Analyse du cadre réglementaire québécois et étranger à l'égard du pourriel, de l'hameçonnage et des logiciels espions

Pierre TRUDEL
France ABRAN
Gabriel DUPUIS

Rapport préparé pour la Direction des politiques du ministère des Services gouvernementaux du Québec

Avril 2007

Chaire L.R. Wilson sur le droit des technologies de l'information et du commerce électronique

Centre de recherche en droit public

Faculté de droit
Université de Montréal

Tables des matières

DEUXIÈME PARTIE
LES TENDANCES DE LA PRATIQUE INTERNATIONALE QUANT À LA RÉGLEMENTATION DU POURRIEL, DE L'HAMEÇONNAGE ET DES LOGICIELS ESPIONS

TROISIÈME PARTIE
ANALYSE DU CADRE RÉGLEMENTAIRE QUÉBÉCOIS DU POURRIEL, DE L'HAMEÇONNAGE ET DES LOGICIELS ESPIONS

SOMMAIRE

Le pourriel est passé de nuisance à danger véritable ; il a favorisé l'apparition de nouvelles menaces, comme les logiciels espions (*spyware*), les courriels hameçons (*phishing*) et la falsification de sites Web de certaines entreprises et institutions. L'ensemble de ces phénomènes est devenu emblématique des entraves au développement d'Internet. Ces fléaux constituent désormais de réelles menaces au développement d'Internet comme environnement digne de confiance.

De plus en plus d'activités commerciales et personnelles reposent sur l'utilisation des ordinateurs et d'Internet. Ces menaces, en diminuant la confiance en l'Internet et en accroissant les coûts liés à la sécurité, risquent de faire paraître la « vieille économie » comme une meilleure alternative, réduisant à néant des années d'efforts.

Phénomène multiforme, le pourriel n'a que récemment fait l'objet d'attention de la part des autorités publiques. Il y a peu de données officielles sur son ampleur et sur son évolution. Mais il est certain que les pratiques liées au pourriel se révèlent de plus en plus dommageables pour les utilisateurs.

Ce rapport s'inscrit dans une logique d'élaboration d'une stratégie d'intervention afin d'orienter les actions gouvernementales touchant les menaces de l'Internet et, plus particulièrement, le pourriel. Tout en apportant des réponses au regard de la portée de la législation actuellement applicable au Québec à l'égard des trois phénomènes, l'étude propose des éclairages sur les stratégies mises en place dans d'autres juridictions afin d'y faire face.

Une première partie fait l'état des lieux et décrit comment se présentent les principales pratiques de pourriel, de l'hameçonnage et des espiogiciels. Le pourriel tend à se métamorphoser en vecteur pour un ensemble d'activités illicites. On y constate la rapidité de développement et les multiples facettes empruntées par ce phénomène afin de contourner tout type de barrière.

Les tendances de la pratique internationale en matière de régulation du pourriel et des autres fléaux d'Internet sont examinées dans la deuxième partie. Certains pays comme l'Australie ont mis en place des initiatives concertées, caractérisées à la fois par des énoncés législatifs forts contre les pratiques liées au pourriel et un large spectre de mesures visant à en assurer l'application effective. De la même façon, les instances européennes ont adopté des directives visant certains aspects du pourriel. Certains États européens ont mis en œuvre ces volontés en instituant des mesures concertées appliquées selon des approches de coopération entre les autorités gouvernementales, le secteur privé et les autorités d'autres pays. Aux États-Unis, l'approche du phénomène est caractérisée, non seulement par la loi fédérale CAN-SPAM mais par des actions législatives prises dans pas moins de 38 états.

La tendance la plus prometteuse paraît être celle mise de l'avant par l'OCDE avec son approche de « boîte à outils » reposant sur le principe selon lequel il faut mobiliser de façon ordonnée plusieurs éléments différents afin de favoriser le développement de stratégies et solutions de lutte contre le pourriel – techniques, réglementaires et d'application de la loi – et faciliter la coopération internationale face à ce problème.

En 2004, le gouvernement du Canada a mis sur pied le Groupe de travail sur le pourriel. Ce groupe a énoncé des recommandations dans le rapport intitulé *Freinons le pourriel-Créer un Internet plus fort et plus sécuritaire*[1] publié en mai 2005. Ce rapport propose l'adoption d'une loi au niveau fédéral et l'implantation d'une stratégie canadienne de lutte au pourriel fondée sur l'approche préconisée par l'OCDE.

1 *Rapport du Groupe de travail sur le pourriel*, mai 2005, < http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/fr/h_gv00248f.html >.

Dans la troisième partie, est examiné le corpus des règles de droit applicables au Québec à l'égard des comportements associés à la production et à l'envoi de pourriel, à l'hameçonnage et aux espiogiciels. On y constate qu'un bon nombre de gestes associés au pourriel, à l'hameçonnage et aux espiogiciels comme la collecte systématique d'adresses, l'expédition de messages non sollicités ou frauduleux de même que l'installation non consentie d'espiogiciels sont déjà en bonne partie visés par des dispositions de lois d'application générale. Les lois applicables à ces gestes sont résumées dans les deux tableaux qui suivent.

Tableau 1 - Lois applicables au pourriel et à l'hameçonnage

La plupart des gestes identifiés ci-dessous sont susceptibles de constituer une faute au sens de l'article 1457 C.c.Q. et d'engager la responsabilité de leur auteur.

COLLECTE D'ADRESSES	EXPÉDITION	CONTENU
Voir section 1.1.1, p. 56 **VENTE OU ACHAT D'UNE LISTE NOMINATIVE SANS LE CONSENTEMENT DE L'INTÉRESSÉ À DES FINS DE PROSPECTION COMMERCIALE OU PHILANTHROPIQUE** *Loi sur la protection des renseignements personnels dans le secteur privé*, art. 22. ► Par dérogation aux principes établis aux articles 6 et 13. ► L'art. 22 affirme qu'une liste nominative peut être constituée d'une adresse technologique (courriel). Ainsi, il s'applique donc à toutes les adresses de courrier électronique, peu importent qu'elles identifient ou non leur détenteur.	Voir section 1.2.1, p. 57 **ENVOI NON SOLLICITÉ** *Loi sur les télécommunications*, art. 41. ► Accorde au CRTC un pouvoir de réglementation sur le pourriel. Ce pouvoir n'a pas encore été exploité à ce jour.	Voir section 1.3.1, p. 58 **FAUSSES REPRÉSENTATIONS VISANT À PROMOUVOIR UN PRODUIT OU UN SERVICE** *Code criminel*, art. 408 (substitution frauduleuse). *Loi sur la concurrence*, art. 52 (sanction criminelle) et 74.01 (sanction administrative). *Loi sur la protection du consommateur*, art. 219. (fausses représentations) *Loi sur les aliments et drogues*, art. 9 (fraude).
Voir section 1.1.2, p. 57 **ATTAQUES PAR DICTIONNAIRE ET DE « FORCE BRUTE »** *Code criminel*, art. 430 (1.1) c) (Méfait) ► Certains affirment que l'art. 342.1 interdit les attaques par dictionnaire. ► Pour être plus précis l'art. 430 (1.1) c) peut interdire ce genre d'attaques dans la mesure où elles « gêne[nt] l'emploi légitime des données » (le courriel, en l'espèce). Une attaque si intense qu'elle ralentit le serveur courriel serait un bon exemple de méfait au sens de l'art. 430. ► L'art. 342.1 (1) c) peut également recevoir application si l'ordinateur d'un tiers est utilisé pour commettre le méfait.	Voir section 1.2.2, p. 57 **USURPATION DES RESSOURCES INFORMATIQUES D'AUTRUI** (Piratage d'un réseau d'entreprise, transformation d'un PC en « zombie »). *Code criminel*, art. 342.1 (utilisation non autorisée d'ordinateur) ► L'art 326 (1) b) (vol de service de télécommunication) ne s'applique pas, car, selon *R.* c. *McLaughlin*, [1980] 2 R.C.S. 331, un ordinateur n'est pas une « installation de télécommunication ».	Voir section 1.3.4, p. 59 **FRAUDES « PUMP AND DUMP »** *Code criminel*, art. 382 b) (manipulations frauduleuses d'opérations boursières). *Code criminel*, art. 380 (2) (fraude). *Loi sur les valeurs mobilières*, art. 195.2 (influencer frauduleusement le cours d'un titre) ► Voir l'art. 204 pour déterminer la sanction.

COLLECTE D'ADRESSES	EXPÉDITION	CONTENU
Voir section 1.1.2, p. 57 **BALAYAGE DU WEB** *Loi sur la protection des renseignements personnels dans le secteur privé*, art. 4-6. ► L'article 342.1 du *Code criminel* portant sur l'utilisation non autorisée d'ordinateur pourrait s'appliquer. Mais il n'est pas certain que sa rédaction puisse donner lieu à un interdit de balayer le Web à la recherche d'adresses courriel.	Voir section 1.2.3, p. 58 **TRAFICAGE DU CHAMP « DE : »** *Code criminel*, art. 372 (1) (faux messages) ► La portée de l'article 372 (1) est assez large pour rendre superflue une mise à jour de l'article 371. Il nécessite toutefois une intention de nuire à la personne. *Loi sur la protection des renseignements personnels dans le secteur privé*, art. 24 (obligation de s'identifier). *Loi sur la concurrence*, art. 52 (sanction criminelle) et 74.01 (sanction administrative). ► Si on considère le mensonge sur l'identité comme constituant une fausse représentation. *Loi sur la protection du consommateur*, art. 238 c), 242 et 219 (fausses représentations).	Voir section 1.3.5, p. 60 **HAMEÇONNAGE** *Code criminel*, art. 380 (interdiction générale de frauder). *Code criminel*, art. 403 (vol d'identité) *Code criminel*, art. 342 (utilisation non autorisée du numéro de carte de crédit) *Code criminel*, art. 362 (escroquerie) *Code criminel*, art. 372 (1). (utilisation de faux prétextes pour amener une personne à divulguer ses renseignements personnels.)
	Voir section 1.2.1, p. 57 **REFUS DE RETIRER UNE PERSONNE D'UNE LISTE NOMINATIVE (OPT-OUT)** *Loi sur la protection des renseignements personnels dans le secteur privé*, art. 24.	Voir section 1.3,5, p. 60 **USURPATION DE MARQUE, DE L'IMAGE CORPORATIVE** *Code criminel*, art. 406. *Loi sur les marques de commerce*, art. 7.
	LOGICIELS FACILITANT LE POURRIEL *Code criminel*, 342.2	Voir section 1.3.3, p. 59 **VIRUS, VERS ET CHEVAUX DE TROIE** *Code criminel*, art. 342.2 et 430 (1.1)

Tableau 2 - Lois applicables aux logiciels espions

NOTE : La plupart des gestes énumérés ci-dessous sont susceptibles de constituer une faute au sens de l'article 1457 C.c.Q. et d'engager la responsabilité de leur auteur.

INSTALLATION	COMPORTEMENT	EFFETS
Voir section 2.1, p. 61 **INSTALLATION NON CONSENTIE (SITES WEB MALICIEUX, FICHIERS CONTAMINÉS, ETC.)** *Code criminel*, art. 342.1 (utilisation non autorisée d'ordinateur) *Code civil du Québec*, art. 36	Voir section 2.2.1, p. 62 **CUEILLETTE D'INFORMATIONS PERSONNELLES, PROFILAGE MARKETING** *Loi sur la protection des renseignements personnels dans le secteur privé*, art. 4-6, 12-15 et 22-25. *Code civil du Québec*, art. 37.	Voir section 2.3, p. 63 **ENVAHISSEMENT DE L'INTERFACE GRAPHIQUE, PANNES ET RALENTISSEMENTS LIÉS À LA PRÉSENCE DE LOGICIELS ESPIONS** *Code criminel*, art. 430 (méfait sur les données). *Code civil du Québec*, art. 1457 et 1458 (responsabilité civile).
Voir section 2.1, p. 61 **INSTALLATION AU CONSENTEMENT « BOITEUX »** *Code civil du Québec*, art. 1399 à 1401 ► Pour juger la validité du consentement à l'installation du logiciel.	Voir section 2,2,2, p. 62 **INTERCEPTION DES COMMUNICATIONS (KEYLOGGING)** *Code criminel*, art. 342.1. ► Certains auteurs affirment que l'art. 184 ne peut recevoir application, étant donné qu'il exige que la communication soit faite entre deux personnes et non entre une personne et un ordinateur. *Charte des droits et libertés de la personne,* art. 5. *Code civil du Québec*, art. 35 et 36.	

INSTALLATION	COMPORTEMENT	EFFETS
	Voir section 2.2.3, p. 63 **APPROPRIATION DES COMMISSIONS D'AUTRUI** *Code criminel*, art. 380.	
	Voir section 2.2.4, p. 63 **FAUSSES ALERTES DE SÉCURITÉ AFIN DE VENDRE UN PSEUDO ANTI-VIRUS** *Code criminel,* art. 380 et 372 (1). *Loi sur la concurrence*, art. 52 (sanction criminelle) et 74.01 (sanction administrative). *Loi sur la protection du consommateur*, art. 219. ► Si la vente de produit de sécurité est réalisée entre le consommateur et le développeur du logiciel espion responsable de la fausse représentation.	

Dans la quatrième partie, sont identifiées les pistes pour la mise en œuvre d'une intervention à volets multiples afin de faire face aux fléaux du pourriel et ce qui en découle. Une telle stratégie d'intervention doit être pensée dans le contexte d'un réseau. Dans un réseau, la normativité se déploie elle aussi en réseau. Cette stratégie est envisagée comme une opération de modulation et de gestion des risques d'Internet. Le défi étant d'augmenter les risques associés aux pratiques nuisibles et de diminuer le plus possible les risques des utilisateurs légitimes du réseau, il faut renforcer l'ensemble des nœuds dans lesquels s'expriment les normes.

Mais il importe surtout d'assurer que les exigences mises en place soient effectivement relayées vers l'ensemble des utilisateurs. Il s'agit de faire en sorte que les activités associées au pourriel soient rendues le plus risquées possible en ayant recours à tous les moyens disponibles.

La loi fixe les règles du jeu à l'égard des acteurs menant une activité possédant un rattachement avec le Québec. Tant par le message fort qu'elle envoie que par sa capacité à poser les règles, la loi est un instrument nécessaire dans une stratégie de lutte contre le pourriel et les fléaux qui y sont associés. Mais en soi, la loi est un outil insuffisant si elle ne s'inscrit pas dans une stratégie dynamique d'application.

