN-Spam Act l'avantage de permettre aux individus de s'adresser directement aux tribunaux et l'intelligence de créer quelques présomptions susceptibles de faciliter la preuve.

Dans le cadre d'une législation qui ne vise qu'à « policer » l'envoi des pourriels, les obligations auxquelles sont soumis les expéditeurs semblent aller de soi. La mise sur pied d'une liste antipourriels, quoiqu'elle impose aux éventuels destinataires plutôt qu'aux expéditeurs l'obligation d'une démarche positive, soit l'inscription sur la liste, plutôt que d'exiger de l'expéditeur l'obtention d'un consentement préalable à l'envoi, pourrait se révéler une approche efficace, pour autant que l'application des règles soit aussi stricte que possible et que les contrevenants encourent un risque réel d'être soumis à des peines dissuasives.

Les obligations imposées au ministre de travailler en collaboration à l'échelle internationale, aussi peu contraignantes soient-elles (le projet de Loi n'exigeant en fait que consultations, partage d'informations et recherche de solution) ont tout de même l'avantage d'imposer des actions qui vont au-delà des vœux pieux.

Alors que la création d'un Conseil de la protection des consommateurs sur Internet semble à prime abord une heureuse initiative, le fait que ce Conseil ne regroupe en réalité que les fournisseurs d'accès (et toute personne proposée par le ministre) et que son mandat soit de représenter à la fois « les intérêts de tous les fournisseurs de services Internet au Canada et de leurs clients », qui, admettons-le, peuvent souvent être en conflit, laisse penser que le nom même de ce Conseil est susceptible d'induire en erreur. Le fait qu'on puisse penser à créer un Conseil de la protection des consommateurs sans songer à imposer la présence sur ce Conseil d'une représentation importante de groupes qui oeuvrent à la défense de leurs droits laisse pour le moins perplexe. De même, s'il semble logique de croire que l'auto-réglementation par les FSI puisse atteindre ses buts lorsqu'il s'agit de veiller à leurs propres intérêts, on peut douter

de l'efficacité de ce type d'intervention lorsqu'il s'agit de veiller au meilleur intérêt de leurs clients, voire l'estimer dangereuse.

Tout en étant conscient que la liste antipourriel recèle des enjeux qui relèvent de la protection des renseignements personnels, on peut aussi se questionner sur la pertinence d'inclure dans une Loi visant à empêcher la diffusion sur Internet de messages non sollicités des dispositions spécifiques sur la communication et le partage de renseignements, soit les adresses électroniques, attendu que l'inclusion de telles dispositions dans une loi particulière soumettent leur application à l'ensemble des dispositions de cette Loi et que ces dispositions risquent de mettre en péril l'application des lois générales, fédérales ou provinciales, portant sur la protection des renseignements personnels.

Aussi imparfait soit-il, on pourrait à tout le moins accorder à ce projet de Loi (et à ses dépôts à répétition) le mérite de médiatiser la problématique de la lutte au pourriel et l'absence actuelle d'un texte statutaire anti-pourriel spécifique. L'approche adoptée par ce projet de Loi et certaines de ses dispositions pourraient même servir de base de réflexion au législateur dans l'hypothèse où celui-ci déciderait d'intervenir sur la question du pourriel.

Le projet de Loi 69[51]

Les efforts législatifs pour tenter de contrer le pourriel ne se limitent pas aux projets de loi fédéraux. En Ontario, un projet de loi privé intitulé Loi visant à empêcher la diffusion sur Internet de messages non sollicités a été déposé en avril 2004 par un député ontarien et a franchi l'étape de la 1ère lecture. En substance, ce projet reprend plusieurs des éléments du projet de Loi S-15 présenté au Sénat par le sénateur Oliver. La définition donnée à « pourriel », par exemple, est exactement la même que celle que l'on retrouve dans le projet de Loi S-15. Tout comme le projet de Loi S-15, ce projet créerait une obligation pour le ministre responsable de ce dossier de procéder à des consultations auprès de divers intervenants (autres gouvernements, représentants de l'industrie) et de faire rapport des progrès réalisés en matière de coopération dans la lutte au pourriel. L'article 4 du projet S-15 prévoit la création d'une liste anti-pourriel (régime d'opt-in) et l'article 9 crée le même type de présomption que celle établie dans le projet de Loi S-15; ainsi un courriel non sollicité reçu en Ontario serait réputé provenir de l'Ontario. Finalement, les sanctions imposées seraient ici aussi plus sévères dans certains cas (ex. messages s'adressant aux enfants, messages contenant de la pornographie, etc.).

Attendu que le gouvernement fédéral tarde à s'engager activement sur la voie législative en vue de contrer le pourriel, les initiatives provinciales sont évidemment bienvenues, ne serait-ce que pour les pressions qu'elles sont susceptibles d'exercer en faveur d'une réglementation plus vaste, qui serait probablement mieux en mesure de s'attaquer à un problème qui est de par sa nature même transfrontalier. Il faut toutefois garder à l'esprit que le partage des compétences entre les législateurs provinciaux et le fédéral fait en sorte que des législations concurrentes soulèveraient certes plusieurs questions et, probablement, quelques réticences.

Les lois actuelles

Plusieurs soutiennent que les lois canadiennes actuelles contiennent déjà les dispositions nécessaires pour permettre de lutter efficacement contre la problématique du pourriel. Ainsi, selon le professeur Michael Geist, la majorité des actions visées par les principales législations

[51] Projet de Loi 69 : Loi visant à empêcher la diffusion sur Internet de messages non sollicités In pourriel.ca. Site de pourriel.ca http://www.pourriel.ca/divers/69.pdf (~~page~~ document consulté~~e~~ en décembre 2004)

anti-pourriel actuellement en vigueur ailleurs dans le monde sont couvertes par nos lois actuelles[52]. Le véritable problème résiderait plutôt alors dans la mise en application de ces lois par les autorités responsables.

Les lois invoquées, dans leur diversité, visent des objectifs et prévoient des moyens différents qui pourraient effectivement, dans certains cas, être invoqués contre les pourrielleurs au vu de certaines de leurs pratiques (ex : protection de la vie privée, fraudes, etc). Sans mettre fin au pourriel, certaines de ces lois permettraient ainsi une lutte indirecte qui, à défaut de stopper le déluge des courriels non sollicités, pourraient être conjuguées pour mettre un peu d'ordre et imposer une certaine discipline aux expéditeurs en leur indiquant clairement ce qu'il peut leur en coûter de dépasser certaines bornes.

Nous effectuerons dans la partie qui suit un survol de ces lois et de leur application possible au pourriel.

La Loi sur les télécommunications[53]

En vertu de l'article 41 Loi sur les télécommunications: « le Conseil (Conseil de la radiodiffusion et des télécommunications canadiennes (CRTC)) peut, par ordonnance, interdire ou réglementer, 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 »[54]. La définition que donne la Loi sur les télécommunications de services de télécommunication (art. 2) se lit comme suit : « *La transmission, l'émission ou la réception d'information soit par système électromagnétique, notamment par fil, câble ou système radio ou optique, soit par tout autre procédé technique semblable* ».

La Loi sur les télécommunications énonce, à son article 7, les divers objectifs de la politique canadienne en matière de télécommunication; parmi ceux-ci on note aux alinéas a) favoriser le développement ordonné des télécommunications; h) satisfaire les exigences économiques et sociales des usagers des services de télécommunication et i) assurer la protection de la vie privée des personnes. Au vu de ces dispositions, il pourrait sembler qu'une lutte au pourriel menée sous l'égide du CRTC bénéficierait de la force et des moyens nécessaires à assurer son efficacité et que cet organisme serait le mieux placé, vu le contrôle qu'il exerce déjà sur les entreprises de télécommunications et celles qui oeuvrent dans des domaines connexes, pour mener à bien cette lutte.

Malheureusement, même si le CRTC possède le mandat et les pouvoirs nécessaires pour intervenir, le Conseil a choisi de ne pas exercer ses pouvoirs dans le domaine de la lutte au pourriel : ainsi, même si des directives ont été implantées pour encadrer la pratique du télémarketing par téléphones et télécopieurs, rien n'a encore été fait en ce qui a trait au pourriel. Le CRTC a, en fait, déjà clairement indiqué qu'il n'entendait pas réglementer Internet, du moins

[52] Lalonde Jean « Les lois canadiennes –actuelles seraient suffisantes » In pourriel.ca. Politique légal. Site de pourriel.ca http://www.pourriel.ca/archives/000749.php (page consultée le 23 mars 2005)

[53] Le texte intégral de la Loi sur les télécommunications (1993 ch. 38) est disponible sur le site Internet du Conseil de la radiodiffusion et des télécommunications canadiennes, au http://www.crtc.gc.ca/frn/LEGAL/TELECOM.HTM (page consultée le 10 juillet 2005)

[54] Loi sur les télécommunications, (1993 ch. 38) 41. (The Commission may, by order, prohibit or regulate the use by any person of the telecommunications facilities of a Canadian carrier for the provision of unsolicited telecommunications to the extent that the Commission considers it necessary to prevent undue inconvenience or nuisance, giving due regard to freedom of expression.)

en ce qui a trait au contenu[55]. En effet, certaines activités liées à Internet sont bel et bien réglementées par le CRTC, mais les interventions du Conseil se limitent essentiellement à quelques directives qui encadrent les pratiques des FSI entre eux (ex. partage des réseaux).

Les règles de procédure du CRTC prévoient qu'une requête en vertu de la « partie VII » de la Loi sur les télécommunications peut être déposée sur toute question qui ne serait pas visée par les autres types de requêtes. Théoriquement, il serait donc possible pour un FSI ou un particulier de demander spécifiquement au CRTC d'intervenir sur la question du pourriel.

Par contre, tant et aussi longtemps que le Conseil reste sur sa position et qu'il refuse d'intervenir sur le contenu en ce qui a trait à Internet et attendu que le CRTC garde toute discrétion pour intervenir ou pas suite à ce type de requête, cette porte semble pour l'instant bel et bien close.

Code criminel

Le Code criminel contient certaines dispositions sur la fraude ou l'utilisation non-autorisée d'un ordinateur qui pourraient être invoquées dans le cadre de la lutte contre le pourriel, en autant que la preuve puisse être faite que les pourrielleurs commettent, sciemment et intentionnellement, les actes qui y sont prévus.

Parmi les nouvelles pratiques de pourriel, on remarque par exemple le Phishing, qui connaît une croissance remarquable et qui représentait en décembre 2004 2,17 % des pourriels envoyés[56]. En avril 2005, l'*Anti-Phishing Working Group* dénombrait à 14 411 les campagnes de Phishing, qui accusent une hausse moyenne de 15% par mois entre avril 2004 et avril 2005[57]. En imitant les sites Internet d'institutions financières respectables et en y attirant des internautes pour les dépouiller de leurs informations personnelles et de leur argent, les auteurs se rendent donc coupables, à première vue, de contrefaçon, d'utilisation de marques réservées, de fausses représentations, de fraude, de vol d'identité et de vol. Le tout par le bais d'un courriel non sollicité qui constitue de fausses représentations. Plusieurs dispositions du Code criminel pourraient évidemment recevoir application…si les auteurs de ces pratiques étaient pris.

L'art. 380 prévoit que: « Quiconque, par supercherie, mensonge ou autre moyen dolosif, constituant ou non un faux semblant au sens de la présente Loi, frustre le public ou toute personne, déterminée ou non, de quelque bien, service, argent ou valeur est coupable d'un acte criminel »[58]. En cas de déclaration de culpabilité, la peine peut aller jusqu'à 10 ans

[55] "Le CRTC ne réglementera pas Internet" In CRTC Communiqué. Site du Conseil de la radiodiffusion et des télécommunications canadiennes. http://www.crtc.gc.ca/frn/NEWS/RELEASES/1999/R990517.htm (page consultée en décembre 2004)

[56] Selon les statistiques de janvier 2005 rapportées sur le site Internet de Le Journal du Net, disponible au http://www.journaldunet.com/cc/03_internetmonde/spam.shtml (page consultée le 10 juillet 2005

[57] Le *Anti-Phishing Working Group* définit ainsi le Phishing et sa variante, le Pharming: Phishing attacks use both social engineering and technical subterfuge to steal consumers' personal identity data and financial account credentials. Social-engineering schemes use 'spoofed' e-mails to lead consumers to counterfeit websites designed to trick recipients into divulging financial data such as credit card numbers, account usernames, passwords and social security numbers. Hijacking brand names of banks, e-retailers and credit card companies, phishers often convince recipients to respond. Technical subterfuge schemes plant crimeware onto PCs to steal credentials directly, often using Trojan keylogger spyware. **Pharming** crimeware misdirects users to fraudulent sites or proxy servers, typically through DNS hijacking or poisoning. Pour plus de détail sur l'évolution de cette pratique, voir le Phishing AvtivityTrend Report, april 2005, http://antiphishing.org/APWG Phishing Activity Report April 2005.pdf disponible sur le site Internet de *Anti-Phishing Working Group, au* http://www.antiphishing.org/ (site visité et document consulté le 10 juillet 2005)

[58] Code Criminel, L.R. 1985, ch. C-46

d'emprisonnement si le montant de la fraude est supérieur à 5000$ ou d'un maximum de 2 ans pour les fraudes sur des montants inférieurs[59].

Soulignons toutefois que seulement 1,94% des auteurs de Phishing trouvent leur hôte au Canada, et que le Canada n'apparaît pas dans la liste des pays les plus menacés par le Phishing[60]. En fait, toutes les dispositions visant les conduites frauduleuses pourraient être invoquées contre les expéditeurs de pourriel frauduleux ou des courriels qui tentent par un moyen ou par un autre de frauder le destinataire. Le moyen et la technologie utilisés pour commettre un acte criminel n'ont que peu d'importance dans la détermination de la commission de l'acte criminel. Cette possibilité ne doit toutefois pas faire perdre de vue que le problème du «Spamming» ne doit pas être confondu avec les buts frauduleux que vise une certaine proportion du pourriel. Soulignons de plus que cet article, puisqu'il vise un fait accompli, soit une fraude réussie, ne pourrait être utilisé pour contrer les envois qui viseraient à tromper le destinataire si ce dernier refuse cette offre et n'est pas effectivement victime de la fraude.

L'article suivant, 381 C.cr, rend coupable la transmission de « lettres ou de circulaires concernant des projets conçus ou formés pour leurrer ou frauder le public, ou dans le dessein d'obtenir de l'argent par de faux semblants », mais limite cette infraction aux envois postaux.

Pour s'attaquer au «Spamming», plutôt qu'aux criminels, le Code criminel recèlerait quelques dispositions qui pourraient peut-être servir à un contrôle plus généralisé dans une lutte anti-pourriel.

L'article 342.1(1) c) du Code criminel prévoit par exemple que quiconque, d'une manière frauduleuse et sans apparence de droit, directement ou indirectement, se sert d'un ordinateur pour commettre une infraction prévue à l'article 430 (détruire ou modifier des données, empêcher, interrompre ou gêner l'utilisation de données) se rend coupable d'un acte criminel.

Nous nous permettons de douter de la pertinence de cette disposition en ce qui a trait à l'envoi de courriels non sollicités, puisque le pourriel en soi, contrairement à certains virus informatiques, ne détruit ni ne modifie les données, pas plus qu'il n'empêche leur utilisation. Nous soulignerons aussi le fait qu'une utilisation qui contreviendrait aux limites contractuelles imposées par le fournisseur de service dans le cadre d'un contrat en bonne et due forme qui autorise à tout le moins l'autorisation ne saurait à notre avis répondre à la définition de « sans apparence de droit » pas plus qu'à celle de « frauduleuse ». Il existe une immense différence entre le « hacking », soit l'accès non autorisé à un ordinateur ou à un système et le non respect des conditions d'utilisation d'un accès autorisé. Le Code criminel ne peut et ne doit servir à régler le non-respect de certaines clauses contractuelles entre deux particuliers.

Nous insistons sur le fait que, peu importe la technologie utilisée, toute infraction à un acte criminel peut entraîner la sanction prévue par la loi, mais qu'il n'est pas de la nature du pourriel d'être criminel et que la lutte au pourriel doit viser le contrôle d'une épidémie plutôt que la chasse à quelques criminels qui se servent de ce médium pour commettre leurs méfaits.

Nous opposerons les mêmes réserves face à l'article 342.1 (1) b), qui interdit d'intercepter ou de faire intercepter toute fonction d'un ordinateur frauduleusement et sans apparence de droit. Certains y ont vu une arme qui pourrait être utilisée pour contrer la collecte automatisée

[59] Code Criminel, L.R. 1985, ch. C-46, art.380 (1)

[60] Selon les statistiques de janvier 2005 rapportées sur le site Internet de Le Journal du Net, disponible au http://www.journaldunet.com/cc/03_internetmonde/spam.shtml (page consultée le 10 juillet 2005)

d'adresse de courriel sur le Web. Avec respect pour les opinions contraires, nous voyons difficilement comment un outil informatique qui recueille des adresses de courriel qui ont été postées sur Internet (le procédé nommé « harvesting ») et qui sont par le fait même accessibles à tous pourrait être considéré comme « interceptant des fonctions », pas plus que nous ne pourrions expliquer en quoi l'automatisation de cette collecte la rendrait frauduleuse.

Il nous semble donc que la tentation d'utiliser le Code criminel en vue d'une lutte contre le pourriel découle d'une certaine confusion entre la problématique du pourriel elle-même et les actes criminels auxquels peuvent se livrer certaines personnes ou entreprises par le biais du pourriel. Nous sommes donc d'avis que, si les criminels doivent être poursuivis en vertu des lois adéquates, le Code criminel n'est pas de nature à être d'un grand secours dans le cadre d'une lutte concertée contre un phénomène qui relève du marketing plus directement que de la criminalité.

La Loi sur la protection des renseignements personnels dans le secteur privé[61]

Le pourriel constitue, dans une certaine mesure, une atteinte à la vie privée, du fait que des messages, la plupart du temps en vue de sollicitation, sont expédiés à une adresse personnelle sans avoir été préalablement sollicités.

La Loi québécoise sur la protection des renseignements personnels dans le secteur privé (LPRPSP) s'applique à toute personne qui collecte, utilise ou transmet à des tiers, des renseignements personnels dans le cadre de l'exploitation d'une entreprise[62]. « Entreprise » s'entend au sens, assez large, que lui donne le Code civil du Québec à l'article 1525, soit: «l'exercice par une ou plusieurs personnes, d'une activité économique organisée, qu'elle soit ou non à caractère commercial, consistant dans la production ou la réalisation de biens, leur administration ou leur aliénation, ou dans la prestation de services »[63]. Le terme « renseignement personnel » est défini à l'article 2 de la LPRPSP : « est un renseignement personnel, tout renseignement qui concerne une personne physique et permet de l'identifier ».

La LPRPSP insiste sur le caractère confidentiel des renseignements personnels et sur le devoir des entreprises qui les recueillent de veiller au maintien de cette confidentialité. Une entreprise ne peut donc légalement vendre ou, sauf exceptions, transmettre à des tiers des renseignements personnels sans le consentement des personnes concernées, consentement qui doit, selon l'article 14, être manifeste. L'article 6 précise d'ailleurs que « La personne qui recueille des renseignements personnels sur autrui doit les recueillir auprès de la personne concernée, à moins que celle-ci ne consente à la cueillette auprès de tiers. »

En ce qui a trait aux listes nominatives, la LPRPSP prévoit à son article 23 que « Une personne qui exploite une entreprise peut, sans le consentement des personnes concernées, utiliser, à des fins de prospection commerciale ou philanthropique, une liste nominative de ses clients, de ses membres ou de ses employés. » et que : « La personne qui utilise à ces fins une telle liste nominative doit accorder aux personnes concernées une occasion valable de refuser que des renseignements personnels les concernant soient utilisés à de telles fins. »

[61] La ~~l~~Loi sur la protection des renseignements personnels dans le secteur privé, L.R.Q., P-39.1

[62] La ~~l~~Loi sur la protection des renseignements personnels dans le secteur privé, L.R.Q., P-39.1, art. 1 – Le texte intégral de la Loi peut être consulté en ligne sur le site Internet de L'Institut canadien d'information juridique (IIJCan), au : http://www.canlii.org/qc/legis/loi/p-39.1/20040323/tout.html (page consultée le 10 juillet 2005)

[63] C.C.Q., article 1525 – Le texte intégral de la Loi peut être consulté en ligne sur le site Internet de L'Institut canadien d'information juridique (IIJCan), au : http://www.canlii.org/qc/legis/loi/ccq/20050513/tout.html (page consultée le 10 juillet 2005)

Le libellé de cette disposition incorpore les réserves que l'on retrouve habituellement dans les lois ou codes qui visent les courriels non sollicités; l'utilisation par une entreprise de la liste nominative de *ses* clients rejoint en effet les « relations existantes » dont on peut trouver mention dans la plupart de ces textes et « l'occasion valable de refuser » est explicitée dans plusieurs de ces textes qui exigent une adresse de retour valable à laquelle le destinataire peut signifier son désir de ne plus recevoir de communications.

La LPRPSP prévoit, en cas de violation de ses dispositions, soit le fait de recueillir, détenir, communiquer à un tiers ou utiliser un renseignement personnel sur autrui sans se conformer à une disposition des sections II, III ou IV, des amendes qui vont de 1000 à 10 000$; ces amendes passent de 10 000 à 20 000$ en cas de récidive. Le fait pour une entreprise de vendre ou de transmettre à des pourrielleurs les informations personnelles de ses clients constituerait donc une infraction au sens de la LPRPSP. La LPRPSP ne prévoit toutefois aucun recours direct qui pourrait être entrepris par le destinataire de pourriels en vue d'obtenir réparation, que ce soit contre l'expéditeur ou contre celui qui aurait communiqué ses renseignements personnels.

La LPRPSP pourrait donc présumément être utilisée pour porter à l'amende certains expéditeurs de pourriel, ceux qui font circuler les listes d'adresses ou ceux qui omettent d'inclure à leurs courriels la possibilité de signifier son intention de ne plus recevoir de cet expéditeur ce type de messages.

Un des problèmes que l'on rencontre pour l'application de cette loi qui vise la protection des renseignements personnels tient justement à la définition de « renseignements personnels ». Une adresse de courriel constitue-t-elle *en soi* un renseignement qui concerne une personne physique et permet de l'identifier? Il apparaît évident qu'une simple adresse de courriel ne pourra, sauf exception, permettre d'individualiser son propriétaire, de l'identifier. Si une adresse de courriel ne répond pas à la définition de « renseignement personnel », aucune des dispositions visant l'utilisation, la collecte ou la transmission de renseignements personnels ne saurait donc s'appliquer aux adresses de courriel. Il nous semble donc que la protection des renseignements personnels ne visera que les adresses de courriel qui permettent véritablement d'identifier son propriétaire ou celles qui seront liées à des renseignements qui permettraient de le faire, l'ensemble de ces informations constituant dès lors des renseignements personnels.

Une législation spécifique aurait bien entendu sur une loi plus générale visant la protection des renseignements personnels l'avantage d'écarter toute ambiguïté quand à la protection accordée aux adresses de courriels et à son application aux pourriels. De plus, le contexte particulier au pourriel pourrait probablement justifier, dans une législation qui viserait à l'enrayer, une approche plus directe, moins conciliante relativement à l'utilisation des renseignements, vu l'ampleur du problème auquel elle serait circonscrite. Les recours directs en recouvrement des dommages et en dommages punitifs pourraient de même aisément être incorporés à une loi de ce type.

La Loi sur la protection des renseignements personnels et les documents électroniques[64]
La Loi fédérale sur la protection des renseignements personnels et les documents électroniques (Personal Information Protection and Electronic Documents Act - PIPEDA) a un champ d'application assez vaste : elle vise toutes les communications interprovinciales ou internationales et protège tous les renseignements personnels recueillis, utilisés ou communiqués dans le cadre d'activités commerciales; la PIPEDA vise aussi les activités intra-provinciales dans la mesure où la province dans laquelle opèrent les entreprises n'a pas de loi jugée essentiellement similaire à la Loi fédérale[65].

En vertu de l'article 4(1), toute organisation qui recueille, utilise ou communique des renseignements personnels dans le cadre d'activités commerciales, est assujettie à la PIPEDA. Par organisation on entend *notamment* les associations, sociétés et organisations syndicales. La définition de « renseignement personnel » est plus restrictive que celle de la Loi québécoise (LPRPSP) puisqu'elle exclut expressément un certain nombre d'informations, qui ne touchent toutefois que les informations liées à l'emploi, et non à la vie privée : « tout renseignement concernant un individu identifiable, à l'exclusion du nom et du titre d'un employé d'une organisation et des adresses et numéros de téléphone de son lieu de travail »[66].

Dans une première décision portant sur le pourriel, le Commissariat à la protection de la vie privée a récemment interprété de manière restrictive cette définition statutaire en refusant d'inclure dans les renseignements non protégés l'adresse électronique au travail et jugeant qu'un courriel publicitaire sans lien avec l'emploi de monsieur Geist, envoyé à cette adresse, contrevenait à la PIPEDA. Le Commissaire note que: « The sale of seasons tickets to a football game is not related to the purpose for which the University of Ottawa makes a listing of its faculty publicly available »[67]. L'adresse électronique ayant été utilisée à d'autres fins que celles pour lesquelles elle avait été "transmise", cette utilisation se trouve donc être fautive.

La PIPEDA confirme que les organisations sont responsables des renseignements personnels dont elles ont la gestion ou qui sont en leur possession et que cette responsabilité implique que les moyens nécessaires doivent être pris pour assurer la protection de ces renseignements personnels, qui ne peuvent, sauf exception, être utilisés ou transmis sans le consentement de la personne concernée.