Les solutions techniques et les pratiques exemplaires des acteurs publics et privés sont au nombre de moyens d'assurer la tenue à jour d'une stratégie anti-pourriel. Il importe en effet de se donner les moyens de suivre les évolutions et d'ajuster en continu les façons de faire. À cet égard, le maintien en phase avec les normes mises de l'avant dans les forums internationaux paraît essentiel.

On aura beau avoir les meilleures normes et pratiques, l'efficacité de la lutte contre le pourriel passe nécessairement par la mobilisation des différents relais par lesquels on assure l'application effective des lois et autres normes. Les stratégies de suivi et de répression des activités illicites doivent être concertées. Les divers acteurs qui prennent part à des activités sur Internet doivent être incités à prendre tous les moyens pour limiter les risques d'Internet. Pour les acteurs légitimes, cela signifie de prendre part aux coordinations mises en place afin d'augmenter les risques de ceux qui se livrent à des pratiques illicites sur le réseau. De tels risques doivent être tenus à un niveau élevé par les acteurs désireux de lutter contre le pourriel.

INTRODUCTION

De simple nuisance, le pourriel est devenu un phénomène franchement dangereux avec l'apparition de nouvelles menaces, comme les logiciels espions (*spyware*), les courriels hameçons (*phishing*) et la falsification de sites Web de certaines institutions. Ces phénomènes sont emblématiques des entraves au développement d'Internet comme environnement digne de confiance.

De plus en plus d'aspects des situations commerciales et de la vie privée reposent sur l'utilisation d'Internet. Les menaces diminuent la confiance et accroissent les coûts liés aux précautions pour les usagers légitimes. L'ensemble des pratiques abusives porte le risque de faire paraître la « vieille économie » comme une meilleure alternative à celle que présente le déroulement en ligne des interactions.

Ce rapport veut contribuer à l'élaboration d'une stratégie d'intervention afin d'orienter les actions touchant les menaces de l'Internet et, plus particulièrement, le pourriel. Il apporte des réponses au regard de la portée de la législation actuellement applicable au Québec à l'égard des trois phénomènes. L'étude propose des éclairages sur les stratégies mises en place dans d'autres juridictions afin d'y faire face.

La première partie propose un état des lieux du phénomène du pourriel, de l'hameçonnage et des logiciels espions. Cette revue documentaire permet de qualifier les phénomènes au plan quantitatif et au plan qualitatif afin de mieux identifier les enjeux réels de régulation qu'ils posent. On y constate que le pourriel est passé d'un embarras relativement inoffensif à des pratiques sophistiquées servant d'amorce à un ensemble de manœuvres ayant souvent un caractère frauduleux.

La seconde partie présente, en plus de la situation canadienne, les mesures prises dans d'autres juridictions, notamment en Europe, en Australie et aux États-Unis, pour endiguer les menaces découlant du pourriel. On y examine les résultats obtenus grâce à ces mesures. Il en ressort que l'approche dite de « boîte à outils » préconisée par l'OCDE est considérée comme la plus à même de donner des résultats intéressants dans la lutte aux phénomènes liés au pourriel.

Afin de déterminer dans quelle mesure, le cadre législatif et réglementaire québécois actuel est suffisant pour faire face à ces menaces, la troisième partie identifie les principales dispositions des lois existantes qui sont susceptibles de trouver application à l'égard de l'un ou l'autre des gestes associés au pourriel.

Enfin, la quatrième partie présente les éléments d'une stratégie québécoise visant à accroître les risques de ceux qui se livrent à des activités illicites fondées sur le pourriel. La stratégie doit également comporter un ensemble de mesures pour renforcer la sécurité des internautes qui se livrent à des activités légitimes. Pour être vraiment efficace, une stratégie de lutte contre les pratiques liées au pourriel doit renforcer les diverses règles, au premier chef les lois, qui concernent les gestes associés au pourriel. Mais la stratégie doit comporter des engagements fermes afin de relayer les exigences des lois. Il faut une action concertée pour assurer l'application effective des règles de manière à maximiser les risques des polluposteurs et minimiser ceux des utilisateurs légitimes d'Internet.

La présente étude a été réalisée pour le compte de la Direction des politiques du Ministère des services gouvernementaux du Québec. Les auteurs ont bénéficié des conseils de M. Jean-Michel Salvador, conseiller scientifique à la Direction des politiques du Ministère des services gouvernementaux et de M. Pierre Sasseville du même ministère. Mme Yolande Côté de l'Office de protection du consommateur a également fourni des informations et formulé des remarques sur une version antérieure de ce rapport. Sans l'aide de ces experts, ce rapport comporterait moins de nuances, développements et bonnes idées qui feront peut-être son intérêt. Mais les carences qui y subsistent ne sauraient être imputées à d'autres qu'aux auteurs. L'équipe a également pû compter sur le bon travail de Mme Erica Stermer, stagiaire au Centre de recherche en droit public, qui a contribué aux recherches documentaires. Enfin, l'excellent

travail de Sylvie Thériault-Sylvestre qui a travaillé à la mise en forme du texte doit également être souligné.

PREMIÈRE PARTIE
POURRIEL, HAMEÇONNAGE
ET LOGICIELS ESPIONS : UN ÉTAT DES LIEUX

Dans cette partie, on dresse un état descriptif des phénomènes du pourriel, de l'hameçonnage et des logiciels espions.

1. Le pourriel et l'hameçonnage

Le pourriel ne conduit pas toujours à l'hameçonnage mais de plus en plus, il est un vecteur pour faciliter la commission de gestes illicites. Les réalités visées ici ont un sens qui peut varier selon les évolutions. Le mot ***pourriel***, proposé par l'Office québécois de la langue française en mai 1997, est un mot-valise construit à partir de *poubelle* et *courriel*. Il concerne primordialement le courriel non sollicité ou non souhaité. Mais par extension, la notion est parfois utilisée afin de désigner diverses pratiques abusives des ressources d'Internet.

L'hameçonnage, en anglais ***phishing***, est une technique utilisée par des personnes mal intentionnées pour obtenir des renseignements personnels. Dans certains cas, ces renseignements personnels pourront faciliter l'usurpation d'identité. La technique consiste à faire croire à la victime qu'elle s'adresse à une entité digne de confiance — banque, administration, etc. — afin de lui soutirer des renseignements personnels : mot de passe, numéro de carte, date de naissance, etc. L'hameçonnage peut emprunter le courriel, des sites falsifiés ou autres moyens électroniques.

1.1 Description et évolution

Pratiquement tout internaute a déjà reçu un courriel d'une source inconnue qui veut lui vendre un produit plutôt douteux. De prime abord, la chose peut paraître banale : l'internaute n'a qu'à supprimer le message. Même s'il fut envisagé d'abord comme une simple nuisance, le pourriel est maintenant considéré par plusieurs comme un fléau technologique, social et économique qu'il faut combattre.

Et pour cause. Le pourriel est de plus en plus présent dans les boîtes à courriels des usagers d'Internet. Son filtrage de même que ses effets coûtent cher à la collectivité. Sans compter qu'il transporte depuis ces dernières années de sérieuses menaces à la sécurité informatique et bancaire.

1.1.1 Définition

Étant donné le manque de consensus à cet égard dans l'industrie, il serait plutôt hasardeux de donner une définition exhaustive de ce qui constitue un pourriel. Il est possible, tout de même, d'identifier les caractéristiques-clés qui permettent — à première vue — de qualifier un courrier électronique de « pourriel » (ou de spam, en anglais). Dans un rapport sur les moyens à prendre pour lutter contre ce phénomène, l'OCDE a constaté que les spécialistes s'entendent pour définir le pourriel à partir des caractéristiques suivantes :

- **Message électronique :** les spams transitent par voie électronique. Le courrier électronique en est le principal vecteur, mais d'autres canaux de transmission sont utilisés dans plusieurs pays (spam mobile : SMS et MMS, spam sur IP, etc.)

- **Dissimulation ou falsification de l'origine des messages :** les spams sont souvent envoyés de manière à ce que l'identité de l'expéditeur soit dissimulée derrière des informations d'en-tête fausses. Les spammeurs utilisent souvent sans autorisation des serveurs de messagerie tiers.

- Un spam ne propose **pas d'adresse valide** et fonctionnelle à laquelle les destinataires peuvent envoyer un message pour demander de ne plus recevoir de messages non sollicités.

- **Contenu illégal et condamnable :** le spam est souvent le vecteur de contenus frauduleux ou trompeurs, de virus, etc. Il peut aussi contenir des contenus pornographiques ou condamnables qui peuvent être illégaux dans certains pays, en particulier lorsqu'ils sont adressés à des mineurs.

- **Utilisation d'adresses sans le consentement du propriétaire :** Les spammeurs utilisent souvent des adresses de courriel collectées sans le consentement explicite de leur propriétaire, souvent en utilisant des logiciels qui recueillent sur le Web ou génèrent des adresses de courrier électronique (collecte et attaque par dictionnaire).

- **Envois en nombre et répétés :** les spammeurs envoient généralement leurs messages en masse de manière non sélective, sans avoir aucune autre information sur les destinataires que leur adresse électronique[2].

L'élément commun de ces critères est le caractère abusif des pratiques. Les polluposteurs n'ont pas su insuffler à leur activité une certaine rigueur et, de ce fait, présenter leur activité comme une méthode de « marketing direct » socialement acceptable. De tels efforts ont pourtant été faits du côté des producteurs de logiciels publicitaires et, à plus forte raison, des annonceurs qui utilisent la poste traditionnelle. Face à ce manque d'autodiscipline, plusieurs pays ont adopté des législations rigoureuses en matière de pourriel[3]. D'ailleurs, le pourriel est de moins en moins le fait d'entreprises légitimes; il se présente désormais comme le support à des activités carrément illicites.

1.1.2 Mesurer le pourriel

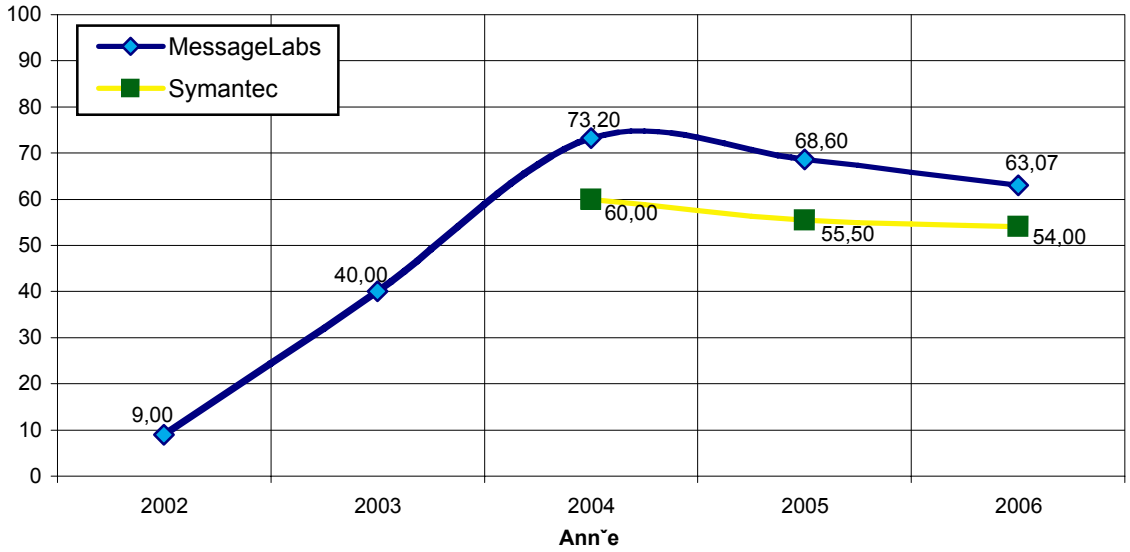

Fig. 1 Ń Courriels non sollicit˜s sur le total de messages exp˜di˜s (en %)

Il n'existe pas de données officielles évaluant la croissance qu'a connu le pourriel ces dernières années. Les données qui existent actuellement sur le pourriel proviennent de fournisseurs de technologies anti-pourriel qui en ont centralisé le filtrage, ce qui leur permet de faire appel à des échantillons de millions de

2 OCDE, *Rapport du groupe de réflexion sur le spam de l'OCDE: boîte à outils anti-spam de politiques et mesures recommandées*, http://www.oecd-antispam.org, pp. 20-21.

3 Voir la section *1. Les tendances des législations* dans la deuxième partie de ce rapport.

boîtes à courriel à travers le monde. À titre d'exemple, la firme MessageLabs fonde ses prétentions sur l'analyse des 180 millions de courriels qu'elle filtre quotidiennement[4]. D'autre part, l'*Internet Security Threat Report* de Symantec recense aussi la proportion de pourriels par rapport à l'ensemble des courriels échangés[5].

La Figure 1 indique que la proportion de pourriels sur le total de courriers électroniques échangés a connu une importante augmentation entre les années 2002 et 2004, pour ensuite se stabiliser, voire même s'amenuiser. Les résultats de Symantec sont relativement inférieurs à ceux de MessageLabs, mais ils indiquent la même tendance : la propagation des pourriels a atteint des sommets en 2004 et semble se stabiliser depuis.

Symantec et MessageLabs ne sont pas les seules firmes à quantifier le phénomène. Selon le Messaging Anti-Abuse Working Group (MAAWG), qui regroupe plusieurs géants de l'industrie (AOL, Microsoft, Yahoo!, Bell Canada, etc.), environ 80% de tous les courriels envoyés peuvent être assimilés à du pourriel[6]. À ce jour, le groupe de travail n'a publié que deux rapports.

D'autres compagnies comme Postini recueillent des statistiques intéressantes à propos du pourriel[7]. Cependant, la présentation des données « en temps réel » n'est pas suffisamment précise pour en permettre la citation et rend difficile les comparaisons dans le temps. Mentionnons du moins que Postini a affirmé, dans un communiqué émis le 14 mars 2007, que 93 % du courriel échangé en février 2007 était du pourriel[8].

Au Québec, dans un rapport réalisé pour le compte de l'Office de la protection du consommateur, la firme Zerospam estime qu'entre décembre 2004 et octobre 2006, 80,9 % du courriel pouvait être qualifié de « nocif » (spam, virus, hameçonnage). Fait à noter : 42 % des courriels qualifiés de nocifs contenaient une tentative d'hameçonnage.

Dans tous les cas, ces moyennes ne doivent pas occulter le fait que le phénomène, envisagé mensuellement, demeure somme toute variable. L'analyse des distributions mensuelles obtenues par MessageLabs met en lumière cette volatilité (voir Figure 2).