Les principes applicables au consentement sont prévus à l'article 5(1) de la PIPEDA, qui procède par renvoi : « Sous réserve des articles 6 à 9, toute organisation doit se conformer aux obligations énoncées dans l'annexe 1. ». L'annexe 1, intitulée *Code type sur la protection des renseignements personnels*, CAN/CSA-Q830-96, reprend pour sa part certains des Principes énoncés dans la norme nationale du Canada. Le troisième principe, énoncé à 4.3 se lit comme suit : « *Toute personne doit être informée de toute collecte, utilisation ou communication de renseignements personnels qui la concernent et y consentir, à moins qu'il ne soit pas approprié*

[64] La L~~l~~oi sur la protection des renseignements personnels et les documents électroniques L.C. 2000, ch. 5. Le texte intégral de la Loi peut être consulté en ligne sur le site du Ministère de la justice du Canada, au http://lois.justice.gc.ca/fr/P-8.6/86834.html (page consultée le 10 juillet 2005)
[65] ~~id.~~ La ~~loi~~Loi sur la protection des renseignements personnels et les documents électroniques L.C. 2000, ch. 5, ~~,~~ art. 26 (2). Le Commissariat à la vie privée du Canada rapporte que seuls le Québec, l'Alberta et la Colombie-Britannique ont adopté à ce jour une loi similaire. Voir à cet effet la Fiche d'information produite par le Commissariat, disponible en ligne sur le site du Commissariat à la vie privée du Canada, au http://www.privcom.gc.ca/fs-fi/02_05_d_15_f.asp (page consultée le 10 juillet 2005)
[66] La ~~loi~~Loi sur la protection des renseignements personnels et les documents électroniques L.C. 2000, ch. 5, ~~id.,~~ art.2
[67] Commissariat à la protection de la vie privée, Décision no. 6100-00780 et 6100-00781 au sujet de M. Michael Geist (plaignant) rendue le 1er décembre 2004 : http://www.mgblog.com/resc/GeistPCCSpamdecision.pdf (document consulté le 25 avril 2005)

de le faire ». Une note complémentaire élabore sur l'énoncé (in fine) de 4.3 et indique, parmi les situations prévues, qu': « *il peut être peu réaliste pour (…) une entreprise de marketing direct souhaitant acquérir une liste d'envoi d'une autre organisation de chercher à obtenir le consentement des personnes concernées. On s'attendrait, dans de tels cas, à ce que l'organisation qui fournit la liste obtienne le consentement des personnes concernées avant de communiquer des renseignements personnels ».* On doit donc comprendre que l'autorisation, dans ces cas, devrait être obtenue pour la transmission plutôt que pour la collecte lorsqu'il s'agit des informations personnelles apparaissant dans des listes d'envoi.

Malgré toutes les exceptions prévues à la Loi et aux Principes relativement à l'exigence d'un consentement, la PIPEDA spécifie bien à son article 5(3) qu'une organisation ne peut recueillir, utiliser ou communiquer des renseignements personnels « *qu'à des fins qu'une personne raisonnable estimerait acceptables dans les circonstances* ».

En cas de violation de la PIPEDA, une plainte peut être déposée devant l'organisme chargé de veiller à son application, soit le Commissariat à la protection de la vie privée[68]. Suite au rapport du Commissaire, qui inclura le cas échéant conclusions et recommandations, le plaignant pourra porter l'affaire devant la Cour fédérale, à qui il reviendra de déterminer des ordonnances qui doivent être rendues et qui pourra accorder au plaignant des dommages-intérêts, notamment en réparation de l'humiliation subie (article 16 (c)).

Nous pourrions répéter ici en substance les commentaires amenés en guise de conclusion à notre survol de la LPRPSP, qui trouvent encore application, essentiellement pour les mêmes motifs.

La disposition qui ouvre la possibilité pour un plaignant d'obtenir réparation n'apporte pas, à notre avis, un avantage bien considérable à une victime du pourriel. La procédure qui prévoit un examen préalable par le Commissariat et le fait que les dommages-intérêts doivent être demandés à la Cour fédérale suite à son rapport nous semblent compliquer inutilement une procédure qui pourrait de toute façon être présentée devant un tribunal de droit commun, en autant que les dommages puissent être prouvés. Nous avons précédemment signalé à cet effet les avantages qu'apportent certaines approches législatives adoptées dans le cadre de la lutte au pourriel qui prévoient d'une part des présomptions qui facilitent la preuve à être faite par le plaignant et, d'autre part, des dommages punitifs quantifiés auxquels la PIPEDA n'ouvre pas la porte.

La précision qu'apporte la PIPEDA sur l'utilisation des renseignements personnels qui doit absolument être restreinte aux *fins qu'une personne raisonnable estimerait acceptables* mériterait bien, pour sa part, d'être soulevée devant le Commissariat et les tribunaux en ce qui a trait au pourriel. Un débat judiciaire sur cette question pourrait permettre de déterminer le degré d'acceptabilité dans une société libre et démocratique des pratiques liées aux courriels publicitaires non sollicités et, le cas échéant, servir d'argument pour inciter les gouvernements à légiférer sur cette question.

[68] Incidemment, mentionnons que « Le Commissariat à la protection de la vie privée du Canada n'est plus en mesure de traiter les plaintes envoyées par courriel. Veuillez donc soumettre votre plainte par courrier. » Site Internet du Commissariat à la vie privée, au http://www.privcom.gc.ca/contactUs/index_f.asp (page consultée le 18 juillet 2005)

La Loi sur la concurrence[69]

Comme nous l'avons vu plus haut, il est courant pour les pourrielleurs d'user d'indications trompeuses dans l'intitulé de l'objet des courriels envoyés ou dans le contenu des courriels, afin d'amener le destinataire ne serait-ce qu'à ouvrir le dit courriel. Certaines approches législatives qui visaient à contrôler le pourriel ont d'ailleurs pensé à intégrer des dispositions rendant illégales ces pratiques.

C'est la Loi sur la concurrence qui, au Canada, vise à contrôler ce type de pratiques. La Partie VII.1, qui porte sur les pratiques commerciales trompeuses, indique que : « Est susceptible d'examen le comportement de quiconque donne au public, de quelque manière que ce soit, aux fins de promouvoir directement ou indirectement soit la fourniture ou l'usage d'un produit, soit des intérêts commerciaux quelconques (…) des indications fausses ou trompeuses sur un point important »[70]. Les sanctions prévues en cas d'offense peuvent aller de l'injonction visant à empêcher la poursuite d'une telle conduite à l'imposition d'amendes allant de 50 000$ à 100 000$ dès la première offense (selon que le contrevenant soit une personne physique ou morale)[71], peines auxquelles peuvent même s'ajouter dans certains cas des peines d'emprisonnement[72].

Le Bureau de la concurrence, chargé de l'application de la Loi sur la concurrence, possède, en vue de l'accomplissement de son mandat, des pouvoirs très étendus, incluant l'usage de mandats de perquisition (visant des lieux ou des ordinateurs) ou d'ordonnances de production de dossiers. Le Bureau a aussi le pouvoir de convenir avec les contrevenants d'engagements[73] qui peuvent emporter diverses obligations, dont celle de rembourser les victimes des actes qui leur sont reprochés.

Le Bureau de la concurrence pourrait vraisemblablement utiliser pour lutter contre les pourrielleurs ses vastes pouvoirs d'enquête et les dispositions qui portent sur les pratiques commerciales trompeuses, les fausses représentations de certains pourriels répondant aux critères qui en font des comportements susceptibles d'examens au sens de la Loi. Dans le cas où des plaintes seraient portées en vertu de la Loi sur la concurrence, il resterait bien sûr à déterminer ce qui, dans un courriel, constitue « un point important ». Alors que les législations qui visent directement le pourriel incluent généralement des dispositions interdisant *toute* fausse information, qu'elles se trouvent dans le corps du message ou dans sa présentation, on pourrait s'interroger, dans l'examen d'un courriel publicitaire entrepris sous l'angle d'une loi sur la concurrence, sur l'importance toute relative que pourrait par exemple présenter l'objet ou l'intitulé du message.

Comme nous le mentionnions dans notre survol du Code criminel, il importe de ne pas confondre la problématique du pourriel et les comportements trompeurs ou illégaux de certains expéditeurs. S'il est admis que les contrevenants doivent être poursuivis en vertu des lois adéquates, la Loi sur la concurrence ne nous semble pas non plus de nature à être d'un grand

[69] Loi sur la concurrence. L.R.1985. ch. C-34. Le texte intégral de la Loi sur la concurrence peut être consulté sur le site Internet du Ministère de la Justice du Canada, au http://lois.justice.gc.ca/fr/C-34/23791.html (page consultée le 10 juillet 2005)
[70] Loi sur la concurrence. L.R.1985. ch. C-34, art. 74.01(1)
[71] Loi sur la concurrence. L.R.1985. ch. C-34, art. 74.1 (1)
[72] Loi sur la concurrence. L.R.1985. ch. C-34, art. 52
[73] Loi sur la concurrence. L.R.1985. ch. C-34, art. 74 (12)

secours dans le cadre d'une lutte concertée contre un phénomène qui relève du marketing[74] de masse plutôt que des pratiques de marketeurs individuels.

[74] Soulignons ici que les dispositions de la Loi sur la concurrence qui visent le télémarketing sont limitées dans leur application, en vertu de la définition qui en est donnée à l'article 52.1(1), aux « communications téléphoniques interactives ».

Moyens supplétifs

Les FSI comptent, nous l'avons vu, parmi les premières victimes du pourriel, du fait de l'encombrement de leurs réseaux et de l'effet de démoralisation qu'entraînent ces pratiques sur leur clientèle. Plutôt que d'attendre des législations qui tardent à venir, ces entreprises tentent de protéger leurs intérêts par différents moyens : code d'éthique, code de bonnes pratiques et clauses contractuelles.

La présente section propose un survol de ces différents outils et tente d'analyser leur portée et leur effet dans le cadre d'une lutte au pourriel.

Code canadien de pratiques pour la protection des consommateurs dans le commerce électronique[75]

Le Code canadien de pratiques pour la protection des consommateurs dans le commerce électronique (CCPPCCE) n'est pas en soi un outil destiné à combattre le pourriel, mais certaines de ses dispositions déterminent toutefois le cadre dans lequel devrait s'effectuer l'envoi de courriels publicitaires. Ce Code longuement mûri dans le cadre d'une collaboration entre entreprises, FSI, groupes de protection des droits des consommateurs et représentants des divers paliers de gouvernement, jette les bases de ce que seraient les comportements acceptables et souhaitables dans le contexte du commerce électronique au Canada.

Le CCPPCCE traite de la question des courriels non sollicités à son Principe 7, les interdisant d'emblée. « *Le commerçant ne doit pas transmettre de courriel publicitaire au consommateur sans son consentement, sauf si une relation à déjà été établie avec ce dernier* ». L'article précise de plus que le seul fait de parcourir ou de visiter le site Web d'un commerçant ne constitue pas une « relation d'affaires » sur laquelle un commerçant pourrait s'appuyer pour expédier des courriels non sollicités. Tout courriel reçu par un consommateur doit de plus lui permettre d'aviser le commerçant, selon une procédure simple, qu'il ne désire pas ou plus recevoir de tels courriels de sa part.

Malgré la prise de position claire du CCPPCCE qui interdirait totalement le pourriel, cet outil fait un peu figure de vœu pieux vu son absence de force obligatoire. Comme il arrive souvent dans le cas de tels codes volontaires, les entreprises ou les commerçants n'ont aucune obligation d'adhérer aux principes de ce Code et ceux qui déclarent y adhérer ne font l'objet d'aucun contrôle qui permettrait de déterminer si, dans leurs pratiques commerciales sur Internet, ils respectent vraiment les principes du Code au moment de leur adhésion ou s'ils continuent de les respecter par la suite. Le document ne prévoit évidemment non plus aucun régime de sanction.

[75] Le texte intégral du Code canadien de pratiques pour la protection des consommateurs dans le commerce électronique peut être consulté sur le site Internet d'Industrie Canada , in Carrefour des consommateurs, au : http://strategis.ic.gc.ca/epic/internet/inoca-bc.nsf/fr/ca01490f.html (page consultée en janvier 2005)

Mentionnons que le CCPPCCE s'est largement inspiré des Lignes directrices régissant la protection des consommateurs dans le contexte du commerce électronique[76], adoptées en 1999 par l'Organisation de Coopération et de Développement économiques (OCDE) dont le Canada est membre. Dans ces Lignes directrices, le deuxième principe, portant sur la loyauté des pratiques en matière de commerce, de publicité et de marketing comporte des dispositions visant spécifiquement le pourriel. Le Canada, avec le CCPPCCE, reprend les dispositions des lignes directrices de l'OCDE et les pousse plus loin encore, ajoutant la mention d'une procédure permettant d'être retiré d'une liste d'envoi et limitant l'envoi de courriels promotionnels non sollicités au cadre d'une véritable relation d'affaires préexistante.

On peut malheureusement douter de l'efficacité d'un tel Code de pratique en l'absence d'une campagne de communication massive visant à le faire connaître auprès des internautes canadiens comme des entreprises et à convaincre des avantages de faire affaire avec une entreprise qui adhère à tel Code. Les commerçants trouveraient sans doute une plus grande motivation à adopter les principes qu'il énonce si cet engagement pouvait permettre d'envisager quelque gain au plan du marketing : un Code de pratiques connu du grand public, un logo facilement identifiable confirmant le respect par l'entreprise des principes qu'il énonce, des consommateurs prêts à faire des achats sur des sites « certifiés », voilà un ensemble de conditions qui pourraient éveiller l'intérêt des commerçants vu les possibilités d'avantages sur le plan économique qu'entraîne une meilleure image aux yeux des consommateurs

Le Code, qui a reçu l'appui de l'industrie, du gouvernement, des FSI et des groupes de défense des droits des consommateurs qui ont collaboré à son élaboration, n'en demeure pas moins un modèle qui peut servir d'exemple à qui voudrait adopter des pratiques saines et reconnues comme telles. Il ne pourra évidemment se révéler d'aucun secours dans une lutte au pourriel tant que les entreprises qui y souscriront ne le feront que parce qu'elles se soucient déjà de la protection du consommateur. La seule arme qui nous semblerait à prime abord utilisable en ce qui a trait aux codes volontaires pourrait être l'utilisation de la Loi sur la concurrence ou, dans une certaine mesure, des dispositions des lois sur la protection des consommateurs qui portent sur les fausses déclarations, qui permettraient de s'en prendre à un commerçant qui affirmerait respecter les principes énoncés dans ces codes alors que ses pratiques ne correspondent pas aux principes qu'ils prônent.