---

4 MessageLabs, *Threat Statistics*, http://www.messagelabs.com/ThreatWatch/ThreatStatistics.

5 Symantec, *Internet Security Threat Report*, vol. VI à X, http://www.symantec.com/enterprise/threatreport.

6 Messaging Anti-Abuse Working Group (MAAWG), *Email Metrics Report – June 2006*, http://www.maawg.com/about/FINAL_1Q2006_Metrics_Report.pdf ; Messaging Anti-Abuse Working Group (MAAWG), *Email Metrics Report – March 2006*, http://www.maawg.com/about/FINAL_4Q2005_Metrics_Report.pdf.

7 http://www.postini.com/stats.

8 http://www.postini.com/news_events/pr/pr031407.php.

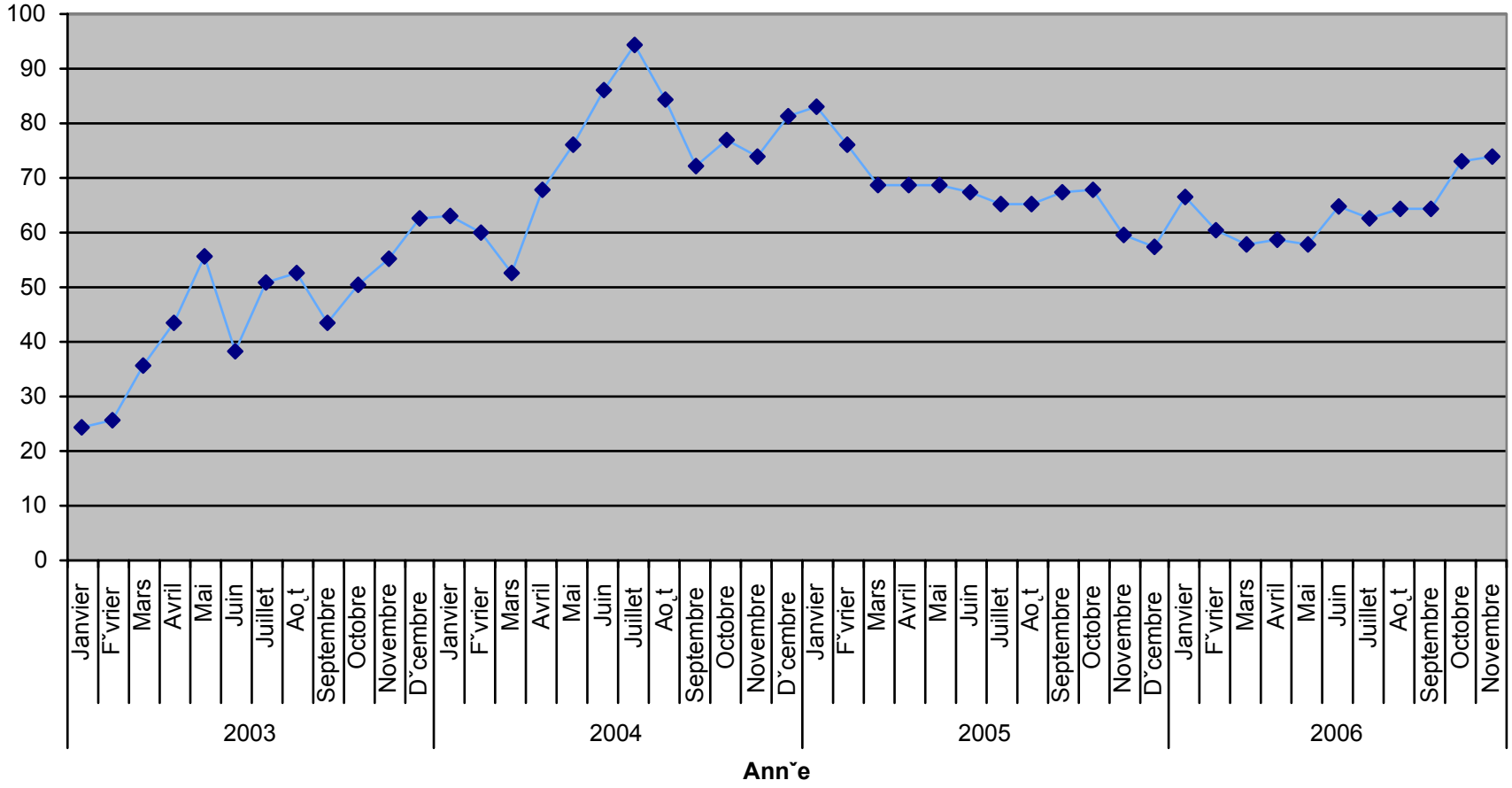

Fig. 2 Ń Courriels non sollicit˘s sur le total de messages exp˘di˘s (en %), 2003-2006

1.1.3 Provenance du pourriel

Des données disponibles indiquent l'origine nationale de l'ordinateur qui a été utilisé pour acheminer le pourriel à son destinataire. Mais la prudence est de mise dans leur interprétation, car les polluposteurs utilisent rarement leurs propres comptes de messagerie électronique pour transmettre des pourriels. Ils préfèrent en effet compromettre le compte d'une autre personne et s'en servir pour mener à bien leurs activités. Ainsi, les attaques sont mieux distribuées, plus difficiles à filtrer et se font dans l'anonymat.

En fait, si ces données ont un mérite, c'est celui d'indiquer où se trouvent les comptes courriels les plus souvent utilisés pour envoyer des courriers électroniques non sollicités. Cependant, même à ce sujet, il est difficile d'en tirer des conclusions trop tranchées étant donné que les résultats auxquels arrivent les firmes de sécurité sont très différents et peu souvent publiés sur une base régulière.

Sophos affirme que pour le dernier quart de l'année 2005, le Canada figurait au 5e rang des pays émettant le plus de pourriel[9], tandis que les statistiques en temps réel de la firme CommTouch excluent le Canada de son « Top 5 » (en date du 19 mars 2007)[10]. Seul le tableau préparé par Symantec nous a semblé mériter reproduction (compte tenu de la réputation de la firme, du caractère systématique de ses recherches et de la publication régulière de ses rapports).

Tableau I
Principaux pays émetteurs de pourriel[11]

Pays	%
États-unis	58
Chine	13
Canada	5
Corée du Sud	5
Royaume-Uni	4
Autres pays de l'UE	4
Belgique	4
Japon	3
France	2
Pologne	2

On remarquera que le Canada figure au troisième rang de ce palmarès. Cette disproportion s'expliquerait par le fait que le Canada (de même que les États-Unis) est un pays où l'accès Internet haute-vitesse est très répandu. Étant toujours activé, ce type de service est en effet plus susceptible d'être la proie d'une attaque, d'autant plus qu'il met à la disposition du polluposteur une bande passante suffisante pour envoyer un grand nombre de courriels.

Spamhaus, un organisme à but non lucratif international dédié au repérage des « Spam Gangs », maintient pour sa part le ROSKO (Register of Known Spam Operations) qui identifie les 200 groupes les

9 http://www.sophos.com/pressoffice/news/articles/2006/01/dirtdozjan05.html.

10 http://www.commtouch.com/site/Resources/statistics.asp.

11 Symantec, *Internet Security Threat Report*, vol. X, p. 90, http://www.symantec.com/enterprise/threatreport/ent-whitepaper_symantec_internet_security_threat_report_x_09_2006.pdf.

plus actifs dans le domaine du pollupostage. Selon l'organisme, le Canada figure au 9e rang des pays ayant le plus de « Spam Gangs » actifs sur son territoire[12].

1.1.4 Autres vecteurs de « spam »

Avec les progrès constants dans le domaine des télécommunications, de nouvelles façons de communiquer sont apparues. Le courriel est l'une de celles-ci. Le Messaging Anti-Abuse Working Group (MAAWG) se vante d'être le seul organisme à lutter contre le pollupostage de façon holistique, c'est-à-dire en tenant compte de ses manifestations par le biais de technologies comme la messagerie instantanée, la téléphonie IP et les communications cellulaires.

1.2 Objectifs des polluposteurs

Historiquement, l'activité informatique malicieuse par excellence était la création et diffusion de virus. La motivation des auteurs de ces programmes « vandales » se résumait, généralement, à une démonstration de force plutôt pompeuse. Un façon « d'épater la galerie », autrement dit. L'arrivée d'Internet a bouleversé cet ordre de chose. Plus que jamais, les personnes qui oeuvrent dans l'industrie du pollupostage ont un intérêt économique à poursuivre leurs activités.

1.2.1 Marketing agressif et ventes fallacieuses

a) Principaux produits annoncés

L'emploi « classique» du pourriel a été et demeure la publicité de produits. C'est une méthode peu coûteuse qui peut se révéler rentable même avec un faible taux de réussite. En cela, le pourriel se distingue de la sollicitation faite par téléphone ou courrier traditionnel. Ces types de sollicitation nécessitent un certain investissement et l'embauche d'employés. Le polluposteur est libéré de ces contraintes, ce qui fait qu'il n'y a pratiquement pas de limite financière à l'étendue de son action. La seule limite qui se dresse devant lui se trouve dans les filtres anti-pourriel qu'élaborent les fournisseurs de services d'accès Internet et ceux qu'utilisent les entreprises et les utilisateurs.

Il existe des données statistiques sur les types de produits les plus fréquemment annoncés par pourriel. Ces données semblent cependant ne pas répondre à des exigences minimales de validité scientifique (comme être fondées sur des catégories exclusives et mutuellement exhaustives). La terminologie employée par les firmes de sécurité change au fil des ans, ce qui fait qu'il est difficile d'établir des comparaisons dans le temps. Qui plus est, les résultats diffèrent grandement d'une compagnie à l'autre. Mais les diverses études sur ce sujet s'entendent pour dire que les produits de santé et financiers, les jeux de hasard et la pornographie figurent parmi les matières les plus annoncées.

b) Une éthique douteuse

Peut-on faire confiance aux détaillants qui font connaître leurs produits par le pourriel? La réponse, négative, à cette question paraît évidente pour une proportion croissante d'internautes. Comme il est mentionné un peu plus haut, l'industrie du pollupostage n'a pas su s'auto-discipliner afin de légitimer ses activités. La simple lecture des pourriels suffit souvent à susciter la méfiance :

- « Magic solution to enlarge your penis! »
- « Get Rich Quick! »
- « Get a degree from a prestigious university NOW! »

12 http://www.spamhaus.org/statistics/countries.lasso.

Les pourriels servent souvent à propager de fausses représentations à propos de produits et services dont on ne connaît pas l'origine réelle. Plusieurs prétendues pharmacies en ligne annonçant leurs produits par pourriel sont en réalité de pures fraudes montées par le crime organisé. Dans le domaine du pourriel pharmaceutique, même lorsque le produit est livré, il s'agit plus souvent qu'autrement d'un simple placebo.

Les répercussions de ces pratiques pour le moins trompeuses sont ressenties par les entreprises qui font du marketing légitime. Le pourriel détruit la crédibilité du médium : le public en vient à ne plus croire à l'ensemble des messages y compris ceux qui proviennent d'entreprises honnêtes se conformant à la loi.

1.2.2 Hameçonnage

a) Définition

L'hameçonnage est une sorte d'attaque informatique qui consiste à leurrer une personne afin de lui faire croire qu'elle se trouve sur le site Web d'une institution de confiance afin de lui subtiliser des informations confidentielles permettant la fraude et le vol d'identité.

b) Techniques traditionnellement employées

Pour obtenir le numéro de carte de crédit, d'assurance sociale ou de folio bancaire de sa proie, le fraudeur doit utiliser des moyens qui relèvent à la fois de « l'ingénierie sociale et technique ». Cette expression, consacrée dans le domaine, veut dire que la réussite de la fraude dépend non seulement des habiletés informatiques de son auteur, mais tout aussi de sa faculté à amener sa victime à lui faire confiance.

Sans conteste, le moyen qui a été le plus utilisé pour faire en sorte que la victime « morde à l'hameçon » a été de suivre la recette suivante :

1° La mystification

Le polluposteur-fraudeur envoie un courriel dont le champ « De : » a été falsifié à plusieurs milliers d'adresses. La personne qui le reçoit a donc l'impression qu'il émane de son institution financière ou d'un autre organisme digne de confiance (ex. service@desjardins.com). Ce maquillage d'adresse est très facile à réaliser, étant donné que le protocole SMTP est par définition insécuritaire.

Pour ajouter de la crédibilité à son envoi, le polluposteur-fraudeur pourra prendre soin d'inclure dans son courriel tous les éléments visuels de l'image corporative de l'institution (logo, police de caractère, noms de produits, etc.).

2° L'attrape

Le polluposteur-fraudeur trouve un stratagème qui va amener sa cible à lui dévoiler des informations confidentielles. Pour ce faire, il prétextera une « mise à jour des comptes », fera miroiter une « assurance anti-fraude », signalera qu'une « opération irrégulière » a été notée au dossier ou demandera des informations pour livrer un bien remporté lors d'un concours.

La victime est avisée de « Cliquer sur ce lien » pour visiter la page Web de l'institution financière. En réalité, le lien est construit de manière à cacher que l'adresse réelle du site n'est pas, par exemple, http://www.desjardins.com, mais bien, toujours à titre d'exemple, http://123.65.125.02.

Cette attrape exploite le fait qu'une personne préfère, paresse aidant, cliquer sur un lien plutôt qu'entrer elle-même l'adresse d'un site Web.

3° Un message réconfortant

Pour éviter que l'opération illicite soit rapidement détectée par les autorités, la victime, après avoir communiqué ses informations confidentielles, est remerciée et assurée que « l'opération s'est faite avec succès » ou que « le compte a été mis à jour » ou même — non sans une dose d'ironie! — que « la protection anti-fraude est maintenant activée ».

On constate dès lors que le pourriel joue un rôle essentiel dans le processus de fraude. C'est lui qui, à la base, transmet à la victime le lien vers le site Web malicieux. À l'instar du spécialiste en marketing « agressif », le polluposteur-fraudeur n'a pas besoin d'un taux de réussite élevé pour rentabiliser l'opération, compte tenu de son faible coût et de la masse de personnes qu'elle peut joindre.

c) Hameçonnage 2.0

Évidemment, les groupes de consommateurs, les gouvernements ainsi que les institutions financières ont réagi à ces attaques en éduquant les usagers, en leur assurant que leur institution n'entrerait pas en contact avec eux par courrier électronique. Même s'il reste encore beaucoup de personnes qui peuvent croire ces courriels, les gens sont de plus en plus méfiants et comprennent qu'il vaut mieux tout simplement supprimer ces pourriels frauduleux.