Les clauses contractuelles; pouvoirs et responsabilité des fournisseurs de services internet (FSI)

Comme nous le mentionnions plus haut, les FSI n'ont pas attendu l'intervention des législateurs pour se doter d'outils pour lutter contre l'action des pourrielleurs : les contrats d'abonnements qui lient les clients aux FSI comprennent des clauses qui fixent des limites visant à empêcher l'utilisation du réseau des FSI par d'éventuels pourrielleurs.

Les conditions de service que l'on retrouve dans les contrats d'un FSI peuvent indiquer qu'une utilisation anormale ou abusive du service d'accès Internet, ou qui aurait pour effet de perturber les services d'accès Internet des autres clients, peut entraîner l'interruption du service du client perturbateur[77]. À titre d'exemple : dans la section « obligations du client », après un énoncé

[76] "OECD Guidelines for Consumer Protection in the Context of Electronic Commerce (1999)" In OCDE. Sécurité de l'information et protection de la vie privée. Site de l'Organisation de coopération et de développement économiques http://www.oecd.org/document/51/0,2340,fr_2649_34255_1824435_1_1_1_1,00.html et http://www.oecd.org/dataoecd/17/59/34023530.pdf (pages consultées en mars 2005)

[77] Conditions d'abonnement. Contrat Internet. In Vidéotron. Service à la clientèle. Site de Vidéotron http://www.videotron.com/services/fr/service_clientele/8_3_1.jsp (page consultée en mars 2005) , voir l'art. 4.4

faisant référence à la Netiquette[78], le contrat d'un FSI avise ses clients qu'il peut interrompre le service d'accès de tout client qui conduit une des activités suivantes : « a) transmettre ou favoriser la transmission de messages non sollicités (pourriel); b) transmettre des chaînes de courriels de nature pyramidale, etc. On peut évidemment s'interroger sur la portée exacte de termes aussi subjectifs que « abusif » ou « anormal » qui laissent une discrétion considérable aux FSI. Et que faire d'une référence à un concept comme celui de la Netiquette?

Dans l'affaire Nexx Online[79], le tribunal a eu à se pencher sur la validité d'une clause de ce type, qui mentionnait justement la Netiquette. La défenderesse, l'FSI Nexx, avait pris l'initiative de mettre fin à l'hébergement du site Internet de la compagnie demanderesse suite aux plaintes qu'elle avait reçues de la part de ses clients relativement au pourriel expédié par la demanderesse. La cour se rangea aux arguments de la défenderesse qui estimait avoir agi à bon droit en se basant sur les règles de la Netiquette: « sending unsolicited bulk commercial e-mail is in breach of the emerging principles of Netiquette, unless it is specifically permitted in the governing contract» [80].

Cette décision qui confirme la latitude des FSI dans le contrôle qu'ils peuvent faire des services d'accès qu'ils offrent les avantages sans aucun doute puisqu'elle leur permet d'intervenir pour limiter les dommages que pourraient leur causer les pourrielleurs. Cette discrétion qui leur est laissée n'est-elle pas de nature, dans une certaine mesure, à entraîner en contrepartie une responsabilité en cas de non-intervention contre des pourrielleurs qui utiliseraient leur réseau?

Concernant la responsabilité des FSI, la Cour suprême a déjà affirmé que: « Les tribunaux doivent présumer que celui qui autorise une activité ne l'autorise que dans les limites de la légalité… »[81]. Précisons que, tant et aussi longtemps qu'aucune loi ne déclare illégal le «Spamming», cette affirmation ne reçoit dans le cas qui nous intéresse qu'une application assez restreinte. Il n'en reste pas moins que, suivant cette logique, tant que les FSI ne seront considérés que comme acteurs passifs, qui ne font que mettre innocemment à la disposition des pourrielleurs les infrastructures nécessaires à la conduite de leurs opérations, ils bénéficieront d'une quasi immunité, que leur consentent d'ailleurs jusqu'à maintenant la plupart des législations ou projets de loi visant à enrayer le pourriel.

---

[78] ~~e~~Ce terme peut être défini de la façon suivante : l'ensemble des conventions informelles de bonne conduite qui se sont développées entre les internautes, particulièrement lors de l'envoi de messages électroniques et de conversations dans des forums de discussion~~;~~. ~~les manquements à ces conventions sont sanctionnés par la communauté des internautes. Une définition plus condensée du site Dico du Net parle de : Règles édictant ce qu'il faut faire et ce qu'on ne doit pas faire sur le réseau~~ on peut trouver un exemple de règle de Netiquette sur le site Internet de l'Université catholique de Louvain, in Infrastructure des réseaux du système d'information, au http://www.sri.ucl.ac.be/SRI/rfc1855.fr.html ou sur celui du Département Informatique de l'École Nationale Supérieure des Télécommunications, au http://www-inf.enst.fr/~vercken/netiquette/netiquette.html (pages consultées le 12 juillet 2005)

[79] 1267623 Ontario Inc. v. Nexx Online Inc. ,(1999)O.J. No 2246 (Sup. Ct.)

[80] 1267623 Ontario Inc. v. Nexx Online Inc. ,(1999)O.J. No 2246 (Sup. Ct.), par. 31

[81] Société canadienne des auteurs, compositeurs et éditeurs de musique c. Associ~~.~~ation canadienne des fournisseurs Internet (2004) CSC 45 par. 122

Code de déontologie et Normes de pratique[82]

L'association canadienne du marketing (ACM), qui compte quelque 800 membres corporatifs[83], reconnaissant que « l'établissement et le maintien de normes de pratiques rigoureuses constituent des responsabilités fondamentales envers le public » et que « De telles normes sont essentielles pour que l'industrie mérite et conserve la confiance du public » s'est dotée en 1990 d'un Code de déontologie et de Normes de pratique (CDNP) visant à encadrer la conduite de ses membres en fixant et en maintenant des normes qui régiront la conduite des activités de marketing[84].

Alors qu'une bonne partie du CDNP se penche en détail sur la *Véracité des représentations* (section B)[85], les *Éléments constitutifs et caractéristiques de l'offre* (section C) et les *Pratiques liées au traitement des commandes* (section D), certaines de ses dispositions pourraient trouver une application directe dans le cadre de la lutte au pourriel.

La section E, intitulée *Normes de pratique spécifiques à certains médias* comprend une section qui porte spécifiquement sur le marketing électronique, incluant « toute communication de marketing acheminée aux consommateurs par le biais de médias numériques comprenant, sans toutefois s'y limiter, le courrier électronique (…) »[86] et qui prévoit des obligations qui s'ajoutent aux obligations générales des sections précédentes.

On retrouve parmi ces obligations : l'identification du motif de la collecte de l'adresse électronique et une utilisation limitée aux fins dévoilées (E4.1.2); l'interdiction d'envoyer du marketing sans consentement préalable explicite du destinataire (sauf relation commerciale existante), d'envoyer de telles communications aux consommateurs qui leur ont dit ne plus vouloir en recevoir et de communiquer une adresse électronique à un tiers sans son consentement (E4.1.3); l'identification de l'expéditeur et une possibilité de refuser les envois ultérieurs (E4.1.4); l'interdiction de recourir à des rubriques fausses ou trompeuses (E4.1.5).

De manière un tant soit peu contradictoire, le CDNP au même article, E. 4.1.3, dans lequel il prévoit l'interdiction d'envoyer du marketing sans consentement préalable explicite du destinataire précise toutefois qu'en livrant son adresse électronique à une entreprise, le consommateur consent tacitement à recevoir des communications électroniques de celle-ci.

Le CDNP énonce plus loin, à sa section J, commentés, les 7 principes de protection de la vie privée adoptés par l'Association canadienne du marketing que tous les agents de marketing doivent reconnaître et respecter : Permettre aux consommateurs de déterminer comment les renseignements à leur sujet sont utilisés; Accorder aux consommateurs le droit d'accès à

[82] Le Code de déontologie et Normes de pratique de l'association canadienne du marketing a été adopté en 1990 et a fait l'objet depuis de 5 amendements : 1993, protection des renseignements personnels, 1997, respect de la vie privée des consommateurs utilisant les technologies interactives, 1999, le marketing destiné aux enfants, 2002, le marketing destiné aux adolescents et, 2004, l'obligation d'inclure l' « opting-out » pour de futurs envois ; le document est disponible sur le site Internet de L'Association canadienne du marketing au http://www.the-cma.org/french/downloads/CodeofEthicsFrench.pdf (document consulté le 12 juillet2005)

[83] "~~Background on CMA" In~~ About CMA". ~~Association Information.~~ Site du Canadian Marketing Association http://www.the-cma.org/about/index.cfm~~http://www.the-cma.org/about/background.cfm~~ (page consultée l~~e~~ ~~janvier~~ 12 juillet 2005)

[84] Code de déontologie et Normes de pratique, op. cit. 123, préambule et A 2.1

[85] Qui insiste sur le fait que Les offres doivent être claires et véridiques et ne pas contenir d'affirmations trompeuses, que l'entreprise doit s'identifier, etc.; Code de déontologie et Normes de pratique, section B

[86] Code de déontologie et Normes de pratique, E. 4.1.1

l'information; Permettre aux consommateurs de réduire la quantité de courrier qu'ils reçoivent[87]; Contrôler l'utilisation des renseignements par les tierces parties; Adopter des mesures de sécurité pour le stockage des renseignements sur les consommateurs; Respecter la confidentialité des renseignements, le septième principe n'étant pour sa part que le mode d'application du processus de plainte aux principes précédents.

Le processus de plainte prévu pas le CDNP se retrouve à la section K. L'ACM s'engage, sur réception d'une plainte, à communiquer avec toute entreprise, membre ou non de l'Association, pour tenter de régler le litige (K2) et insister sur l'application du CDNP (K3). Après enquête, le Conseil d'administration pourra, après une audience équitable, annoncer publiquement les faits relevés pendant l'enquête portant sur le non membre (K5.2). Une annonce publique pourra aussi être faite, après une audience équitable, si le Conseil d'administration est convaincu qu'une entreprise membre a contrevenu sciemment et régulièrement au Code de déontologie et aux Normes de pratiques. Le Conseil pourra aussi décider l'expulsion de ce membre (K6)

Comme rien n'oblige les personnes morales ou physiques qui font du marketing à adhérer à une association professionnelle, on peut aisément présumer que seules les entreprises sérieuses auront à cœur de suivre les consignes émises par l'ACM, ce qui exclut les pourrielleurs, qui ne sont pas membres de l'ACM qui interdit à ses membres le «Spamming» et l'acquisition de listes de courriels en vue de marketing et ne craignent donc pas d'en être expulsés.

Comme c'est aussi le cas pour le Code canadien de pratiques pour la protection des consommateurs dans le commerce électronique, la promotion de l'adhésion volontaire à quelque norme de pratique ou d'éthique a le défaut de ne prêcher qu'aux convaincus. Personne n'est encore parvenu à mettre fin à un fléau en insistant auprès des éléments déchaînés pour qu'ils fassent preuve de bonne volonté ou de coopération.

Il faut aussi garder à l'esprit que l'ACM ne vise, avec ce CDNP qu'à remplir sa mission et à atteindre ses objectifs, qui consistent à « Créer un milieu qui stimule la croissance du marketing » et à « Représenter les intérêts des agents de marketing » et que les outils qu'elle pourrait développer ne viseront toujours qu'à atteindre ces buts. Un article qui apparaît sur le site de l'ACM, Dealing with Spam, nous oriente d'ailleurs vers cette interprétation : « Known as spam e-mail, these offensive and annoying messages clog inboxes; waste time; and can cause you to miss legitimate e-mails offers from companies you already do business with. »[88] (nos soulignés). C'est d'abord et avant tout à ses membres qui désirent expédier des courriels publicitaires légitimes que nuit le plus, aux yeux de l'ACM, le problème du pourriel.

[87] Excluant le « consommateur actuel », soit celui qui a effectué un achat d'un agent de marketing au cours des six derniers mois ou pendant un cycle d'achat normal. Code de déontologie et Normes de pratique, Section J, Principe 3

[88] Dealing with Spam, sur le site de l'Association canadienne du marketing, au http://www.the-cma.org/consumer/spam.cfm (page consultée le 12 juillet 2005)

4. LA SITUATION EN AUSTRALIE

L'Australie a adopté en matière de lutte au pourriel une approche proactive avec la mise en place d'un cadre législatif spécifique. Entré en vigueur en avril 2004, le Spam Act 2003[89], dont l'application a été confiée à l'organisme régulateur national en matière de télécommunications, l'Australian Communications Authority (ACA ou ACMA)[90], a une portée très large

Le Spam Act 2003 propose, à son article 3, un court résumé des moyens retenus :
- Interdiction d'expédier de courriels commerciaux non sollicités;
- Obligation d'indiquer dans les messages électroniques commerciaux les informations concernant la provenance de l'autorisation;
- Les messages électroniques commerciaux doivent contenir un processus fonctionnel permettant de se désinscrire;
- Les logiciels permettant la récolte d'adresses (harvesting) ne peuvent être utilisés, fournis ou acquis;
- Les listes électroniques d'adresses produites par un tel logiciel ne peuvent être utilisées, fournies ou acquises;
- Les remèdes principaux en cas de contravention sont les « civil penalties » et les injonctions.

Le Spam Act 2003 entend s'attaquer au pourriel, sans égard à son mode de diffusion, d'où l'utilisation du terme « message électronique » plutôt que courriel, qui a une acception plus restreinte. Selon l'article 5, sont donc visés par le terme « message électronique » : tous les courriels, les SMS (short message service : messages textes reçus et/ou envoyés via un téléphone cellulaire), les MMS (multimedia messaging[91]) et les IM (instant messaging[92]).

Afin de s'assurer que tous les messages commerciaux électroniques qui peuvent circuler en Australie sont visés par la Loi, le Spam Act 2003 interdit d'envoyer ou d'ordonner l'envoi d'un message électronique non sollicité qui ait quelque lien avec l'Australie. Selon l'article 7 du Spam Act 2003, un « lien avec l'Australie » peut être établi dans l'un cas suivants :
1. le message origine de l'Australie;
2. il a été expédié ou commandé par une personne ou une organisation qui était présente en Australie au moment où le message a été envoyé ou y a ses organes de contrôle;
3. l'appareil utilisé pour recevoir le message est localisé en Australie;
4. le destinataire était physiquement présent en Australie au moment de la réception ou y exerce ses activités;
5. si le message n'et pas parvenu à destination parce que l'adresse est inexistante,

[89] Le Spam Act 2003, no.129 2003 peut être consulté en ligne sur Australian Law Online In Attorney-General's Department, sur le site Internet du gouvernement australien, au http://scaleplus.law.gov.au/html/comact/11/6735/0/CM000590.htm (page consultée en décembre 2004)

[90] Consumer Information. Site de la Australian Communications Authority. http://internet.aca.gov.au/ACAINTER.65636:HOMEPAGE:760085865:pc=PC_3,tlp=PC_3 (page consultée en décembre 2004). Le 1er juillet 2005, l'Australian Broadcasting Authority et l'Australian Communications Authority ont été fusionnés pour former l'Australian Communications and Media Authority (ACMA). C'est l'ACMA qui est maintenant responsable de l'application du Spam Act 2003. Le site Internet de ce nouvel organisme se trouve à l'adresse suivante : http://www.acma.gov.au/acmainter (page consultée le 12 juillet 2005)

[91] Les MMS permettent la transmission notamment d'images, de messages textes et de fichiers musicaux via des téléphones ou ordinateurs utilisant un réseau de communication sans fil avec le protocole WAP

[92] Les IM permettent de créer une sorte de session de « chat » privé sur Internet.

il est raisonnable de croire que l'appareil ou le serveur qui aurait servi à la réception du message, si telle adresse avait existé, aurait été localisé en Australie .

L'article 9 du Spam Act 2003 précise que n'est pas considéré comme expéditeur celui qui se limite à fournir le transport (carriage) du message.

En plus d'interdire l'envoi de messages électroniques commerciaux à des adresses inexistantes ou des messages commerciaux qui ne sont pas identifiés comme tel, l'article 16 interdit totalement l'envoi de messages commerciaux sauf si l'expéditeur a reçu le consentement préalable de la personne visée (article 16 (2))[93]. Le Schedule 2 du Spam Act 2003 (Consent) définit ce que la Loi entend par consentement. Le consentement doit être exprès, à moins qu'il ne puisse être raisonnablement inféré de la conduite du destinataire du message commercial ainsi que des affaires et relations qui ont pu être établies entre l'expéditeur et le destinataire. Le point 4 du Schedule 2 précise que le simple affichage en ligne d'une adresse électronique ne doit pas laisser supposer qu'il y a consentement à recevoir des messages électroniques, à moins que ces messages n'aient un lien direct avec le motif de cet affichage[94].

L'ACMA possède pour l'application du Spam Act 2003 d'importants pouvoirs d'enquête (collecte d'information auprès des entreprises, utilisation de mandats de perquisition, de saisie ou de surveillance permanente dans certains cas) ainsi que le pouvoir de conclure avec les entreprises des ententes en vue d'engagements volontaires exécutoires (Spam Act 2003, partie 6). L'ACMA peut aussi entreprendre devant la Cour fédérale des procédures en vue d'obtenir la condamnation des contrevenants à des amendes (article 26) et pour demander à la Cour d'imposer aux contrevenants diverses mesures, comme par exemple de verser une compensation au destinataire qui aurait subi des pertes ou d'imposer le recouvrement par l'État des profits que le contrevenant aurait pu tirer directement ou indirectement des actes posés en contravention du Spam Act 2003 (articles 28 et 29). Pour la détermination du montant des amendes imposables, la Cour fédérale pourra considérer la nature, l'importance et les circonstances de la contravention, les dommages qu'elle a pu entraîner, l'existence d'antécédents, y compris de condamnations du contrevenant dans des juridictions étrangères (article 24). Les pénalités financières peuvent aller jusqu'à 1,1 millions de dollars (australiens) par jour, pour les sanctions civiles[95], dans le cas d'une entreprise avec des antécédents (art. 25(5)), alors que pour un particulier avec antécédents, le maximum prévu est de 220 000 dollars[96]. Pour un particulier sans antécédent, le montant maximum de l'amende sera de 44 000 dollars (art. 25(4)i).

En vue de garantir la poursuite de la lutte contre le pourriel, Le Spam Act 2003 confie à l'ACMA certaines tâches complémentaires (Partie 7, Article 42 Additional ACA functions) qui vont de la coordination de programmes d'éducation et de sensibilisation (à être menés conjointement avec des représentants de l'industrie, des groupes de défense des droits des consommateurs et du

[93] L'article 16(9) interdit aussi toute participation à l'un des actes prohibés.
[94] Le Commissariat à la vie privée du Canada a tiré des conclusions au même effet dans le dossier Geist, Op. cit 67
[95] ~~I~~Le dollar australien s'échange~~ant~~ pratiquement au pair avec le dollar canadien : http://www.xe.net/ucc/convert.cgi
[96] ~~mentionnons que I~~Le Spam Act 2003 fait référence à des « penalty unit »; le valeur de ces unités de pénalité est établie par ~~ce qui équivaut selon~~ l'article 4AA du ~~le~~ Crimes Act ~~de~~ 1914 à 110$ autraliens par unité. Voir Australian Law Online In Attorney-General's Department, sur le site Internet du gouvernement australien, au http://scaleplus.law.gov.au/html/histact/13/6894/0/HA000880.htm ; ~~http://www.austlii.edu.au/au/legis/cth/consol_act/ca191482/s4aa.html~~(page consultée le 12 juillet 2005)

gouvernement) à celle de programmes de recherche, en passant par un rôle de liaison en vue d'une coopération internationale qui viserait la prohibition ou la réglementation des messages électroniques commerciaux non sollicités et des logiciels servant à récolter des listes de courriels.

En vue de faciliter la portée extraterritoriale de sa Loi, l'Australie a déjà conclu des accords avec plusieurs pays, dont ses principaux voisins : la Thaïlande et la Corée du Sud , ainsi qu'avec les États-Unis et la Grande-Bretagne[97].

Le sérieux dont a fait preuve l'Australie dans l'élaboration de son Spam Act 2003 et des moyens mis en œuvre pour son application devrait constituer un modèle pour tout législateur qui se déclare soucieux de la gravité de la problématique du pourriel et qui considère les types d'intervention les plus prometteurs.

L'ingéniosité des dispositions du Spam Act 2003 lui confère une portée inégalée, tant sur l'objet même que vise à contrôler la Loi que sur les sources possibles des messages. L'importance des pénalités et la latitude donnée à la Cour pour déterminer leur quantum démontre aussi la nette volonté de sévir en vue de contrer le problème. Le double rôle confié à l'ACMA qui, en plus de s'assurer de l'application de la Loi, doit veiller au développement, local et international, des pistes de solution confirme la volonté du législateur d'envisager le problème de façon globale afin de tenter de trouver et d'appliquer, à court et à long terme, des remèdes efficaces à l'envahissement des messages électroniques non sollicités.

[97] Anti Spam. Consumer Information. Site de la Australian Communications Authority. http://internet.aca.gov.au/ACAINTER.2293792:STANDARD:2081803710:pp=DIR2_25,pc=PC_1966#Spamact (page consultée en décembre 2004)

5. COOPÉRATION INTERNATIONALE

La nature même d'Internet, qui ignore les frontières, assure qu'une tentative de solution au problème du pourriel qui n'aurait d'effet qu'au plan national ne pourra jamais être que très partiellement efficace. Les États, s'ils peuvent, comme le tente le Spam Act 2003 adopté en Australie, concevoir des moyens applicables à des entreprises qui ne sont pas sises sur leur territoire, ne pourront que difficilement mettre à exécution leurs lois à moins d'une collaboration et d'une entraide internationale en ce sens.

Le Plan d'action de Londres sur la coopération internationale relative à l'application des lois antipourriel [98] a vu le jour en octobre 2004 au terme de la rencontre de représentants de l'industrie, des organismes publics et parapublics et des gouvernements de 27 pays qui s'étaient réunis en vue d'échanger sur l'harmonisation nécessaire à l'application des lois anti-pourriel nationales. Résultat des efforts conjugués de groupes tels l'Organisation de coopération et développement économique (OCDE), l'Union internationale des télécommunications (UIT), l'Union européenne (UE), l'International Consumer Protection and Enforcement Network (ICPEN) et le Forum de coopération Asie-Pacifique (APEC), ce Plan d'action vise à lutter contre le pourriel et certaines autres pratiques électroniques contestables (telle le *phishing*[99]). Avec ce Plan d'action, les différents acteurs concernés ont convenu de prendre divers engagements.

Les représentants des gouvernements et organismes publics s'engagent à désigner des points de contact au sein de leur organisme afin de répondre aux demandes de renseignements sur l'application des lois anti-pourriel; ils s'engagent de plus à promouvoir la coordination et la communication entre les diverses agences et organismes chargés de l'application de ces lois ainsi qu'à prendre part à d'autres conférences, forums ou groupes de travail afin, notamment, de faire un suivi des mesures prises et des développements en matière de législation, mise en application des lois, campagnes de sensibilisation, etc.

Les représentants du secteur privé ont de leur côté pris des engagements sensiblement similaires et devront en plus participer sur demande et s'il y a lieu à des audioconférences pour aider les organismes d'application de la loi à engager des poursuites contre les polluposteurs et s'efforcer d'y faire rapport des causes de pourriel, des nouvelles tendances en matière technologique relativement au pourriel, des obstacles à la coopération, tant avec les

[98] Le texte intégral du Plan d'action de Londres sur la Coopération internationale relative à l'application des lois antipourriel est disponible sur le site Internet d'Industrie Canada, in l'Économie numérique au Canada, http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/fr/gv00288f.html, au http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/vwapj/London%20Action%20Planf.pdf/$file/London%20Action%20Planf.pdf (Document consuté le 12 juillet 2005) ~~« Groupe de travail sur le pourriel ; table ronde des intervenants clés » In L'économie numérique au Canada. Industrie Canada. Site d'Industrie Canada http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/fr/gv00267f.html (page consultée en décembre 2004)~~

[99] Le Dictionnaire de la high tech de l'Internaute magazine donne du phishing la définition suivante : ~~voici une définition de cette pratique :~~ « Un cas d'usurpation d'identité. Des sites miroirs semblables à des portails de renom sont créés puis les internautes sont arrosés au hasard avec un courrier non sollicité (Spam) qui reprend à son tour l'habillage graphique du portail détourné. Le but~~.~~ est alors d'attirer un internaute réellement client du site plagié. Ce Spam invite l'internaute à se rendre sur le faux site pour remettre à jour certains renseignements personnels dans un questionnaire tout aussi faux. L'internaute ainsi dupé laisse numéros de téléphone, de sécurité sociale, de compte bancaire et parfois de carte de crédit. Autant d'informations lucratives pour les escrocs en ligne. »~~.~~. Dictionnaire de la high tech, in l'Internaute magazine http://encyclopedie.linternaute.com/definition/591/11/0/phishing.shtml (page consultée le 12 juillet 2005). Voir aussi à cet effet la note 57

organismes du secteur public qu'avec des membres du secteur privé, et contribuer à la formation du personnel des organismes publics chargés de lutter contre le pourriel, dans des domaines où le secteur privé aura acquis une expertise particulière.

La mise en application de ce Plan d'action est pour l'instant binationale: ce sont le Bureau britannique de la concurrence et la Commission fédérale du commerce des États-Unis qui s'en chargeront. Bien que l'on puisse se féliciter de l'amorce d'une telle coopération, force est de constater que la lourdeur d'un tel processus de coopération et les défis amenés par les nécessaires harmonisations législatives et la coordination des stratégies anti-pourriel des différents États hypothèqueront sûrement à court terme l'efficacité du plan. Cet exercice nous semble tout de même indispensable et peut certainement être bénéfique, ne serait-ce que par la diffusion et le partage à l'échelle internationale des expériences des divers participants impliqués dans cette lutte, et par la prise de conscience de la collaboration qui sera essentielle à l'application outre frontière d'une multitude de lois nationales.