Les firmes spécialisées en sécurité informatique s'attendent à ce que la réplique des fraudeurs face à ces nouveaux défis soit de réduire la part d'ingénierie sociale dans leurs attaques. Bref, de limiter au minimum leur dépendance envers la crédulité de l'utilisateur.

Pour atteindre cet objectif, plusieurs possibilités s'offrent aux hameçonneurs[13].

1° Falsification de la barre d'adresse URL

Anciennement, il était facile d'identifier un faux site Web d'institution financière, car son adresse URL correspondait à une adresse IP plutôt qu'à son nom de domaine (par exemple, http://129.23.53.232 au lieu de http://www.desjardins.com). Bien que les fraudeurs pouvaient maquiller le lien indiqué dans leurs courriels, il reste qu'ils demeuraient incapables de modifier l'adresse URL affichée dans la barre réservée à cet effet par le navigateur Web. Avec le temps, ils ont réussi à abuser de bogues de sécurité du navigateur (p. ex. JavaScript) afin de trafiquer cette adresse.

2° Attaques de type « pharming »

Une attaque de type «pharming» est particulièrement vicieuse, car l'utilisateur de compétence moyenne — ou même avancée — ne peut s'en prémunir. Son but est de rediriger le trafic d'un site Web légitime vers le site du fraudeur de façon complètement invisible pour l'utilisateur. La technique généralement employée fait encore appel à une vulnérabilité du navigateur Web pour exécuter sur le poste de la victime un micro-programme qui modifie le fichier *Hosts* afin d'obliger le système d'exploitation à rediriger les requêtes s'adressant à un nom de domaine légitime (desjardins.com) vers l'adresse IP du serveur Web du fraudeur. Plusieurs firmes de sécurité notent que les routers sans-fil mal configurés (dont le nombre est en croissance, d'ailleurs) pourraient constituer une cible de choix pour les fraudeurs. Il faut néanmoins se garder de sombrer dans l'alarmisme étant donné que l'expérience montre que — pour l'instant du moins — ces attaques demeurent très rares.

13 Sur ces différentes tactiques, voir « Pêcheurs de compte (bancaires) », *Le Monde*, jeudi 22 mars 2007, pp. 24-25.

3° « Spy-phishing »

Jusqu'à maintenant, la méthode d'hameçonnage « classique» se limitait à l'envoi d'un courriel demandant à la victime de mettre à jour son dossier chez son institution financière en cliquant sur un lien. Celle-ci a l'illusion qu'elle est sur la page Web de son institution, alors, qu'en vérité, elle se trouve le site du fraudeur. Sans le savoir, elle lui communique ses informations bancaires.

Comme les autorités policières peuvent facilement retracer et fermer un site Web, ce genre de supercherie a une durée de vie limitée à quelques jours (d'autant plus que le courriel est envoyé à des milliers de personnes à la fois).

Les spécialistes en sécurité Informatique craignent que les logiciels espions soient de plus en plus utilisés par le crime organisé pour faciliter la cueillette d'informations bancaires et autres renseignements permettant la fraude et le vol d'identité. Le logiciel espion, agissant comme enregistreur de frappe, peut transmettre invisiblement à son développeur le nom d'usager, mot de passe ou numéro d'assurance sociale d'un utilisateur lorsqu'il détecte que celui-ci visite le site Web d'une institution financière ou gouvernementale. Aucune intervention de la personne ciblée n'est requise. Il peut s'écouler plusieurs semaines ou mois avant que la victime se rende compte que la sécurité de son ordinateur est compromise. L'attaque est donc beaucoup plus durable dans le temps qu'une attaque « classique » d'hameçonnage, car elle n'exige pas la création d'un lien vers un serveur Web public. Quoiqu'elle a crû de 234 % entre les années 2005 et 2006[14], il faut admettre que cette méthode de fraude reste marginale. Pour l'instant, la majorité des logiciels espions demeurent employés à des fins de marketing « agressif ».

d) La criminalisation du pollupostage

1° En croissance depuis 2004

Tous les analystes s'entendent pour dire que le pollupostage est un champ d'activité qui se criminalise de plus en plus. Jadis surtout utilisé par des spécialistes du « marketing agressif », le pourriel est désormais l'affaire de groupes organisés impliqués dans d'autres sphères de criminalité. Selon la firme CommTouch[15], le crime organisé serait responsable d'environ 80 % du pourriel qui atteint nos boîtes à lettre électroniques. La hausse spectaculaire de l'hameçonnage depuis l'été 2004 n'est pas étrangère à ce phénomène.

2° Un réseau de criminels

Tout comme les réseaux de distribution de drogue, les groupes criminels qui sont impliqués dans des activités d'hameçonnage sont structurés et chaque complice a un rôle qui lui est propre. Voyons cela de plus près :

— ***Le polluposteur*** — Son rôle est de collecter des adresses courriels afin de monter une banque de victimes potentielles et de leur envoyer un courrier électronique les incitant à se rendre sur le site Web de l'organisation.

— ***Le pirate*** — C'est le crack en informatique du groupe. Il est responsable de dénicher un serveur Web vulnérable. Une fois piraté, le serveur héberge le faux site d'une institution financière. Le tout se fait sans le consentement de l'administrateur du serveur exploité. Le pirate est également responsable de programmer ou de créer de nouvelles variantes de « bots » pour envoyer le pourriel (cet aspect est traité plus loin dans ce document).

---

14 « Spy-phishing – A new breed of blended threats », http://www.trendmicro.com/en/security/white-papers/overview.htm.

15 Oren DRORI, « Commercial and non-commercial approaches to fighting SPAM », *Virus Bulletin Conference October 2005*, http://www.commtouch.com/downloads/VB2005_Approaches_To_Fighting_Spam.pdf.

— *Le* ***« carder »*** — C'est le dernier maillon de la chaîne. Il achète les services du pirate et du polluposteur. On le nomme « carder », car il appose les informations personnelles dérobées sur une carte de crédit vierge afin d'effectuer le vol de fonds comme tel.

3° Le « stock spam »

Le « stock spam » représente un autre usage frauduleux du pourriel. Pour ses instigateurs, le but est de faire fluctuer le prix de certaines valeurs mobilières échangées sur un marché de gré à gré américain (*Pink Sheets* ou *OTC Bulletin Board*). La stratégie la plus souvent employée est celle du « pump and dump ». Pour ce faire, les fraudeurs achètent des actions d'une compagnie dont le prix est dérisoirement bas. Ils envoient ensuite massivement des courriels alertant ceux qui les lisent que la compagnie :

- A fait une découverte tout à fait révolutionnaire
- Est sur le point d'être achetée
- Va bientôt signer une entente avec une multinationale
- Etc.

La compagnie ne possède bien sûr aucune valeur réelle. Parfois, il s'agit d'un pur éléphant blanc créé exclusivement pour l'opération. Les polluposteurs-spéculateurs profitent de la demande suscitée par l'envoi des pourriels pour vendre en bloc leurs actions à un prix anormalement élevé. Très vite, l'astuce est découverte et la valeur des actions de la compagnie fond comme neige au soleil.

1.3 Stratégies employées

1.3.1 La cueillette d'adresses

Les polluposteurs ont besoin d'adresses courriels comme nous avons besoin d'air pour respirer. Pas d'adresses, pas de pourriels. La chose est simple à ce point.

a) Vente d'informations personnelles sans le consentement de l'intéressé

Pour collecter des adresses, les polluposteurs ont traditionnellement fait appel à des webmestres désirant faire un peu d'argent. Il y avait donc un marché noir de liste d'adresses courriels. Maintenant que le pourriel est une chose de moins en moins acceptée, la plupart des propriétaires de sites Web ont adopté des politiques concernant la protection des renseignements personnels qui interdisent strictement la revente à un tiers des adresses courriels recueillies.

b) Sondages, concours et consentement « boiteux»

Une technique toujours populaire se résume à organiser des concours, tirages, etc. qui exigent — comme condition de participation — une adresse courriel et l'autorisation d'y envoyer du pourriel. Le problème est que, trop souvent, les termes du contrat ne sont pas correctement explicités. Le consentement du participant peut donc qu'être qualifié de boiteux, tout au mieux.

c) Balayage du Web, de forums de discussion et de la base de données WHOIS

Les deux méthodes que nous venons de mentionner sont essentiellement utilisées par les polluposteurs qui œuvrent en tant que spécialistes du marketing. Comme ce type de pourriel est en déclin, une nouvelle façon de cueillir gratuitement des adresses est apparue avec le temps. La méthode consiste à créer un programme qui explore automatiquement le Web à la recherche d'adresses courriel. Les entreprises sont particulièrement affectées par cette méthode de cueillette, car elles indiquent leurs coordonnées au

moyen d'une page « Nous contacter ». Les personnes qui participent à des forums de discussion (USENET, Google Groups) sont aussi très touchées. Publiquement accessibles, les registres WHOIS[16] et DNS constituent aussi une source de choix, puisque les propriétaires de sites Web doivent y inscrire une adresse courriel valide afin de communiquer avec l'autorité qui gère leur nom de domaine.

d) Les attaques par dictionnaire et la validation des adresses

Les polluposteurs disposent de techniques afin de confirmer qu'une adresse courriel est valide et fonctionnelle. Souvent, les polluposteurs ont recours à des attaques par dictionnaire (« *Dictionary Harvest Attacks* ») afin de produire des listes d'adresses courriel. Lors d'une telle opération, le polluposteur utilise un programme qui génère toutes les combinaisons possibles de caractères fréquemment employés dans les adresses courriel par rapport à un nom de domaine. L'attaque se fonde sur l'idée qu'il y a, par exemple, de fortes chances que l'adresse john.smith@microsoft.com existe réellement. Si le message envoyé ne « rebondit » pas, l'adresse est considérée valide.

Une autre méthode consiste à insérer une image dans le texte du pourriel. Le nom de l'image est déterminé par un code qui identifie l'adresse de la personne qui reçoit celle-ci. Lorsqu'elle se charge, l'image transmet ainsi une preuve au polluposteur que le pourriel a bel et bien été reçu et qu'il peut continuer à envoyer des messages à cette adresse. Pour cette raison, plusieurs logiciels de courrier électronique désactivent par défaut l'affichage des images.

1.3.2 L'expédition des messages

Au fil des années, l'industrie a mis en place diverses initiatives à l'égard du contrôle du courriel non sollicité. Par l'emploi de diverses techniques, celle-ci a réussi à compliquer considérablement le travail des polluposteurs. Sans compter que plusieurs pays ont adopté des lois sévères interdisant le pourriel. De sorte qu'il est désormais nécessaire que les polluposteurs fassent appel à une méthode d'expédition qui 1) a un faible coût, 2) est anonyme et 3) s'appuie sur un réseau qui n'est pas sur une « liste noire ».

a) Fournisseurs « Bulk-friendly »

L'immense majorité des fournisseurs d'accès Internet interdisent strictement à leurs clients d'utiliser leur compte pour expédier du pourriel. C'est une obligation prévue par le contrat entre le fournisseur et le client. Mais un certain nombre d'entreprises offrent des services qualifiés de « bulk-friendly » ou de « bulletproof ». Ces entreprises signent avec les polluposteurs ce que l'on nomme un « contrat rose » leur permettant d'envoyer autant de pourriel qu'ils le désirent. Il est à noter toutefois que les prétentions de ces compagnies sont parfois trompeuses : beaucoup de serveurs courriel sont configurés pour refuser automatiquement tout message qui émane d'un de ces fournisseurs soi-disant « bulletproof ». En outre, ces entreprises font généralement partie d'un plus grand réseau qui interdit à ses revendeurs de proposer de tels services. Pour ces raisons, le recours à un fournisseur « bulk-friendly » est de moins en moins attrayant aux yeux des polluposteurs.

De leur point de vue, la solution réside dans le fait d'utiliser le réseau d'un tiers pour que leurs pourriels se confondent avec des messages légitimes.

16 WHOIS (mot formé par la contraction de l'expression *who is ?*, signifiant littéralement *qui est ?*) désigne un service de recherche fourni par les registres de noms de domaine permettant d'obtenir des informations sur une adresse IP ou sur un nom de domaine.

b) Accès à un serveur SMTP d'une entreprise

1° Relais ouverts

À ses débuts, Internet était un réseau surtout utilisé par les universités et les institutions gouvernementales. Il apparaissait donc normal de présumer la bonne foi des personnes qui s'y connectent. C'est pourquoi l'insécurité du protocole SMTP reflète la façon dont il a été conçu à l'origine.

Au début des années 1990, l'envoi des courriers électroniques se faisait à l'aide de serveurs intermédiaires (les relais SMTP). Au lieu d'envoyer le courriel directement au fournisseur d'accès Internet de celui à qui il est destiné, on jugeait qu'il était préférable qu'il soit relayé de serveurs en serveurs jusqu'à sa destination. Cette méthode d'expédition s'apparente à une sorte de course à relais électronique.

La pratique dominante, à cette époque, était de permettre à toute personne qui le souhaite de transférer ses courriels à l'aide du relais. Pour cette raison, on dit que ces serveurs sont « ouverts ». Il va sans dire que les polluposteurs ont su exploiter rapidement cette faille et utiliser à leur profit les relais SMTP ouverts. L'avantage pour le polluposteur est le suivant : en demandant au relais ouvert d'acheminer le courriel à sa place, l'identité du polluposteur est substituée par celle du relais ouvert. Il devient donc très difficile de le retracer.

Aujourd'hui, les courriels sont expédiés directement à leur destinataire, sans autre intermédiaire. Les relais SMTP ouverts ont pratiquement tous disparus. Ceux qui restent sont, règle générale, incapables d'expédier du courriel, étant inscrits sur une « liste noire » d'adresses IP à bloquer (tout comme bien des fournisseurs « bulk-friendly »).

2° Proxys ouverts et autres portes d'entrée

Les administrateurs de réseaux ont vite compris qu'aujourd'hui, l'Internet ne repose plus sur la confiance mutuelle. C'est pourquoi les relais ouverts ont été fermés. Toute personne qui se branche à un serveur SMTP pour transmettre un courriel doit désormais démontrer qu'elle fait partie du même réseau que celui-ci (à l'aide de son adresse IP). Si la connexion provient de l'extérieur, elle sera refusée.