6. LE PLAN D'ACTION CANADIEN DANS LA LUTTE AU POURRIEL

Le ministre de l'Industrie a annoncé en mai 2004 le lancement d'un Plan d'action antipourriel pour le Canada, afin de doter le pays d'une stratégie spécifique dans la lutte au pourriel. Le Plan d'action canadien devait s'articuler principalement autour de quatre volets : 1) une meilleure application des lois existantes, notamment du Code criminel et de la Loi sur la protection des renseignements personnels et les documents électroniques; 2) des démarches entreprises par les FSI afin de résoudre les problèmes de gestion de réseaux causés par le pourriel; 3) des codes de pratiques améliorés pour les industries qui utilisent le courriel à des fins commerciales légitimes et 4) l'éducation et la sensibilisation du public à la problématique du pourriel[100].

Un groupe de travail a été formé afin de réunir des représentants des divers intérêts concernés par le problème du pourriel[101]. Cinq sous-groupes de travail ont ensuite été créés afin de se pencher, de manière plus approfondie, sur: 1) l'examen de la législation et son application; 2) les pratiques exemplaires de gestion de réseaux; 3) la validation du courriel commercial; 4) l'éducation et la sensibilisation des consommateurs; et 5) la collaboration internationale.

Voyons maintenant les résultats du travail de chacun de ces groupes.

1) Groupe de travail sur l'examen de la législation et son application.
   Son mandat consistait essentiellement en l'examen des législations actuelles en vue de déterminer les outils actuellement disponibles pour lutter contre le pourriel et les aménagements qu'il serait nécessaire de leur apporter pour leur permettre une plus grande efficacité. Alors que le groupe avait la discrétion de proposer l'adoption d'une nouvelle loi pour réduire le pourriel, le libellé du mandat du groupe favorisait très clairement l'aménagement de la législation actuelle.
   Le groupe de travail a donc étudié toutes les lois fédérales susceptibles d'être utilisées dans le contexte d'une lutte au pourriel – soit : le Code criminel, la Loi sur la concurrence et la Loi sur la protection des renseignements personnels et les documents électroniques – afin d'évaluer leur efficacité dans ce contexte.

   Le constat auquel en est arrivé le groupe de travail est double. D'une part, les lois actuelles sont insuffisantes pour lutter contre le pourriel et d'éventuels changements à ces lois ne pourront, à eux seuls, amener une solution aux problèmes que soulève le pourriel. D'autre part, les agences responsables de l'application des lois étudiées n'ont pas suffisamment de ressources pour pouvoir remplir le mandat qui leur est confié d'une manière optimale et le pourriel ne figure pas nécessairement parmi leurs priorités.

   Le Groupe de travail a convenu qu'il devrait travailler avec le Commissaire à la protection de la vie privée du Canada et avec les ministères et agences du gouvernement fédéral pour examiner comment pourrait s'articuler une démarche nationale concertée en vue d'une meilleure utilisation des lois existantes.

[100] « Document d'information » L'Économie Numérique au Canada. Site d'Industrie Canada http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/fr/gv00291f.html (page consultée en avril 2005)

[101] Notons au passage que sur les 10 membres du Groupe de travail, une seule association de consommateurs était représentée. Voir la liste des membres du Groupe de travail : « Document d'information » In L'Économie Numérique au Canada. Site d'Industrie Canada http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/fr/gv00291f.html (page consultée en avril 2005)~~, voir la liste des membres du Groupe de travail au milieu de la page.~~

2) Groupe de travail sur les pratiques exemplaires de gestion de réseaux.
Son mandat était d'encourager les FSI et autres gestionnaires de grands réseaux commerciaux canadiens à adopter des technologies et pratiques de gestion permettant de lutter efficacement contre le pourriel.

Le groupe a recueilli des données afin de mesurer l'ampleur du problème du pourriel au pays (en terme de volume de courriels), ce qui permettra de mieux mesurer l'évolution de la situation. Il a aussi étudié des questions connexes : le pourriel ciblant les téléphones cellulaires, les logiciels espions et l'impact d'un nouveau protocole Internet sur le problème du pourriel.

Le groupe a réussi à établir un consensus sur des recommandations quant aux mesures techniques à adopter pour lutter contre le pourriel. Les Pratiques exemplaires recommandées pour les fournisseurs de services Internet et autres exploitants de réseaux sont au nombre de 9[102]. Parmi ces mesures : limiter l'utilisation du port 25 par les utilisateurs finaux[103]; bloquer les pièces jointes aux courriels lorsqu'elles transportent des virus ou filtrer les pièces jointes; gérer et éliminer des éléments de réseau infectés constituant une source de pourriel; établir un processus inter entreprises afin de réagir d'une manière efficace et coordonnée aux rapports d'incidents provenant d'autres réseaux; communiquer aux abonnés les mesures de sécurité des gestionnaires de réseaux et les politiques de sécurité; mettre en œuvre la validation du courriel sur tous leurs serveurs SMTP; limiter les avis de non-remise aux cas de messages électroniques légitimes. Les fournisseurs d'accès et autres exploitants de réseaux doivent de plus surveiller étroitement le volume de courriels entrants et sortants afin de repérer les activités inhabituelles dans le réseau et leur source, et prendre des mesures en conséquence

3) Groupe de travail sur la validation du courriel commercial.
Son mandat visait à policer certaines pratiques de l'industrie en matière de marketing, notamment en incitant l'industrie à authentifier les courriels commerciaux légitimes et en adoptant des codes de pratique qui interdisent l'utilisation du pourriel en tant que technique de marketing.

Le groupe a décidé que la certification[104] des courriels était une voie de solution aux problèmes soulevés par les participants. Il a été convenu que le groupe poursuivrait ses travaux afin de faire l'étude des modèles de certification existants et l'évaluation de celui qui serait le plus apte à être transposé dans le contexte canadien.

4) Groupe de travail sur l'éducation et la sensibilisation des consommateurs.

---

[102] « Pratiques exemplaires recommandées pour les fournisseurs de services Internet et autres exploitants de réseaux », L'Économie Numérique au Canada. Site d'Industrie Canada http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/fr/gv00286f.html (page consultée en avril 2005)

[103] L'IANA (Internet Assigned Names Authority) a rattaché un numéro de port à chaque application Internet; ainsi la transmission de courriels se fait par le port 25 : cf. « The reasons why Port 25 is blocked on connections » In NDO.com. Site de Ndo.com http://www.ndo.com/ndo/Support/The_reasons_why_Port_25_is_blocked_on_connections/port25why.html (page consultée en avril 2005)

[104] La certification a été définie comme suit par le groupe : « une façon d'identifier le courriel légitime en y insérant un algorithme, un timbre, un jeton de contrôle ou autre certificat qui permet aux établissements et aux fournisseurs de services ou aux utilisateurs de déterminer s'il provient d'une source valide vérifiable »
dans « Document d'information », L'Économie Numérique au Canada. Site d'Industrie Canada http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/fr/gv00291f.html (page consultée en avril 2005)

Son mandat était de déterminer les pratiques que pourraient adopter les canadiens afin de réduire le volume de pourriel qu'ils reçoivent et trouver un moyen de communiquer ces conseils à la population d'une manière efficace.

Une stratégie de communication a été établie afin de faire connaître aux canadiens les meilleurs moyens de lutter contre le pourriel. Une première campagne a vu le jour pour diffusion sur Internet. 3 conseils-clé ont été rédigés et mis en ligne sur un site Web autonome, « arretezlepourrielici.ca »[105] sous le titre Combattre le pourriel : trois conseils clés. Ces conseils sont les suivants:

- Protégez votre ordinateur en installant anti-virus, antipourriel et coupe-feu et maintenez à jour ces logiciels. Vérifiez toujours la source d'un courriel qui contient une pièce jointe;
- Protégez votre adresse électronique en créant des adresses distinctes en fonction de vos divers usages d'Internet et en ne la communiquant qu'à des personnes de confiance;
- Protégez-vous en supprimant systématiquement tout pourriel reçu. Pas de réponse, pas de désabonnement, pas de visite des sites Web qui, tous, sont susceptibles de confirmer votre adresse.

En vue de diffusion de ces conseils, un logo « Arrêtez le pourriel ici », qui sert d'hyperlien vers la page Web du site, est affiché sur les sites Internet de tous les partenaires recrutés (mouvements associatifs, industries, agences gouvernementales, établissements d'enseignements et autres groupes ou entités intéressés à collaborer dans la lutte au pourriel).

Un rapport interne annonce qu'un rapport et des recommandations devront être remis au ministre de l'Industrie dans les mois à venir[106]. Dans ce même rapport, on retrouve le bilan des actions entreprises et un plan qui prévoit que : 1) de décembre 2004 à avril 2005, le groupe continuera de recruter des partenaires de divers horizons pour les associer à sa campagne; le groupe continuera de répondre aux demandes qui lui parviendront via son site Web et il s'efforcera de prendre des mesures pour rendre son site plus accessibles (notamment aux plans graphique et linguistique), 2) l'étude de la faisabilité et de l'utilité d'une campagne de communication plus étendue a été entreprise, 3) le groupe a entrepris de lancer des campagnes plus ciblées auprès de certains groupes ou organisations (les représentants des petites entreprises, les jeunes, etc.) de décembre 2004 à mars 2005, afin de développer des outils de communication plus spécifiques pour rejoindre ces groupes. De plus, le site Web sera bonifié pour inclure certaines applications nouvelles, comme un questionnaire permettant aux visiteurs du site de savoir s'ils ont un comportement sécuritaire face au pourriel.

5) Groupe de travail sur la collaboration internationale.
Son mandat était d'assurer au gouvernement du Canada ainsi qu'aux FSI nationaux une meilleure visibilité sur la scène internationale, de coordonner les efforts de chacun et de mettre en œuvre des politiques bilatérales ou internationales.

Le groupe participe à plusieurs tribunes sur la question du pourriel et fait rapport de ses activités; il participe ainsi au groupe de réflexion de l'Organisation de coopération et de

[105] Combattre le pourriel : trois conseils clés; in arrêtezlepourrielici.ca, disponible au http://arretezlepourrielici.ca/ (page consultée le 12 juillet 2005)

[106] « Public Education and Awareness Working Group » Work Plan (January 2004-April 2005). Document interne distribué aux membres du groupe de travail sur l'éducation et la sensibilisation des consommateurs.

développement économiques (OCDE) sur le pourriel et a transmis à l'OCDE les travaux de certains des groupes de travail canadiens sur le pourriel afin d'enrichir les réflexions. Les discussions de l'OCDE ont conduit à la rencontre, à Londres, en octobre 2004, de représentants de 27 pays et de nombreux organismes publics et privés, afin de signer une entente de collaboration visant non pas à supplanter les accords internationaux existants mais plutôt à établir un cadre de communication et de coopération plus formel entre les divers acteurs en présence; par le biais, notamment, d'un dialogue continu, assuré par des conférences régulières sur les développements survenus et le suivi des actions entreprises[107].

Le groupe de travail participe également aux travaux du Forum de coopération économique Asie-Pacifique (APEC), du Dialogue mondial des entreprises sur le commerce électronique (GBDe), de l'Union internationale des Télécommunications, et suit les discussions de la Conférence des Nations Unies sur le commerce et le développement, l'Internet Engineering Task Force (IETF) et de l'International Consumer Protection and Enforcement Network (ICPEN).

[107] Il s'agit du Plan d'action de Londres sur la coopération internationale relative à l'application des lois antipourriel dont nous avons traité plus haut. « Groupe de travail sur le pourriel ; table ronde des intervenants clés » In L'économie numérique au Canada. Industrie Canada. Site d'Industrie Canada http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/fr/gv00267f.html (page consultée en décembre 2004)

CONCLUSION

« En quelques années seulement, le volume de messages électroniques commerciaux non sollicités – communément appelés « pourriel » – est devenu, d'un ennui mineur qu'il était, un problème social et économique important qui mine la productivité individuelle et commerciale des Canadiens. Le pourriel entrave l'utilisation efficace du courriel aux fins de communications personnelles ou commerciales et menace la croissance et l'acceptation du commerce électronique légitime. (…)

L'ampleur des préoccupations suscitées au sein du grand public et le coût croissant qu'a à subir notre économie indiquent clairement que le moment est venu pour que les pouvoirs publics, le milieu des affaires, l'industrie du marketing et les consommateurs fassent front commun afin de réduire et contrôler les messages électroniques commerciaux non sollicités. »[108]

Malgré ces déclarations alarmantes, aucune loi visant à interdire ou même à encadrer le pourriel n'a, à ce jour, été adoptée au pays, contrairement a ce qui s'est fait aux États-Unis et ailleurs, et malgré le dépôt à répétition d'un projet de Loi plus qu'intéressant (S-15).

L'absence d'une loi spécifique visant le pourriel ne fait cependant pas du Canada un « Cyber Far-West » où tous les abus sont permis. Comme le soulignait récemment le professeur Michael Geist: « Notwithstanding the global anti-Spam legislative efforts, in which it may now be reasonably said that virtually every developed country has implemented legal measures that can be used to combat Spam, the amount of Spam has continued to increase». «The answer may lie not in yet more laws, however, but rather in better renforcement of what we already have »[109].

Listant les lois existantes qui pourraient être utilisées dans le cadre d'une lutte contre le pourriel (Code criminel, Loi sur la protection des renseignements personnels et les documents électroniques, Loi sur la concurrence), l'auteur abonde dans le sens de la politique gouvernementale actuelle, que l'on retrouve dans une directive d'Industrie Canada[110] intitulée « L'Internet et le courrier électronique en vrac non sollicité » : « Le gouvernement estime qu'une combinaison bien dosée de politiques, de lois, de solutions technologiques, de sensibilisation des consommateurs et de responsabilisation des intervenants de l'industrie Internet constitue le meilleur moyen de composer avec les comportements qui apparaissent dans l'environnement nouveau et changeant des communications en ligne » [111].

Toutefois, comme nous l'avons vu précédemment, il n'est pas certain que les tribunaux canadiens seraient en mesure de pousser l'interprétation des textes existants aussi loin que le souhaiteraient les partisans de l'application des lois actuelles. De plus, si certaines des lois

[108] Un Plan d'action antipourriel pour le Canada, Industrie Canada, Mai 2004, in L'économie numérique au Canada, sur le site Web d'Industie Canada, au http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/fr/h_gv00246f.html (page consultée le 12 juillet 2005)

[109] Geist Michael " Untouchable: a Canadian perspective on the anti-spam battle" In Michael Geist.ca. Site de Michael Geist http://www.michaelgeist.ca/geistSpam~~/~~.pdf, p.30-31 (~~page~~document consulté~~e~~ en décembre 2004)

[110] « L'internet et le courrier électronique en vrac non sollicité » In L'Économie Numérique au Canada. Site de Industrie Canada. http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/fr/gv00188f.html (page consultée en décembre 2004)

[111] ~~id.~~ « L'internet et le courrier électronique en vrac non sollicité » In L'Économie Numérique au Canada. Site de Industrie Canada. http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/fr/gv00188f.html (page consultée en décembre 2004)

actuelles peuvent clairement appuyer des poursuites visant quelques actions illégales commises par le biais du «Spamming» (le Code criminel contre la fraude, la Loi sur la concurrence contre l'usurpation d'identité commerciale), les poursuites isolées contre quelques contrevenants ne nous semblent susceptibles ni de discipliner l'industrie du pourriel ni de réduire de façon tangible les problèmes que le seul nombre de communications sollicitées entraîne. Ajoutons que la multiplication des intervenants chargés de l'application de ces différentes lois complique la tâche de coordination indispensable à une lutte concertée contre un problème global et que les coûts qu'entraîne cette multiplication peuvent aisément constituer un frein à cette lutte.

Il nous semble clair, notamment au regard de l'expérience australienne, qui s'avère particulièrement efficace[112], que l'adoption d'une loi anti-pourriel spécifique permettrait de mieux canaliser les initiatives de l'industrie, du gouvernement et des mouvements de consommateurs, qui collaborent d'ailleurs déjà, de manière ponctuelle, aux tables de travail sur divers sujets liés au commerce électronique et/ou à la protection de la vie privée, dans le cadre de projets pilotés par nos gouvernements.

Les nouvelles technologies engendrant des nouvelles problématiques, qui gagnent en complexité[113], il est normal que les solutions qui devront être mises en place pour y faire face doivent aussi être imaginatives et adaptables. Les modifications qui pourraient, par voie d'amendements ponctuels, être apportées à des lois sectorielles existantes en vue de répondre aux nouvelles problématiques à mesure qu'elles se présentent risquent toujours de complexifier leur application et leur coordination, surtout si les buts visés par ces lois et les organismes chargés de leur application diffèrent.

Une loi anti-pourriel, dont l'application ne serait confiée qu'à un seul organisme, aurait l'avantage de prévoir des définitions claires, des obligations formelles et des sanctions qui seraient de nature à policer l'industrie du pourriel, dans le cadre d'objectifs clairement déterminés. Une loi spécifique aurait aussi l'avantage de prévoir des modes de preuve et de recours adaptés à cette problématique et favoriserait, plus qu'un ensemble de lois dispersées aux objectifs et aux portées disparates, des ententes internationales visant une application efficace.

Les industries, celle du pourriel et celle de la fourniture de services d'accès Internet, bénéficieraient certainement d'une loi unique qui leur permettrait d'être clairement au fait de leurs droits et obligations sur la question. Les particuliers, qui sont eux aussi victimes du pourriel, seraient certainement mieux servis s'ils pouvaient bénéficier d'un « guichet unique » pour recueillir les plaintes et pour agir en leur nom. Il nous semble aussi important qu'une législation anti-pourriel ouvre la porte à des recours directs contre les entreprises qui ont pu leur causer des dommages, et que cette législation veille à alléger le fardeau de preuve, que ce soit pour l'évaluation du dommage, celle de son quantum ou pour l'établissement de la faute de l'expéditeur.

Une loi spécifique aurait l'avantage de centraliser les moyens d'action et de sanction et pourrait s'adapter plus facilement aux nouvelles formes que pourrait emprunter une problématique

[112] Dumont, Estelle; L'Australie mène la lutte anti-spam – Disponible sur le site Web de Z-Net, au : http://www.zdnet.fr/actualites/internet/0,39020774,39162215,00.htm (page consultée le 12 mai 2005)

[113] Mentionnons à titre d'exemple ce nouveau virus qui arrive en pièces détachées dans des messageries électroniques pour se réassembler une fois franchie avec succès l'étape de l'anti-virus.

donnée ou à ses nouvelles manifestations. Le Canada peut maintenant profiter des expériences étrangères, évaluer le succès d'une approche comme celle qui a été adoptée en Australie et le peu de résultats d'une approche qui ne pénalise que certains excès tout en refusant de bannir la pratique[114].

L'opinion publique est maintenant alertée; le nombre de personnes qui sont affectés par le pourriel et qui réclament qu'il soit rendu illégal est impressionnant. En 2003, 74% des répondants à un sondage américain mené par Harris Interactive insistaient pour que cette pratique soit déclarée illégale, alors qu'entre 70 et 80% des répondants se déclaraient en faveur d'actions légales contre les pourrielleurs. [115]

Au regard des modèles que nous offrent les législations existantes et les projets de lois déposés, et au vu des problématiques que soulève le pourriel, une loi anti-pourriel devrait à notre avis prévoir:

- Une définition très inclusive des messages électroniques visés;
- Une interdiction de tout envoi ou de toute commande d'envoi de messages électroniques publicitaires non-sollicités;
- Des règles claires quand à la nature et la portée des autorisations;
- Des obligations quant à l'affichage (entête, objet, texte, identification);
- L'obligation d'inclure une option qui permette de retirer l'autorisation donnée;
- Une interdiction de concevoir, de distribuer ou d'utiliser des outils d'automatisation de la collecte d'adresses de courrier;
- Une interdiction de générer au hasard des adresses de courrier en vue d'expédier de messages électroniques non-sollicités ou de concevoir ou de distribuer quelque outil permettant de le faire;
- Des obligations pour les fournisseurs de service d'assurer un « monitoring » de leurs réseaux en vue d'interdire l'accès aux pourrielleurs;
- L'obligation pour l'agence chargée de l'application de la loi de travailler à l'élaboration et la conclusion d'ententes internationales en vue de faciliter l'application de la loi;
- Des recours disponibles à toute personne ou entreprise pour qui le pourriel entraînerait des dommages, assortis d'un régime de preuve approprié, prévoyant des présomptions relatives par exemple aux actes reprochés et aux dommages;
- Un régime de sanctions administratives et civiles sérieuses, incluant la possibilité de dommages exemplaires.

Parmi les avantages que présente l'adoption d'une loi anti-pourriel, on pourrait donc de prime abord souligner : 1) l'adaptation à une problématique en évolution ; 2) facilitation du travail des procureurs de l'administration publique, qui pourraient invoquer systématiquement cette loi dans les poursuites relatives aux messages électroniques; 3) développement d'une jurisprudence plus constante et mieux spécialisée; 4) meilleure information du public et de l'industrie sur leurs droits, obligations et recours; 5) facilitation des ententes de coopération internationales visant l'application et l'exécution de la loi .

[114] Selon le magazine Wired, qui cite des sources de l'industrie, l'adoption de la Loi qui, contrairement à plusieurs lois antérieures adoptées par des États américains, empêche les poursuites individuelles au civil à l'encontre des pourrielleurs, n'a pas entraîné de baisse notable du volume de Spam; Ulbrich Chris « Spam travels into gray area » In Wired News. Site de Wired http://www.wired.com/news/technology/0,1282,62087,00.html?tw=wn_tophead_2 (page consultée en mars 2005)

[115] Morrisey, B. "Spam Annoyance on the Rise", InternetNews.com, sur le site Internet de Internetnews.com, au http://www.clickz.com/news/article.php/1564101 (page consultée le 18 juillet 2005)

Plusieurs responsables de la lutte au pourriel aux États-Unis font observer que de nombreux pourrielleurs qui opèrent en dehors du territoire américain n'ont pas semblé jusqu'à présent, malgré l'adoption du CAN-Spam Act, modifier leurs pratiques[116]. Une loi anti-pourriel peut difficilement être parfaitement efficace en l'absence d'un traité de coopération multinational qui viendrait mettre en place le cadre coopératif entre autorités chargées de la lutte au pourriel qui permettrait l'exécution à l'extérieur des frontières des lois nationales .

Le succès de la lutte au pourriel reposerait donc en grande partie sur la coopération internationale. C'est à cette conclusion qu'en arrive, entre autres, le FTC, l'agence fédérale américaine responsable de l'application de la loi fédérale anti-pourriel, qui demandait au Congrès l'autorisation de collaborer plus étroitement avec des autorités étrangères dans le cadre de sa mission de lutte au pourriel. Cette initiative a reçu l'appui d'un des représentants de la Floride au Congrès, qui considérait qu'une lutte au pourriel qui serait limitée au plan domestique ne pourrait qu'être vouée à l'échec, étant donné la dimension internationale du problème et la facilité pour des pourrielleurs d'opérer hors des frontières des États s'étant dotés de lois anti-pourriel trop restrictives[117].

Nous noterons malgré tout que, au plan des actions bilatérales, bien peu a été fait jusqu'à présent. Bien que l'Australie, le Royaume-Uni, les États-Unis et quelques autres aient signé des accords de coopération, le Canada n'a toujours pas rejoint de coalition de ce genre, bien que le gouvernement canadien et les groupes de travail qu'il a mis sur pied se soient prononcés en faveur de telles actions. Le manque de ressources serait à la source de ce manque d'implication[118].

Les expériences ont démontré que les campagnes de sensibilisation devaient être mises à profit en vue d'alerter les victimes du pourriel et de publiciser les solutions ou les pistes d'actions. M. Coroneos, chef de la direction de la Internet Industry Association of Australia, confirmait l'efficacité de cette approche lorsqu'il déclarait que le dépôt du Spam Act 2003 avait suscité beaucoup d'intérêt de la part des médias et que cela avait contribué grandement à publiciser auprès du public le processus de dépôt de plaintes contre le pourriel[119]. Consumers International se prononçait aussi en faveur de la sensibilisation du public, plaidant pour la mise en place d'une vaste campagne, nommée « hit delete », à être utilisée conjointement avec des lois efficaces[120].

Le bilan de l'adoption des codes volontaires et lignes directrices est difficile à mesurer à court terme, puisque leur effet dépend totalement de l'adhésion que ces textes remportent auprès de la communauté de commerçants. Chose certaine, pour que leur rôle de moteur de changement se concrétise, il faut que l'adoption de ce genre d'instruments soit complétée par des actions plus proactives de la part des différents intervenants : actions visant à assurer une participation maximale des associations de l'industrie; supervision continuelle de la part de l'État de

[116] Smith Joshua « Can Spam I told you so's » In Security, Privacy, Policy, Law. Site de Unsecure Privacy. http://www.unsecureprivacy.com/internet/ (page consultée en février 2005)
[117] id.
[118] "Canada won't join international anti-spam coalitions due to lack of resources" In NewsTarget.com. Site de News Target.com http://www.newstarget.com/001912.html (page consultée en avril 2005).
[119] « Éducation et sensibilisation du public : de la sensibilisation à l'action. » In L'Économie Numérique au Canada. Site de Industrie Canada. http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/fr/gv00276f.html #Courtois (page consultée en mars 2005)
[120] Internet Industry Association NEWS RELEASE, Friday, 26 September 2003; disponible au: http://security.iia.net.au/downloads/global%20campaign%20news%20release1.pdf (document consulté le 12 mai 2005)

l'application intégrale par les adhérents des principes visés et communication des principes au public afin que celui-ci puisse également jouer son rôle de chien de garde de l'industrie.

Ici tout comme dans plusieurs pays industrialisés, les grandes industries semblent, pour lutter contre cette problématique, s'en remettre à la technologie plutôt qu'au système juridique. Ainsi, des compagnies comme Spamhaus ont constitué des systèmes, comme des listes de pourrielleurs avec leurs adresses IP en temps réel, afin de bloquer l'accès des comptes de messageries électroniques de leurs clients à partir de ces adresses; ce système de liste de Spamhaus aurait déjà été, depuis 2003, adopté par plusieurs grandes compagnies, agences gouvernementales ainsi que par des millions de particuliers[121].

Les initiatives technologiques foisonnent elles aussi et peuvent représenter un outil complémentaire dans la lutte au pourriel : de nombreux services ou logiciels anti-pourriel ont été mis sur le marché, de même que certaines solutions intermédiaires, comme celle proposée par la société française Kasmail : les adresses électroniques jetables[122] pouvant être utilisées, par exemple, lors d'une inscription à un forum de discussion ou à certains sites « douteux » et que l'on pourra jeter si on y reçoit du pourriel.

Au vu de l'ampleur qu'a très rapidement pris le problème, le temps semble venu de mettre à profit les connaissances et l'expérience acquises pour passer à l'action.