Les polluposteurs, pour utiliser les ressources d'une entreprise, doivent donc faire croire au serveur SMTP que leur requête provient de l'intérieur du réseau. Pour ce faire, ceux-ci ont beaucoup utilisé dans le passé des serveurs proxys ouverts ou malhabilement configurés. La vigilance des administrateurs réseau étant maintenant plus grande, un proxy ouvert est plutôt hors du commun. Néanmoins, il demeure toujours possible qu'un polluposteur réussisse à dénicher une autre faille de sécurité lui permettant de prétendre faire partie du réseau interne de l'entreprise.

c) Comptes courriels gratuits

Les comptes courriel du genre *Hotmail* jouissent d'une grande popularité. Ils sont gratuits, fiables et peuvent être créés dans le plus complet anonymat. Étant donné leur nombre élevé d'utilisateurs, aucun fournisseur ne pourrait se permettre de les bloquer. Toutes ces caractéristiques constituent des avantages indéniables pour les polluposteurs. C'est pourquoi, dans les années 90, ceux-ci en ont abondamment fait usage. Les fournisseurs ont répondu à ces abus en développant des programmes qui détectent l'expédition de pourriel sur leur réseau. Une fois l'abus détecté, le compte est immédiatement fermé. Qu'à cela ne tienne, les polluposteurs ont développé des « scripts » ayant pour fonction de créer automatiquement des comptes « jetables ». Afin d'enrayer cette pratique, les fournisseurs demandent à l'utilisateur, lors de l'inscription, de valider le formulaire en entrant un code inscrit sur une image.

Fig. 3 — Exemple de CAPTCHA utilisée par Hotmail

Comme on le voit, les caractères sont si difficiles à lire qu'un logiciel de reconnaissance optique de caractères (OCR) ne peut arriver à interpréter l'image. Dans le domaine, c'est ce que l'on appelle une CAPTCHA (pour « Completely Automated Public Turing test to Tell Computers and Humans Apart »).

Les polluposteurs savent toutefois redoubler d'audace et d'ingéniosité lorsque vient le temps de contourner ce type de barrière. Le subterfuge se résume ainsi :

1. Un internaute visite une page qui offre de la pornographie gratuitement.
2. À cet instant, le script du polluposteur remplit un formulaire d'ouverture de compte courriel gratuit.
3. Lorsque l'internaute clique sur un lien du style « Voir les images pour adultes », on lui demande d'interpréter la CAPTCHA (importée automatiquement depuis le formulaire d'abonnement).
4. L'internaute interprète la CAPTCHA et obtient en retour la pornographie promise.
5. Le script entre dans le formulaire les caractères inscrits par l'internaute et le soumet afin de créer le compte courriel.

Si cette astuce fait sourire, il reste qu'elle montre bien en quoi aucune technologie ne résiste longtemps à la créativité des polluposteurs. Toutefois, comme un expert le remarque, l'emploi d'une CAPTCHA demeure utile :

> *Avant le recours aux Captcha, ces trucs permettaient d'ouvrir un million de comptes hotmail par jour, mais maintenant, s'ils attirent 10,000 personnes sur le site de porno gratuite, ils peuvent configurer 10,000 comptes. C'est beaucoup, mais d'un ordre de grandeur moindre.*[Nous traduisons] [17]

Pour les polluposteurs, le recours aux comptes courriel gratuits demeure donc possible, bien que moins intéressant qu'auparavant.

17 "*Before the Captcha those bots could open a million Hotmail accounts a day, but now, if they can attract 10,000 people to their free porn site, they can set up 10,000 accounts, which is a lot, but still an order of magnitude less" ;* http://news.zdnet.co.uk/security/0,1000000189,39153933,00.htm.

d) Les réseaux de zombies (« botnets »)

En janvier 2004, le fondateur de Microsoft, Bill Gates, prédisait que le problème du pourriel sera résolu d'ici deux ans[18]. Évidemment, M. Gates s'est trompé. À cette époque, l'affirmation n'était pourtant pas dépourvue de sens.

Après tout, les administrateurs réseau préviennent de mieux en mieux l'abus de leur infrastructure par les polluposteurs. De plus, l'immense majorité des relais ou proxys ouverts ont été soit fermés soit bannis par les autres fournisseurs d'accès Internet. Comme nous venons de le voir, les CAPTCHAs rendent le recours aux comptes du type *Hotmail* moins aisé qu'il y a quelques années. Quant aux filtres anti-pourriel, ils sont de plus en plus performants.

Mais la lutte au pourriel est un incessant jeu de chat et de souris. Comme les polluposteurs tirent un bénéfice économique de leurs activités, ils savent redoubler d'imagination pour développer de nouvelles méthodes d'expédition. Ceux-ci ont bien compris que le maillon faible d'un réseau informatique, côté sécurité, c'est le poste personnel de l'utilisateur. Leur dernière trouvaille : les réseaux de zombies (ou « botnets », en anglais).

Un réseau de zombies regroupe un nombre important d'ordinateurs infectés par un logiciel malveillant (les « zombies ») qui permet à un tiers d'en prendre le contrôle à distance. L'infection se propage rapidement, car un ordinateur infecté cherchera automatiquement d'autres cibles vulnérables. La taille des réseaux de zombies est variable. Parfois, elle est spectaculaire : en 2005, la police danoise a arrêté un individu qui contrôlait un réseau d'environ 1 500 000 ordinateurs[19]. Plusieurs semaines peuvent s'écouler avant qu'une personne soit informée de la présence d'un « bot » sur son PC.

Les réseaux de zombies sont utilisés pour expédier du pourriel, pratiquer l'extorsion (par le biais d'attaques de déni de service distribuées) ou subtiliser des renseignements personnels. Pour les polluposteurs, c'est le véhicule idéal. Selon plusieurs estimations, environ 80 % du pourriel est expédié par le biais de réseaux de zombies[20].

Lorsqu'un pourriel provient d'un ordinateur « zombie », on ne peut retracer le véritable polluposteur, mais uniquement la victime de l'infection. En outre, les fournisseurs d'accès Internet ne peuvent bannir ces machines de leur réseau sans risquer de bloquer tout le courriel de l'ensemble des clients du fournisseur du poste infecté (étant donné l'assignation dynamique des adresses IP). La popularité des forfaits Internet haute-vitesse offre aux réseaux de zombies une grande capacité de bande passante, facilement disponible et presque gratuite.

Pour ces raisons, les réseaux de zombies sont d'une grande valeur aux yeux du crime organisé : il s'agit d'un bien qui s'achète et se vend. Pour les fabricants de produits de sécurité, les « botnets » changent la donne. Jadis, les virus étaient créés pour épater la galerie, faire une démonstration de force… Or, ce n'est plus le cas.

Le cas SpamThru

SpamThru est sans nul doute un des « bots » les plus avancés qui soient. Plusieurs variants de ce virus se propagent sur Internet et sont responsables d'une grande quantité de pourriels.

SpamThru a la particularité d'être capable de continuer à opérer même si le serveur qui le contrôle a été fermé. En effet, SpamThru interrogera d'autres machines infectées qui sont à sa portée afin de savoir quelle est la nouvelle adresse IP du serveur auquel il doit se rapporter.

Ce qui est encore plus innovateur, c'est que SpamThru télécharge une copie illégale de l'anti-virus Kaspersky afin d'éradiquer tout programme malveillant qui lui fait concurrence. La copie de Kaspersky qu'il télécharge a bien sûr été modifiée pour éviter que SpamThru soit détecté.

Source : *MessageLabs 2006 Annual Security Report*. http://www.messagelabs.com/portal/server.pt/gateway/PTARGS_0_0_406_789_-789_43/http%3B/0120-0176-CTC1%3B8080/publishedcontent/publish/threat_watch_dotcom_en/intelligence_reports/2006_annual_security_report/2006_annual_security_report_5.pdf.

18 http://www.cbsnews.com/stories/2004/01/24/tech/printable595595.shtml.

19 http://www.techweb.com/wire/security/172303160

20 *MessageLabs 2006 Annual Security Report*, http://www.messagelabs.com/Threat_Watch.

Aujourd'hui, la plupart des virus ne cherchent pas à endommager les ordinateurs qu'ils infectent, mais à les transformer en machines à émettre du pourriel.

La plupart des « bots » sont contrôlés à distance à l'aide du protocole IRC. Toutefois, les réseaux de zombies de seconde génération font appel au protocole HTTP afin de faire échec à de nouvelles stratégies de filtrage de la part des administrateurs réseau. Comme le protocole HTTP est à la base du Web, on ne peut le bloquer diamétralement.

Certains analystes vont même jusqu'à se demander si la bataille contre le pourriel est définitivement perdue, étant donné qu'il y aura toujours sur Internet un bassin important d'ordinateurs personnels vulnérables[21] (les pays en voie de développement, qui utilisent des systèmes d'exploitation désuets, constitueraient une cible particulièrement intéressante) et que la sophistication des « bots » s'améliore à un rythme incroyable (voir l'encadré 1 sur le virus *SpamThru*).

1.3.3 Le contournement des filtres anti-pourriel

Avec les réseaux de zombies, les polluposteurs disposent d'une méthode d'expédition quasi infaillible. Il leur reste toutefois à s'assurer que leurs courriels passent à travers les filtres anti-pourriel des fournisseurs d'accès Internet et des grandes entreprises.

a) Varier l'écriture des mots associés au pourriel

La première stratégie à avoir été employée par les polluposteurs fut de modifier l'orthographe des mots qui permettent au filtre de qualifier le courrier électronique de pourriel. C'est pour cela que bien des pourriels sont écrits dans un langage intelligible pour un humain, mais incompréhensible pour une machine. Par exemple, le mot Viagra peut être orthographié Vi@gra, V1agra, Via-gra, etc.

Cette méthode a ses limites. Aujourd'hui, les filtres anti-pourriel sont suffisamment développés pour identifier toutes les variations dans lesquelles un mot peut être écrit.

b) Remplacer le texte par une image

La possibilité d'ajouter du code HTML à un courriel fait en sorte qu'un polluposteur peut inscrire le texte de son pourriel dans une image, ce qui met en échec les filtres anti-pourriel primitifs.

Il va de soi que les firmes qui conçoivent ces filtres ont rapidement réagi en intégrant à leurs filtres un module de reconnaissance optique des caractères (*OCR*, en anglais). De cette façon, le filtre « lit » les mots contenus dans l'image du pourriel.

On se souviendra que les fournisseurs de comptes courriel gratuits font appel à des images très difficiles à lire afin d'éviter que les polluposteurs fassent appel à des technologies OCR. Ceux-ci ont bien compris l'astuce et l'utilisent désormais à leur propre compte afin de contourner les filtres, comme le montre cette image :

21 http://www.eweek.com/print_article2/0,1217,a=191391,00.asp.

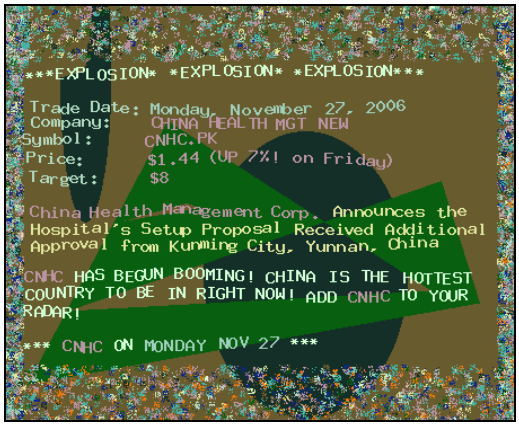

Fig. 4 — Exemple d'image complexe employée dans un pourriel

On remarque immédiatement que le texte est 1) entouré de formes géométriques, 2) incorrectement aligné, 3) affiché en plusieurs couleurs et 4) encadré de motifs étranges. Toute cette mise en scène sert à faire croire au filtre anti-pourriel qu'il s'agit d'une photo, et non d'un texte. Il est très délicat de bloquer une image de ce type sans bloquer de véritables et légitimes courriels. Pour les développeurs de filtres, il s'agit d'un défi majeur.

1.4 Conséquences

L'époque où le pourriel se limitait à de simples publicités non sollicitées est désormais révolue. Comme nous l'avons vu, le crime organisé est aujourd'hui très actif dans ce domaine. Fraude, vol d'identité et piratage informatique sont de l'ordre du commun pour les personnes actives dans cette sphère. Si les opérations de ces groupes peuvent sembler « virtuelles », les dommages qu'elles entraînent sont malheureusement bien réels.

À l'échelle mondiale, la firme Ferris Research a estimé à près de 50 milliards les pertes économiques découlant du pourriel en 2005 (en dollars US) [22]. Au Canada seulement, les pertes causées par le courriel seraient d'environ 1,5 milliards. Sont comptabilisées dans ce montant, les pertes de productivité causées par le temps requis pour supprimer ces messages et les coûts qu'engendre leur filtrage.

- Infrastructure informatique

Le volume croissant de pourriel exerce une pression énorme sur les réseaux informatiques des grandes entreprises et des fournisseurs d'accès Internet. Cela les force à constamment renouveler leurs équipements pour faire face à cette augmentation du trafic courriel et à disposer des meilleurs filtres anti-pourriel.

De même, le pourriel engage d'importantes dépenses en matière de sécurité informatique. Désormais, les entreprises ne peuvent plus se permettre la moindre brèche dans leur infrastructure. L'incessant jeu du chat et de la souris entre les polluposteurs et les administrateurs requiert d'importantes ressources humaines et techniques ainsi que de constantes reconfiguration. À titre d'exemple, l'utilisation croissante d'images pour contenir le texte du pourriel (afin d'éviter les filtres) augmente considérablement la bande passante consommée par les serveurs SMTP (étant donné qu'une image est beaucoup plus lourde que du texte).

22 Ferris Research, *The Global Economic Impact of Spam 2005*.

- Pertes découlant de l'hameçonnage

Pour l'année 2006, la firme Gartner avance que l'hameçonnage a coûté à l'économie américaine 2,8 milliards (en dollars US)[23]. En moyenne chaque victime a perdu 1 244 $, une très forte hausse par rapport à la moyenne de 2005 (257 $). La firme de recherche observe que les attaques envers eBay et Paypal demeurent plus efficaces et lucratives que celles visant les banques traditionnelles.

Malheureusement, nous n'avons pu trouver de statistiques concernant le Canada ou le Québec. Il est à noter cependant que les attaques de hameçonnage visent maintenant les institutions financières québécoises et sont rédigées dans un français très crédible bien que parfois approximatif.

- Rupture du lien de confiance

La conséquence du pourriel la plus difficile à chiffrer demeure la perte de confiance qu'il engendre dans l'esprit des internautes à l'endroit du courrier électronique et de la cyberéconomie en général. Aux États-Unis, Gartner a estimé que près de 2 milliards de dollars ont été ainsi perdus en raison de la peur des consommateurs envers le commerce en ligne. Plusieurs personnes hésitent encore à faire des affaires en ligne, compte tenu du nombre de fraudes et du caractère apparemment incontrôlé de la cyberéconomie.

2. Les logiciels espions

Les logiciels espions participent à diverses malversations pouvant être commises sur Internet. Dans cette partie, on définit les notions et fait état des principales fonctions et méfaits auxquels ils peuvent donner lieu.

2.1 Définition

Un logiciel espion est un programme informatique qui accumule, dans le but de les transmettre à des tiers, des informations sur l'utilisateur d'un ordinateur, et ce, sans avoir obtenu au préalable son véritable consentement. Il s'agit d'un type particulier dans la famille des logiciels malveillants qu'il ne faut pas confondre avec d'autres genres de programmes indésirables, comme les virus, vers et chevaux de Troie. Un logiciel espion est généralement employé pour effectuer du cybermarketing « agressif» et — dans de plus rares cas — prendre possession de renseignements personnels pour réaliser des activités illicites.

Dès lors, il n'est pas étonnant qu'une caractéristique fréquemment rencontrée d'un logiciel espion soit sa capacité à masquer son installation et à faire échec à toute tentative de désinstallation par une personne qui n'est pas spécialisée dans le domaine. Comme nous le verrons plus loin, les logiciels espions sont responsables d'un grand nombre de pannes et désagréments liés à l'usage de l'ordinateur, et ce, tant dans les entreprises que dans les foyers. Pour cette raison, leur prolifération préoccupe un nombre croissant d'internautes.

2.2 Principales fonctions

Bien que les fonctionnalités des logiciels soient variées, elles ont en commun l'emploi d'un ordinateur à des fins non véritablement consenties par son utilisateur. Les lignes qui suivent en présentent trois des plus fondamentales[24].

---

23 http://www.gartner.com/it/page.jsp?id=498245.

24 Pour un portrait complet, on peut consulter le tableau préparé par l'Anti-Spyware Coalition, http://www.antispywarecoalition.org/documents/documents/ASCDefinitionsWorkingReport20060622.pdf.

2.2.1 Profilage marketing

La majorité des logiciels espions sont développés par des firmes de cybermarketing afin de déterminer les habitudes de consommation et les préférences de navigation des internautes. De façon complètement invisible, ils transmettent systématiquement ces informations à un serveur appartenant à leur développeur. Ainsi, celui-ci pourra vendre à des entreprises les profils de consommateurs qu'il a collectés ou bien s'en servir pour optimiser son propre programme de publicité ciblée. C'est donc en ce sens que les logiciels espions constituent un risque pour le droit à la vie privée.

2.2.2 Publicité ciblée

Rares sont les logiciels espions qui se contentent d'uniquement dresser des profils de consommateurs. En fait, la collecte de ces renseignements a souvent pour but la diffusion, à des moments stratégiques, de publicités ciblées au sein même de l'environnement graphique de l'utilisateur. La méthode la plus couramment employée est de programmer dans le logiciel espion une fonction qui génère des fenêtres publicitaires très encombrantes. Si, à titre d'exemple, un logiciel espion détecte que l'utilisateur s'informe sur des produits de santé et qu'il a dernièrement fréquenté des sites pornographiques, il pourrait faire apparaître une publicité d'un détaillant en ligne de Viagra.

Il va sans dire que l'exposition répétée à cette forme de publicité donne une impression d'envahissement, d'autant plus qu'il arrive assez fréquemment qu'un même ordinateur soit infecté par plusieurs logiciels espions qui se chevauchent. Ces messages intempestifs constituent, pour la plupart des gens, l'indicateur le plus apparent de la présence de logiciels espions sur leur ordinateur et la principale raison pour laquelle ils sont considérés comme étant un véritable fléau.

2.2.3 Détournement de trafic

Un autre moyen employé par ces firmes pour imposer leur publicité est de détourner le trafic d'un site Web légitime et populaire vers celui d'un annonceur. Ainsi, bon nombre de logiciels espions modifient à l'insu de l'usager la page d'accueil, les favoris et le moteur de recherche préféré de son navigateur Web. De sorte qu'une personne croyant faire, par exemple, une recherche sur Google sera redirigée automatiquement vers un faux moteur de recherche ne présentant que des liens commerciaux.

2.3 Moyens de propagation

Sauf exception, les logiciels espions ne sont pas répandus sur Internet par leurs propres développeurs. Les firmes de cybermarketing préfèrent plutôt conclure des ententes avec des personnes qui sont en position de joindre un grand public. En contrepartie, elles acceptent de rémunérer ces partenaires en fonction du nombre d'installations, de fenêtres de publicité ou de transactions commerciales que leur participation engendre.

2.3.1 Téléchargement de logiciels « contaminés »

a) Gratuiciel commandité

Lorsqu'un logiciel gratuit atteint un certain degré de popularité, il peut être tentant pour son auteur d'y inclure un ou plusieurs logiciels espions afin de financer son développement. Au début des années 2000, il est arrivé que des développeurs respectés en distribuent avec leurs programmes[25]. Il faut comprendre, qu'à cette époque, les effets néfastes des logiciels espions étaient peu connus et que leur inclusion ne suscitait aucun tollé.

25 "GetRight Ad History", *HeadLight software*, http://www.getright.com/ad_history.html.

Avec le temps, les internautes sont devenus plus sensibilisés à ce phénomène et ont graduellement commencé à exiger des programmes exempts de tout logiciel espion. En fait, ce n'est qu'en juin 2000 que le premier programme anti-logiciel espions est apparu[26]. En avril 2005, Download.com, le plus populaire répertoire de logiciels à télécharger au monde, annonce qu'il adopte une politique de tolérance zéro envers les logiciels espions[27].

b) Logiciel-appât

Il est désormais très rare qu'un développeur de gratuiciel annexe à son produit un logiciel espion, car cela nuit énormément à son image et est de moins en moins toléré. Qu'à cela ne tienne, les firmes de cybermarketing ont ajusté leur stratégie à cette réalité et trouvé de nouveaux partenaires. Ces nouveaux distributeurs de logiciels espions n'ont aucune réputation à sauvegarder et se spécialisent dans le développement de petits programmes peu complexes et sans réelle utilité. Autrement dit, le programme constitue une sorte d'appât qui, une fois téléchargé, installe de façon invisible des logiciels espions pour le compte de la firme de cybermarketing auquel il est associé.

Parmi ces programmes, on trouve typiquement des économiseurs d'écran, de prétendus «accélérateurs d'Internet », des collections d'« émotiocônes» (pour la messagerie instantanée) et de fausses barres d'aide à la navigation. Un phénomène particulièrement inquiétant est l'apparition de logiciels espions déguisés en anti-logiciel espion[28]. La malhonnêteté de l'attrape est déconcertante: un site Web complice fait apparaître une fenêtre informant l'utilisateur qu'il est victime d'« une infection grave de logiciel espion» et lui suggère de télécharger gratuitement un programme pour l'éradiquer. D'un point visuel, le logiciel a toutes les apparences d'un véritable produit de sécurité informatique, mais, dans les faits, il n'est aucunement efficace. Sa véritable fonction est plutôt d'installer en arrière-plan de nouveaux logiciels espions et d'encombrer l'interface graphique de publicités et de fausses alertes de sécurité.

2.3.2 Sites Web malveillants

Les propriétaires de sites Web sont également d'importants partenaires des développeurs de logiciels espions. En exploitant un bogue de sécurité du navigateur, ils peuvent réussir à en installer dans un ordinateur sans que l'utilisateur n'ait à faire quoi que ce soit. Le phénomène est important : en 2005, le fabricant de produit de sécurité informatique Symantec a recensé 48 nouvelles vulnérabilités affectant le navigateur Internet Explorer[29]. Ces vulnérabilités découlent du fait que certaines technologies Web avancées (ActiveX, JavaScript, Java, etc.) permettent à un webmestre d'exécuter des instructions informatiques par l'ordinateur de chaque visiteur dans un environnement dont les frontières sont — en théorie — contrôlées par le navigateur.

L'installation non-autorisée se produit lorsque le navigateur faillit à sa responsabilité de protéger l'utilisateur contre ces intrusions en accordant des privilèges anormaux à un « script» contenu dans une page Web. Le navigateur demeure vulnérable jusqu'à ce que l'utilisateur installe une mise à jour émise par son concepteur. Or, il s'écoule en moyenne 49 jours entre la découverte d'un « trou de sécurité » et la production d'une mise à jour par le fabricant[30].

---

26 « Spyware », *Wikipedia*, http://en.wikipedia.org/wiki/Spyware; « History of Spyware », http://www.pcsecuritynews.com/spyware_history.html.

27 « CNET Download.com Announces New Zero-Tolerance Adware Policy », *C|net*, http://pressreleases.cnetnetworks.com/phoenix.zhtml?c=67325&p=irol-newsArticle&ID=702769 .

28 « The Spyware Warrior List of Rogue/Suspect Anti-Spyware Products & Web Sites », http://www.spywarewarrior.com/rogue_anti-spyware.htm.

29 Symantec Internet Security Threat Report (vol. IX), http://www.symantec.com/enterprise/threatreport, p. 62.

30 Symantec Internet Security Threat Report (vol. IX), http://www.symantec.com/enterprise/threatreport, p. 5.

Une étude de l'Université de Washington observe que sur un échantillon de 45 000 pages Web, environ 2 pages sur 1 000 exploitent un bogue de sécurité au sein du navigateur Web afin d'installer un ou plusieurs logiciels espions sans aucune intervention de l'utilisateur[31]. Elle démontre de même que certaines catégories de sites Web sont plus susceptibles que d'autres de propager des logiciels espions par cette méthode, telles que les sites qui distribuent des logiciels piratés, des images de célébrités ou de pseudo-jeux[32]. D'autres supercheries moins sophistiquées, mais deux fois plus fréquentes[33], exigent de l'utilisateur une confirmation avant d'accéder au contenu du site en appuyant sur un bouton « OK », profitant du fait que celui-ci comprend rarement qu'il est en train d'autoriser l'installation d'un logiciel espion.

2.3.3 Réseau d'échange de fichiers entre pairs (P2P)

a) Présence dans les clients d'accès au réseau

Ayant connu un succès fulgurant depuis le lancement de Napster, les réseaux d'échange de fichiers entre pairs sont surtout utilisés pour télécharger des chansons, films, jeux et applications piratées. En soi, leur utilisation n'entraîne pas l'installation de logiciels espions. Le problème réside plutôt dans le fait que les programmes les plus populaires pour y accéder figurent parmi les derniers logiciels véritablement utiles à être commandités par des producteurs de logiciels espions.

Quoique qu'on en dise, ces réseaux ont d'abord et avant tout été créés pour faciliter la violation du droit d'auteur. Leurs développeurs ont par conséquent peu de scrupules à associer leurs produits aux logiciels espions. C'est notamment le cas de Sherman Networks qui n'hésite pas à prétendre en grosses lettres que Kazaa, son client pour accéder au réseau FastTrack, est exempt de tout logiciel espion, alors que le contraire fut pourtant démontré par l'organisme StopBadWare[34]. Selon le rapport de l'organisme, l'installation de Kazaa entraîne automatiquement l'installation du logiciel espion RX Toolbar et de plusieurs autres logiciels publicitaires dont il est impossible de se départir sans l'aide d'un expert.

b) Présence dans les fichiers échangés entre utilisateurs

Si les réseaux d'échange entre pairs ont été associés aux logiciels espions, c'est notamment parce qu'une partie considérable des fichiers auxquels ils donnent accès en sont infestés.

Jusqu'à l'arrivée des protocoles P2P, les fichiers étaient mis en ligne par le biais de serveurs HTTP et FTP. Ces serveurs étant généralement sous la supervision d'administrateurs réseau, ils ne contiennent pas ou très peu de logiciels malveillants. Les technologies P2P permettent désormais à tout internaute de facilement partager des fichiers présents sur son ordinateur personnel. Le problème est que, contrairement aux administrateurs réseau, les utilisateurs peu avancés n'ont pas les compétences requises pour garantir que leurs fichiers sont exempts de logiciels espions.

Qui plus est, on a longtemps considéré que seul un fichier exécutable était en mesure d'installer un logiciel malveillant. Une personne pouvait donc se dire : « Tant que je ne télécharge que des chansons, je suis à l'abri des virus. » Toutefois, il a récemment été découvert que la fonction de gestion des droits

---

31 Alexander Moshchuk et al., « A Crawler based study of Spyware on the Web », www.isoc.org/isoc/conferences/ndss/06/proceedings/html/2006/papers/spycrawler.pdf, p.11.

32 Alexander Moshchuk et al., « A Crawler based study of Spyware on the Web », www.isoc.org/isoc/conferences/ndss/06/proceedings/html/2006/papers/spycrawler.pdf, p. 12.

33 Alexander Moshchuk et al., « A Crawler based study of Spyware on the Web », www.isoc.org/isoc/conferences/ndss/06/proceedings/html/2006/papers/spycrawler.pdf, p. 11.

34 http://stopbadware.org/reports/reportdisplay?reportname=kazaa.

numériques d'un fichier Windows Media (.wma ou .wmv) peut être exploitée à mauvais escient[35]. Pour acquérir une licence, ce format de fichier permet au lecteur Windows Media d'ouvrir une page Web. Or, certaines firmes de cybermarketing et leurs partenaires abusent de cette fonction pour commander l'ouverture d'une page Web malicieuse qui installe des logiciels espions en exploitant une vulnérabilité du navigateur.

Il est difficile, par conséquent, de distinguer les fichiers potentiellement dangereux de ceux qui ne le sont pas sur ces réseaux.

2.4 Conséquences

2.4.1 Informatiques

La présence de logiciels espions sur un ordinateur réduit sa performance, sa stabilité et la qualité de l'expérience qu'il procure. Lorsqu'un ordinateur en est infecté, il l'est, règle générale, par une multitude de logiciels espions qui se chevauchent dans leur exécution et qui mobilisent une part considérable des ressources du système.

Cette perte de performance est aggravée par le fait que leurs concepteurs en bâclent le débogage et ne font peu de cas des pannes qu'ils occasionnent. En ajoutant à ces désagréments la diffusion envahissante et répétitive de fenêtres de publicités, on comprend dès lors le besoin d'en épurer le système.

2.4.2 Économiques

a) Pertes de productivité et frais de reconfiguration

La prolifération des logiciels espions sur Internet coûte cher aux entreprises et aux particuliers. Ces logiciels réduisent la productivité des travailleurs en rendant leur ordinateur si lent qu'il devient quasi inutilisable. En outre, ils sabotent leurs recherches en redirigeant leurs requêtes vers de pseudo-engins de recherche destinés uniquement à promouvoir des produits commerciaux et, trop souvent, carrément frauduleux. Dans bien des cas, l'utilisateur sera entraîné malgré lui vers un site Web pornographique, ce qui — on en conviendra — n'est pas approprié dans la plupart des milieux de travail.