[121] « About Spamhaus » In Spamhaus Project. Working to Protect Internet Networks Worldwide. Site de Spamhaus http://www.spamhaus.org/organization/index.html (page consultée en janvier 2005)
[122] « Disposable Email» In Kasmail. Accueil. Site de Kasmail http://kasmail.com/ (page consultée en décembre 2004)

RECOMMANDATIONS

Attendu que les lois actuelles ne semblent pas adaptées, de par leur conception, leur application, leur objet ou les moyens mis en œuvre pour atteindre ces objectifs, pour lutter efficacement contre la problématique des messages électroniques non sollicités;
Attendu que le pourriel constitue maintenant un problème sérieux, et ce, sur plusieurs plans;
Attendu les dommages qu'entraînent déjà pour les consommateurs les coûts, en frais et en productivité que le pourriel engendre;
Attendu que les expériences étrangères ont tracé la voie pour ce qui pourrait être une législation anti-pourriel efficace;
Attendu que le simple encadrement du pourriel ne semble pas susceptible de contenir le problème;
Attendu les risques que peuvent générer les moyens à mettre en œuvre dans une simple politique de contrôle (par exemple : les Do-Not-Spam Lists), par opposition à une approche qui vise l'interdiction;
Attendu que les développements rapides de la technologie suggèrent que de nouveaux problèmes risquent fort de voir le jour dans la foulée du pourriel;
Attendu qu'une nouvelle législation doit avoir une portée assez vaste pour éviter d'être dépassée par les développements technologiques;

L'Union des consommateurs recommande :

- Que le gouvernement fédéral s'engage dans l'élaboration d'une loi spécifique visant à interdire les communications électroniques non sollicitées;
- Que la législation anti-pourriel à être élaborée veille à inclure :
  - Une définition très inclusive des messages électroniques visés;
  - Une interdiction de tout envoi ou de toute commande d'envoi de messages électroniques publicitaires non-sollicités;
  - Des règles claires quant à la nature et la portée des autorisations;
  - Des obligations quant à l'affichage (en-tête, objet, texte, identification);
  - L'obligation d'inclure une option qui permette de retirer l'autorisation donnée;
  - Une interdiction de concevoir, de distribuer ou d'utiliser des outils d'automatisation de la collecte de courriel;
  - Une interdiction de générer au hasard des courriels en vue d'expédier de messages électroniques non sollicités ou de concevoir ou de distribuer quelque outil permettant de le faire;
  - Des obligations pour les fournisseurs de service d'assurer un « monitoring » de leurs réseaux en vue d'interdire l'accès aux pourrielleurs;
  - L'obligation pour l'agence chargée de l'application de la loi de travailler à l'élaboration et la conclusion d'ententes internationales en vue de faciliter l'application de la loi;
  - Des recours offerts à toute personne ou entreprise pour qui le pourriel entraînerait des dommages, assortis d'un régime de preuve approprié, prévoyant des présomptions relatives par exemple aux actes reprochés et aux dommages;
  - Un régime de sanctions administratives et civiles sérieuses, incluant la possibilité de dommages exemplaires;

Attendu que le problème du pourriel est, de par sa nature même, transfrontalier;
Attendu que les législations nationales ont une portée limitée dans leur application et leur exécution;
Attendu que le succès de la lutte au pourriel reposerait en grande partie sur la coopération internationale;
L'Union des consommateurs recommande :

- Que le gouvernement canadien s'engage dès maintenant activement dans des processus internationaux en vue de conclure des ententes visant à faciliter l'application et l'exécution de sa législation anti-pourriel;

Attendu que les expériences ont démontré que les campagnes de sensibilisation devaient être mises à profit en vue d'alerter les victimes du pourriel et de publiciser les solutions ou les pistes d'actions;
Attendu que le Groupe de travail sur l'éducation et la sensibilisation des consommateurs mis sur pied par le ministre de l'Industrie en est arrivé à la conclusion que les campagnes d'éducation et de sensibilisation devaient se poursuivre;
L'Union des consommateurs recommande :

- Que le gouvernement canadien veille à ce que se poursuive le travail d'éducation et de sensibilisation du public quant au pourriel;

Attendu que plusieurs intérêts sont touchés par la problématique du pourriel (Industrie du télémarketing, FSI, consommateurs, etc.) et que diverses associations veillent à la protection de ces intérêts;
Attendu que ces différents groupes d'intérêt ne disposent pas de ressources équivalentes pour faire valoir adéquatement leurs positions;
L'Union des consommateurs recommande :

- Que le gouvernement sollicite la participation active des groupes de défense des droits des consommateurs dans l'élaboration de sa loi anti-pourriel, des ententes internationales visant à en assurer l'application et l'exécution ainsi que dans les campagnes de sensibilisation à être entreprises, et qu'il leur fournisse les ressources nécessaires à une participation adéquate;

Attendu que l'industrie reconnaît l'importance et la pertinence des codes de pratique applicables à des secteurs spécifiques de l'industrie et du commerce;
Attendu que l'adhésion volontaire à ces codes de pratique n'est pas de nature à garantir leur respect par l'ensemble des intervenants de ces différents secteurs;
Attendu les conséquences souvent minimes qu'entraîne le non respect de ces codes;
L'Union des consommateurs recommande :

- Que les gouvernements fédéral et provinciaux étudient la possibilité et la pertinence de rendre obligatoire à différents secteurs de l'industrie et du commerce l'adhésion à une association professionnelle reconnue;
- Que les gouvernements fédéral et provinciaux imposent à ces associations professionnelles l'adoption de codes de pratique;
- Que les gouvernements fédéral et provinciaux prévoient dans les lois pertinentes des moyens de s'assurer du respect des codes de pratique et de l'application des règles qu'ils fixent, ainsi qu'un régime de sanction applicable aux contrevenants;

- Que les gouvernements fédéral et provinciaux sollicitent la participation active des groupes de défense des droits des consommateurs dans l'élaboration des codes de pratique et de leurs modes d'exécution, et qu'ils leur fournissent les ressources nécessaires à une participation adéquate.

MÉDIAGRAPHIE

Anti-Phishing Working Group, Phishing AvtivityTrend Report, april 2005, http://antiphishing.org/APWG_Phishing_Activity_Report_April_2005.pdf

Arrêtezlepourrielici.ca, Combattre le pourriel : trois conseils clés, arrêtezlepourrielici.ca, http://arretezlepourrielici.ca/

California Business and Professions Code, FindLaw, États-Unis, http://caselaw.lp.findlaw.com/cacodes/bpc.html

Canadian Marketing Association (CMA), CMA, 2005,
About CMA, http://www.the-cma.org/about/index.cfmhttp://www.the-cma.org/about/background.cfm
Dealing with Spam, http://www.the-cma.org/consumer/spam.cfm

CHEZZI, Derek, You've got Spam, Macleans.ca – Technology, Macleans. http://www.macleans.ca/topstories/technology/article.jsp?content=20040223_75808_75808

Clearswift, Statistiques, Mag-Securs, 2004, http://www.mag-securs.com/article.php3?id_article=868

Communications and Media Authority, Australian Communications and Media Authority (ACMA), 2005,
Consumer Information
http://internet.ACMA.gov.au/ACAINTER.65636:HOMEPAGE:760085865:pc=PC_3,tlp=PC_3
Spamact
http://internet.aca.gov.au/ACAINTER.2293792:STANDARD:2081803710:pp=DIR2_25,pc=PC_1966#Spamact

CRTC, Communiqué de presse : CRTC ne réglementera pas Internet, Conseil de la radiodiffusion et des télécommunications canadiennes, http://www.crtc.gc.ca/frn/NEWS/RELEASES/1999/R990517.htm

Dictionnaire de la high tech, définition du phishing, Internaute magazine, http://encyclopedie.linternaute.com/definition/591/11/0/phishing.shtml

DUMONT, Estelle, L'Australie mène la lutte anti-spam, Z-Net, http://www.zdnet.fr/actualites/internet/0,39020774,39162215,00.htm

FCC Consumer Facts, CAN-SPAM : Unwanted text messages and e-mail on wireless phones and other mobile devices, Communications Commission Consumer and Governmental Affairs Bureau. http://ftp.fcc.gov/cgb/consumerfacts/canspam.html

Federal Trade Commission, Keep your email address unlisted : there is no national do not email registry, FTC Consumer Alert,
http://www.ftc.gov/bcp/conline/pubs/alerts/dnealrt.pdf

GEIST, Michael, Untouchable: a Canadian perspective on the anti-spam battle, Michael Geist, http://www.michaelgeist.ca/geistSpam/.pdf

GROSS, Grant, Update : majors ISPs sue hundred of spammers, The Standard.com, http://www.thestandard.com/article.php?story=20040310183418590&

HARDING, Jon, Canada won't join international anti-spam coalitions due to lack of resources, 15 septembre 2004, cnews, canoe, http://cnews.canoe.ca/CNEWS/TechNews/Internet/2004/09/15/629956.html

HAWKE, David Wolfgang, et al., Complaint and Exhibits, (nom de la cause)America Online, Findlaw.com, http://news.findlaw.com/hdocs/docs/cyberlaw/aolhawke30904cmp.pdf

IANA (Internet Assigned Names Authority), Reasons why Port 25 is blocked on connections, NDO.com, http://www.ndo.com/ndo/Support/The_reasons_why_Port_25_is_blocked_on_connections/port25why.html

Industrie Canada, Économie numérique au Canada, Industrie Canada,
Plan d'action de Londres sur la Coopération internationale relative à l'application des lois antipourriel, http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/fr/gv00288f.html
Document d'information, http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/fr/gv00291f.html
Plan d'action antipourriel pour le Canada, http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/fr/h_gv00246f.html
L'internet et le courrier électronique en vrac non sollicité, http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/fr/gv00188f.html
Éducation et sensibilisation du public : de la sensibilisation à l'action http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/fr/gv00276f.html #Courtois

Industrie Canada, Code canadien de pratiques pour la protection des consommateurs dans le commerce électronique, Carrefour des consommateurs, 2005, http://strategis.ic.gc.ca/epic/internet/inoca-bc.nsf/fr/ca01490f.html

Internet Industry Association, News release, 26 septembre 2003, http://security.iia.net.au/downloads/global%20campaign%20news%20release1.pdf

Kasmail, Disposable Email, Accueildu site, Kasmail http://kasmail.com/

KRIM, Jonathan, Spam's costs to business escalates, Washington Post, 12 mars 2003, http://www.washingtonpost.com/ac2/wp-dyn/A17754-2003Mar12

LALONDE, Jean, Les lois canadiennes –actuelles seraient suffisantes, pourriel.ca. Politique légale, pourriel.ca http://www.pourriel.ca/archives/000749.php

Microsoft Sécurité, Conseils, Microsoft France, http://www.microsoft.com/france/securite/gpublic/email/options.mspx

MORRISSEY, B., Spam Annoyance on the Rise, InternetNews.com, http://www.clickz.com/news/article.php/1564101

Nucleus Research, Spam : the silent ROI killer, http://www.nucleusresearch.com/research/d59.pdf

OECD, Guidelines for Consumer Protection in the Context of Electronic Commerce (1999), Sécurité de l'information et protection de la vie privée, http://www.oecd.org/document/51/0,2340,fr_2649_34255_1824435_1_1_1_1,00.html

Page contactez-nous, Commissariat à la vie privée, 2005, http://www.privcom.gc.ca/contactUs/index_f.asp

POULAIN, Charles, Les pourriels coûtent plus d'un milliard au Québec, Journal de montréal, 7 novembre 2003, http://www2.canoe.com/techno/nouvelles/archives/2003/11/20031107-062614.html

Pratiques exemplaires recommandées pour les fournisseurs de services Internet et autres exploitants de réseaux, http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/fr/gv00286f.html

REID, Thelen, California Enacts Two "Anti-Spam" Bills Targeting Unsolicited E-mail. ConstructionWebLink, http://www.constructionweblinks.com/Resources/Industry_Reports__Newsletters/Oct_2_1998/oct_2_1998.htm

ROOSE, Dave, Spam Queen : just trying to make a living, G4, ~~In G4. Site de G4~~ http://www.techtv.com/screensavers/showtell/story/0,24330,3407919,00.html

SMITH, Joshua, Can Spam I told you so's,Security, Privacy, Policy, Law. Site de Unsecure Privacy. http://www.unsecureprivacy.com/internet/ (page consultée en février 2005)

SMITH, Robert H., School of Business, Statistiques de janvier 2005, Le Journal du Net, http://www.journaldunet.com/cc/03_internetmonde/spam.shtml

SORKIN, David E., Spam Laws, Spam Laws United States; Virginia, Spam Laws. http://www.Spamlaws.com/state/va.html

ULBRICH, Chris, Spam law generates confusion, Wired News, http://www.wired.com/news/business/0,1367,62031,00.html

ULBRICH, Chris, Spam travels into gray area, Wired News. 2005, http://www.wired.com/news/technology/0,1282,62087,00.html?tw=wn_tophead_2

Vidéotron, Conditions d'abonnement. Contrat Internet. In Vidéotron. Service à la clientèle. http://www.videotron.com/services/fr/service_clientele/8_3_1.jsp

WARD, Mark, How to make spam unstoppable, BBC News Worl Edition, http://news.bbc.co.uk/2/hi/technology/3458457.stm

Working to Protect Internet Networks Worldwide, About Spamhaus, Spamhaus Project. Working to Protect Internet Networks Worldwide. Spamhaus, http://www.spamhaus.org/organization/index.html

United States Government, Fraud and Related activity in connection with computers. US Code Collection, Legal Information Institute http://www4.law.cornell.edu/uscode/18/1030.html