Les techniciens et gestionnaires de réseaux qui oeuvrent en entreprise sont également affectés par leur présence dans la mesure où elle augmente le nombre d'appel de support technique qu'ils reçoivent. Leur désinstallation étant très ardue, voir impossible dans certains cas, il s'avère que la seule façon de s'en désencombrer est de procéder à la reconfiguration complète du poste de travail, — ce qui peut exiger plusieurs heures de travail. Le fabricant d'ordinateurs Dell note que les logiciels espions sont à la source de la plupart des appels à son service de support technique[36].

b) Usurpation de revenus publicitaires et de commissions

Les logiciels espions nuisent particulièrement à la cyberéconomie lorsqu'ils attribuent frauduleusement à leur auteur des ventes faites sur un site Web pour le compte d'un détaillant en ligne auquel il est affilié. Les programmes d'affiliation sont répandus chez les détaillant de livres et disques compacts comme Amazon.com. Leur fonctionnement est assez simple: l'auteur d'un site Web propose à ses visiteurs la lecture d'un livre et inclus un lien vers la page du produit sur le serveur du détaillant. Ce lien contient un code d'identification unique qui permet à celui-ci de connaître l'identité du partenaire qui a référé le client

35 John Leyden, « Trojans exploit Windows DRM loophole », *The Register*, http://www.theregister.co.uk/2005/01/13/drm_trojan/.

36 « The Latest High-Tech Legal Issue: Rooting Out The Spy In Your Computer », *The New York Times*, http://www.nytimes.com/ 2004/ 04/26/technology/26spyware.html (Page publiée le 26 avril 2004).

pour lui verser une commission. Le logiciel espion intercepte ce lien et y substitue son propre code d'identification unique. Il peut s'écouler des semaines avant que le détaillant prenne connaissance de cette usurpation.

Une autre façon de subtiliser des revenus revenant à des sites Web légitimes est de remplacer leurs bandeaux publicitaires par ceux du développeur d'un logiciel espion. Claria Corporation, qui possède le logiciel espion Gator, a été poursuivie par le *New-York Times* qui lui reprochait une telle conduite[37]. Il va sans dire que ce type de détournement frappe de plein fouet le modèle actuel de financement des fournisseurs de contenu gratuit sur Internet, puisqu'ils ont besoin des revenus générés par la publicité.

c) Croissance du marché des produits de sécurité

Pour toutes ces raisons, il s'est développé autour du logiciel espion une crainte généralisée qui stimule les ventes des fabricants de produits de sécurité informatique. Entre les années 2004 et 2005, ce marché a cru de 15 % selon Gartner[38]. Les chiffres pour l'année 2006 ne sont pas encore disponibles, mais rien ne laisse présager une diminution de cette tendance. Au cours des premières années du phénomène, les « majors » de l'industrie anti-virus ont tardé à ajouter à leurs produits des méthodes de détection des logiciels espions. Ils ont préféré créer des produits distincts, donc une dépense supplémentaire pour les entreprises et consommateurs. Toujours selon Gartner, il semble désormais que la mode soit à la réunion de leurs solutions anti-virus et anti-logiciel espion au sein d'une version « premium » de leurs produits.

2.4.3 Sur les utilisateurs

a) Violation du droit à la vie privée

La présence de logiciels espions sur un ordinateur personnel donne l'impression que celui-ci a été « vandalisé » sur le plan technique. Mais ce n'est pas tout.

Est-il nécessaire de rappeler que la fonction première d'un logiciel espion est d'accumuler des informations sur le comportement de l'usager sans son autorisation et de les transmettre à un tiers? Cela peut constituer une violation des règles en matière de protection des renseignements personnels. Sans sombrer dans l'alarmisme, il est également à noter que la plupart des experts prévoient que les logiciels espions seront de plus en plus utilisés par le crime organisé afin de faciliter la fraude bancaire et le vol d'identité dans le cadre d'attaques multidimensionnelles, c'est-à-dire faisant appel à la fois au courriel, au Web et à ces logiciels.

Développement d'appréhensions quant à l'utilisation d'Internet

Étant donné que les logiciels espions s'installent discrètement et proviennent de diverses sources, il est assez difficile pour une personne qui n'est pas bien familiarisée avec la sécurité informatique de s'en prémunir. Il en résulte une sorte d'angoisse incitant certains à limiter leurs activités sur Internet. Un sondage auprès de 2000 Américains a révélé que :

- 81 % des internautes ont cessé d'ouvrir des pièces jointes à un courriel d'une source inconnue.
- 48 % évitent des sites qu'ils considèrent potentiellement malveillant.
- 25 % ont arrêté de télécharger des fichiers sur des réseaux d'échange entre pairs.
- 18 % ont opté pour un autre navigateur Web qu'Internet Explorer.

Source : Susannah Fox. « Pew Internet & American Life Project May-June 2005 Survey », http://www.pewinternet.org.

37 Le litige a été réglé hors cour. Voir « Web publishers settle with Gator », *News. corn*, http://news.com.com/Web+publishers+settle+with+Gator/2100-1023_3-983870.html. Pour de plus amples renseignements sur cette pratique: http://www.thiefware.com.

38 http://www.gartner.com/it/page.jsp?id=496491.

2.5 La position des firmes de cybermarketing

2.5.1 Logiciel publicitaire ou logiciel espion ?

Un écueil majeur dans la détermination des mesures à prendre pour contrer la diffusion des logiciels espions est la difficulté de l'industrie à produire une définition du phénomène faisant l'unanimité.

a) La définition des éditeurs

> Seulement **12 %** des internautes croient qu'il est convenable que l'installation d'un logiciel espion soit divulguée par la lecture d'un contrat de licence. **83 %** considèrent que la mention devrait être plus visible.
>
> Source : Fox, Susannah, *opt. cit.*

Pour répondre aux critiques, plusieurs firmes de cybermarketing ont modifié leurs méthodes pour les rendre plus transparentes et moins envahissantes. C'est à ce moment que l'industrie a proposé la distinction entre un logiciel publicitaire et un logiciel espion. Pour bien la saisir, il suffit de garder en tête que le concept d'espionnage est intimement lié à celui de clandestinité. Selon cette définition, le logiciel publicitaire se distingue du logiciel espion dans la mesure où ses fonctions de profilage marketing et de distribution de publicité sont *honnêtement* et *clairement divulguées* à l'utilisateur. Ce dernier peut alors, en toute conscience, accepter de « vendre » une partie de son droit à la vie privée en échange de la possibilité d'utiliser gratuitement un logiciel qu'il juge utile. Contrairement aux logiciels espions, le logiciel publicitaire se désinstalle facilement, ce qui permet à l'utilisateur de révoquer son consentement à sa présence à tout moment, au risque cependant de rendre le logiciel qu'il finance inutilisable.

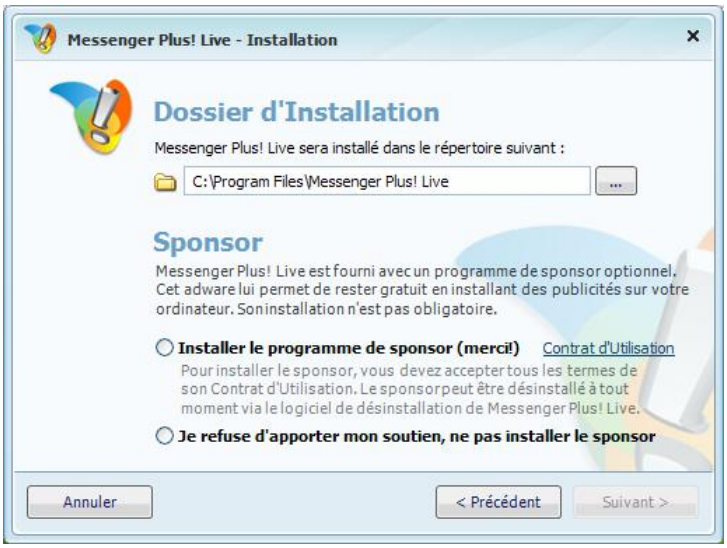

Fig. 5 — Installation clairement divulguée et optionnelle d'un logiciel publicitaire

Dans tous les cas, le développeur offre en général une version payante de son logiciel qui en retire l'aspect publicitaire. D'autres éditeurs plus soucieux de ne pas contrarier leurs utilisateurs choisissent même de présenter l'installation du logiciel publicitaire comme tout à fait optionnelle. La minorité de personnes qui choisissent malgré tout d'installer le logiciel publicitaire le font donc pour « encourager» et remercier son développeur (voir la Figure 5).

b) La réponse des groupes opposés aux logiciels espions

Toutefois, cette distinction proposée par l'industrie du cybermarketing ne fait pas consensus, surtout parmi les groupes opposés aux logiciels espions[39]. Pour certains[40], la qualification de «logiciel publicitaire» exige que le programme s'abstienne de dresser tout profil de consommateurs; il doit se contenter d'afficher «passivement» des publicités, c'est-à-dire sans transmettre de renseignements personnels ou sur l'historique de navigation à un serveur distant. Cette exigence s'explique par le fait que, selon eux, le consentement de l'utilisateur à transmettre ses habitudes de navigation n'est pas vraiment déterminant puisque que la plupart de gens ne lisent pas les contrats de licence avant d'installer un logiciel. L'Electronic Frontier Foundation (EFF) note par ailleurs que ces contrats contiennent souvent des clauses abusives qui, par exemple, interdisent d'utiliser des outils d'analyse (« *packet sniffer* ») afin de vérifier que le logiciel publicitaire ne communique pas d'informations non autorisées à son éditeur[41].

Il est à noter qu'une caractéristique qui irrite particulièrement les internautes est l'habitude des logiciels publicitaires d'afficher des fenêtres de publicité même quand l'utilisateur ne fait que visiter des pages Web. Leur raisonnement est que si un logiciel publicitaire est installé pour financer le développement d'un logiciel gratuit, alors la publicité qu'il diffuse ne devrait être vue que lorsque que ce logiciel est utilisé. C'est entre autres la position prise par le répertoire Download.com dans sa politique d'utilisation adressée aux développeurs de logiciels :

> *Nous autorisons certains types de logiciels distribués grâce à la publicité, incluant un petit nombre d'éléments de publiciels que nous évaluons au cas par cas. La publicité doit être limitée uniquement à l'interface qu'utilise l'usager et ne doit pas comporter de procédés publicitaires intrusifs tels les publicités s'ouvrant dans des fenêtres intruses.* [42] [Nous traduisons]

Cela explique pourquoi Download.com inclut un logiciel comme Eudora (qui représente l'exemple à suivre en cette matière) dans son répertoire, tandis qu'il exclut le Zango Messenger (car sa publicité est beaucoup plus intrusive et se manifeste même lorsque le logiciel « commandité » n'est pas utilisé). Dans le futur, il n'est cependant pas certain que Download.com continuera à exclure les logiciels publicitaires « intrusifs » étant donné que son propriétaire, CNET, participe à un programme de certification des logiciels publicitaires fondé sur des pratiques exemplaires[43]. Ce « Trusted Download Program » de l'organisme TRUSTe reste néanmoins très critiqué[44], car les pratiques exemplaires qu'il établit ne concernent que le consentement à l'installation du logiciel publicitaire et ne limitent pas suffisamment l'aspect intrusif des publicités qu'il diffuse.

---

39 L'expression « groupes opposés aux logiciels espions » inclut des organismes voués à la défense du droit à la vie privée sur Internet (www.epic.org) ou à la défense des droits des cybercitoyens (www.eff.org), des éditeurs d'anti-espiogiciels et la « communauté » constituée des utilisateurs expérimentés d'Internet.

40 Voir à ce propos : http://www.webopedia.com/DidYouKnow/Internet/2004/spyware.asp et http://www.stopbadware.org/reports/reportdisplay?reportname=zangomessenger.

41 http://www.eff.org/wp/eula.php.

42 "We allow certain types of advertising-supported software, including a small number of adware components we evaluate on a case-by-case basis. Ad-serving behavior must be restricted to the program's actual user interface, and may not include pop-ups or other forms of intrusive advertising"; http://www.upload.com/1200-21_5-750430.html.

43 http://www.truste.org/trusteddownload.php.

44 http://news.com.com/Will+certification+legitimize+adware/2100-1029_3-5956985.html?tag=st.prev et http://www.securityfocus.com/brief/313.

c) Une question de confiance

Il existe également un problème de confiance entre l'industrie du cybermarketing - qui tente de refaire son image avec des politiques claires quant au type de données recueillies et à leur usage - et les internautes au fait du phénomène. Mais plusieurs doutes se profilent à l'égard de ces promesses.

En dépit des propos rassurants de ces entreprises sur le comportement de leurs logiciels, plusieurs s'interrogent au sujet de leur volonté réelle à respecter leurs règles de bonne conduite. Par exemple, le statut de WhenU, un logiciel publicitaire très répandu, est sujet à controverse. Lavasoft, l'entreprise qui produit l'anti-espiogiciel Ad-Aware, l'avait retiré de sa liste de logiciels espions, mais a renversé sa décision à la suite des pressions des usagers[45]. Un test, effectué par un militant anti-logiciel espion, a démontré que WhenU ne respecte pas sa promesse pourtant claire de ne transmettre aucune information à ses serveurs[46]. L'entreprise a fait les précisions nécessaires dans sa politique depuis, mais cette révélation embarrassante n'a fait que confirmer les craintes des groupes opposés aux logiciels espions.

De Gator à Claria Corporation : les métamorphoses d'une industrie

À la fin des années 1990, au plus fort de la bulle boursière des « .com », de jeunes programmeurs cherchent une façon de financer un petit logiciel qu'ils ont développé. L'idée est simple, mais novatrice : joindre au logiciel un programme qui note les habitudes de navigation de son utilisateur. Des offres publicitaires seront offertes en fonction de celles-ci. Gator corporation est née.

L'entreprise connaît un succès fulgurant. Des millions d'internautes mordent à l'hameçon et téléchargent le logiciel « gratuit ». La compagnie obtient un investissement de $12.5 millions en 1999. Ses revenus passent de $14.5 millions en 2001 à $40.5 millions un an plus tard. Elle fait affaires avec de grands noms, tels que Sony, *The Wall Street Journal* et Yahoo!

Les utilisateurs, pendant ce temps, se demandent pourquoi leur ordinateur affiche tant de publicités. Ils ne savent pas qu'elles sont dues à l'installation d'eWallet, le logiciel-vedette de la société. Des anti-espiogiciels sont développés et Gator en est l'une des premières cibles. Les groupes de consommateurs se réveillent. L'entreprise est même dans la mire de la Federal Trade Commission (FTC). Les poursuites civiles s'accumulent. La réputation de la compagnie est gravement mise en cause. Gator reporte ses plans pour une première émission publique d'actions.

Mais la compagnie demeure rentable. En 2003, elle réalise un profit de $35 millions sur des revenus de $90 millions. Elle n'a qu'un problème d'image: Gator change son nom pour Claria Corporation.

La nouvelle compagnie renonce à ses pratiques les plus controversées. Le concept de « logiciel publicitaire » est proposé. Elle règle à l'amiable la plupart des poursuites qui la visent et engage un ancien employé de la FTC à titre de «Chief Privacy Officer ». L'entreprise considère qu'elle s'est refait une virginité. En conséquence, elle entame des poursuites pour diffamation envers ceux qui qualifient ses produits de logiciels espions. L'opération est si réussie que des rumeurs de rachat par Microsoft circulent dans le *New York Times*.

Consciente que les utilisateurs sont de moins en moins dupes et que les fenêtres de publicités constituent une espèce en voie de disparition, Claria développe un nouveau type de logiciel publicitaire: PersonaWeb. Ce nouveau produit perpétue la tradition de recueillir des profils de consommateurs, mais innove dans la façon de présenter la publicité qui y est liée. La publicité sera affichée directement sur des sites Web de partenaires, — sans générer une fenêtre supplémentaire. L'idée est qu'au fond, les utilisateurs sont prêts à tolérer que leur comportement en ligne soit épié en échange de logiciels gratuits. Pour autant, bien sûr, que cela leur soit divulgué et que la publicité se fasse sans obstruer leur environnement graphique ou ralentir leur ordinateur. Pour Claria, tout le monde y gagne.

Source : Annalee Newwitz. « Don't Call It Spyware », *Wired*, http://www.wired.com/wired/archive/13.12/spyware_pr.html.

45 http://www.spywareinfo.com/articles/spyware/whenu _detection _dropped.php (page consultée le 31 octobre 2006).

46 http://www.benedelman.org/spyware/whenu-privacy.

2.5.2 Le cas de CoolWebSearch

L'un des plus virulents logiciel espion qui circule sur Internet demeure CoolWebSearch et ses variants. S'installant en exploitant divers bogues de sécurité d'Internet Explorer, il a su se perfectionner au point d'être pratiquement impossible à désinstaller sans reconfigurer le système au grand complet.

Pour survivre, il s'installe dans des fichiers critiques de Windows XP (difficiles à manipuler) et bloque carrément l'exécution d'anti-espiogiciels. Pire encore, certains variants utilisent les milliers d'ordinateurs qu'il infeste pour mener des « attaques par saturation » dirigées contre les sites Web qui hébergent un des seuls antidotes efficaces qu'on lui connaisse (CWShredder)[47].

L'entreprise russe CoolWebSearch – qui exploite un pseudo-engin de recherche – prétend ne pas être mêlée à ces activités. Elle soutient qu'elle ne fait que rémunérer des partenaires qui lui envoient des visiteurs et qu'elle n'est pas responsable des méthodes douteuses employées par certains. Plusieurs observateurs mettent néanmoins en doute cette affirmation. Le problème de la preuve de la responsabilité des firmes de cybermarketing reste donc entier.

***

Le pourriel tend à se métamorphoser en vecteur pour un vaste ensemble d'activités illicites. En plus, les comportements abusifs à l'égard des ressources d'Internet connaissent des évolutions qui suivent de près les avancés du web lui-même. Ainsi, le phénomène des « splogs » (contraction de « spam » et de « blog») tend à empoisonner la vie de ceux qui tiennent ou fréquentent les blogs. Les splogs sont des blogs spécialement créés à des fins marketing[48]. De tels splogs peuvent être créés par centaines. Ils comportent des liens vers des sites Web. Or, les moteurs de recherche comme Google utilisent entre autres la notoriété (le nombre de liens vers un site) pour les classer. La méthode des polluposteurs consiste donc à grossir artificiellement le classement de ces sites dans les résultats délivrés par les moteurs de recherche.

Prenant appui sur le caractère ouvert et collaboratif des sites généralement associés à l'Internet 2.0, les polluposteurs acheminent des informations non souhaitées sur les blogs, les wikis ou même les sites comme « My Space », encombrant ces sites de liens abusifs[49]. Par exemple, le « link spamming » désigne la pratique consistant à placer de façon répétée des hyperliens sur les sites offrant des accès éditoriaux aux usagers, tels les blogs. De telles pratiques visent souvent à augmenter artificiellement et parfois frauduleusement le nombre de liens pointant vers un site. Les « sploggers » utilisent des programmes automatisant l'affichage de messages sur des milliers de sites en même temps.

Ainsi, on doit désormais prendre pour acquis que le pourriel et les fléaux qui y sont associés connaît et connaîtra des évolutions à la mesure de celles que connaîtra l'Internet dans son ensemble. C'est dire l'importance que revêt dorénavant les stratégies afin de combattre de tels fléaux.

---

47 « CoolWebSearch is winning Trojan War », *The Register*, 29 juin 2004, http://www.theregister.co.uk/2004/06/29/cws_shredder.

48 "Splog! Or How to Stop the Rise of a New Menace on the Internet", [2006] 19 *Harvard Journal of Law & Technology*, 467-484; < http://jolt.law.harvard.edu/articles/v19.php >, " Splog: quand le spam rencontre le blog", *Journal du net*, 5 septembre 2006, < http://www.journaldunet.com/0609/060905-splogs.shtml >.

49 Caroline McCARTHY, "MySpace sue 'Spam King' Richter", *ZDNet*, 22 janvier 2007, < http://news.zdnet.com/2100-1009_22-6152230.html >.

DEUXIÈME PARTIE
LES TENDANCES DE LA PRATIQUE INTERNATIONALE QUANT À LA RÉGLEMENTATION DU POURRIEL, DE L'HAMEÇONNAGE ET DES LOGICIELS ESPIONS

Dresser l'état des lieux des pratiques abusives entourant le pourriel permet de constater la rapidité de développement et les multiples facettes empruntées par ce phénomène pour contourner tout type de barrière. Plusieurs pays se sont dotés d'un cadre législatif, souvent spécifique, pour lutter contre le pourriel. Plusieurs des initiatives visent les messages non sollicités, donc le pourriel au sens étroit du terme. L'encadrement des pratiques associées à l'hameçonnage et aux espiogiciels demeure en grande partie assuré par des dispositions à caractère général comme celles relatives à la fraude et à la protection contre la surveillance illicite.

Mais les tendances observées dans la pratique internationale laissent de plus en plus voir que la réglementation à elle seule ne peut venir à bout de ce fléau. Un large consensus semble se dessiner autour de l'à-propos d'une approche coordonnée à volets multiples, de type « boîte à outils », dans laquelle tous les acteurs concernés jouent un rôle actif[50].

1. Les tendances des législations

De nombreux pays se sont dotés de politiques et de législations spécifiques pour lutter contre le pourriel. Mais le phénomène du pourriel est transversal et les pratiques abusives peuvent enfreindre les protections prévues dans les lois sur la protection du consommateur, le droit pénal, les lois sur la protection des données personnelles, les lois sur les télécommunications, la législation sur le commerce des valeurs mobilières etc. Les cadres nationaux se présentent généralement comme complexes et diversifiés[51].

1.1 Australie

En Australie, la législation limitant l'envoi de pourriel originant d'Australie n'est pas considérée comme l'unique réponse au fléau. C'est plutôt un élément d'une stratégie plus globale. Pour combattre le pourriel, l'Australie a adopté une stratégie en plusieurs volets : en plus d'une loi visant le pourriel originant d'Australie, sont prévues des mesures axées sur l'éducation et la sensibilisation des internautes et des entreprises de même que la mobilisation de solutions techniques, des partenariats avec l'industrie et de la coopération internationale[52].

En Australie, de nombreuses lois sont susceptibles de s'appliquer à différents aspects du pourriel, quoiqu'elles n'ont pas été conçues dans ce but. Mais, selon les autorités australiennes, une loi spécifique interdisant le pourriel complète et rend plus efficaces les mesures prises car elle indique une intention claire de la part du législateur. C'est dans cet esprit qu'a été adoptée une loi pour réduire le pourriel originant d'Australie, le *Spam Act 2003*, entrée en vigueur le 10 avril 2004, et qui est sous la responsabilité de l'Australian Communications and Media Authority (ACMA).

---

50 Jörg HLADJK, "Effective EU and US approaches to spam? Moves towards a co-ordinated technical and legal response", [2005] 10 *Communications Law*, 71-83 et 111-120.

51 OCDE, *Rapport du Groupe de réflexion sur le spam de l'OCDE : Boîte à outils anti-spam de politiques et mesures recommandées,* 19 mai 2006, p. 27, DSTI/CP/ICCP/SPAM/(2005)3/FINAL.

52 Les informations qui suivent sont tirées du site de l'Australian Communications and Media Authority (ACMA), *Spam-Junk email & messages*, < http://www.acma.gov.au/WEB/STANDARD//pc=PC_2008 >.

Cette loi interdit l'envoi d'un message commercial électronique non sollicité qui comporte un lien australien. Un message a un lien australien s'il origine ou s'il est envoyé à partir de l'Australie ou s'il vient d'ailleurs mais est envoyé à une adresse accessible en Australie. La loi vise les messages commerciaux électroniques par courriel, téléphone mobile (SMS), multimédia (MMS) et la messagerie instantanée (IM).

Un message électronique commercial doit être conforme à trois conditions, sinon il sera considéré comme du pourriel : le consentement du destinataire, l'identité de l'expéditeur et une fonction de désabonnement. Le message doit être envoyé avec le consentement du destinataire, qui peut être explicite[53] ou déduit[54] (*inferred*) de la conduite ou d'une relation commerciale ou autre relation préexistante. Le message doit aussi comporter des informations exactes sur la personne ou l'organisation qui a autorisé l'envoi du message et des informations sur la façon de la contacter. L'information doit être exacte et valide pour une période d'au moins 30 jours après que le message ait été reçu. Le message doit contenir une fonction de désabonnement pour permettre à la personne qui en manifeste le désir de ne plus recevoir de message (*opt-out*) et une pareille requête doit être honorée dans les cinq jours.

Si un message électronique commercial ne rencontre pas ces conditions, il est considéré comme du pourriel et il est en conséquence interdit. La loi interdit également l'utilisation de logiciel de cueillette d'adresses et les listes d'adresses produites à l'aide de tels logiciels.

La loi prévoit des amendes pouvant aller jusqu'à $1.1 million par jour pour des infractions répétées. Les sanctions sont graduées, en tenant compte de la gravité de la violation : lettre avisant de la violation et exigeant des explications, lettre formelle d'avertissement, amendes et procédures judiciaires. Des violations sérieuses et répétées entraînent des amendes plus lourdes.[55]

C'est en avril 2006 qu'a été intentée la première poursuite d'un polluposteur australien en cour fédérale de Perth pour violation du *Spam Act 2003*[56]. La cour a condamné respectivement Clarity1 Pty Ltd et son directeur à des amendes de $4.5 millions et de $1 million pour avoir envoyé des messages électroniques commerciaux non sollicités et pour avoir utilisé des listes d'adresses de courriels produites à l'aide de logiciels de cueillette d'adresses, et ce, en contravention du *Spam Act 2003*. L'ACMA avait soumis entre autres à la cour que Clarity avait envoyé pas moins de 231 millions de messages, la plupart illégaux, sur une période de douze mois depuis la mise en vigueur de la loi.

Le *Spam Act 2003* s'applique à l'envoi de messages non sollicités et non au contenu du message. Le contenu du message (par exemple : fraude, hameçonnage, escroqueries de type « Nigeria », ou « pump and dump », gains de loterie, publicité de produits de santé, atteinte à la vie privée, etc) peut aussi constituer une infraction à d'autres lois australiennes. L'ACMA assure la coordination nationale. Elle peut recevoir une plainte à l'égard d'un pourriel originant d'Australie et s'il viole d'autres lois, transférer la

---

53 Voir Australian Government, *Spam Act 2003: A Practical Guide for Business*, National office for Information Economy, Australian Communications Authority, February 2004, p. 9. Un consentement express se rencontre, entre autres, dans les circonstances suivantes : la personne a demandé spécifiquement ce matériel à l'entreprise par écrit ou verbalement; la personne a volontairement eu un accord avec un tiers qui fournit des adresses électroniques à l'entreprise afin de les utiliser à des fins de marketing ; la personne a volontairement ajouté son adresse à la liste d'adresses de l'entreprise, a donné son adresse électronique par téléphone ou par écrit à l'entreprise et s'il est clairement compris que des messages électroniques peuvent lui être envoyés à cette adresse.

54 Un consentement déduit ne peut être déduit du simple fait que l'adresse électronique a été publiée et se rencontre lors de relation commerciale pré-existante ou lors de la diffusion manifeste et publique d'une adresse reliée au travail. Mais dans ce dernier cas, pour que ce consentement soit valide, le message envoyé doit être directement relié au travail. Il existe des cas où on ne peut présumer du consentement. Voir Australian Government, *Spam Act 2003: A Practical Guide for Business*, National office for Information Economy, Australian Communications Authority, February 2004, p. 9.

55 ACMA, *Spam-Frequently Asked Questions,* http://www.acma.gov.au/WEB/STANDARD//pc=PC_1793.

56 ACMA, *ACMA welcomes Federal Court spam decision*, 27 octobre 2006, MR 129/2006, http://www.acma.gov.au/WEB/STANDARD//pc=PC_100888.

plainte à l'organisme pertinent[57]. L'ACMA travaille étroitement avec les autres instances gouvernementales qui ont un rôle à jouer dans la lutte contre certaines pratiques associées au pourriel[58].

Des mesures d'éducation et de sensibilisation font partie de la stratégie anti-pourriel de l'Australie. L'ACMA a produit du matériel éducatif et mis sur pied des séminaires destinés aux entreprises commerciales qui envoient des messages électroniques à leurs clientèles afin de les familiariser avec leurs obligations en vertu du *Spam Act 2003*[59]. L'ACMA offre aussi du matériel éducatif et des conseils pour les consommateurs afin de réduire le pourriel et augmenter la sécurité sur Internet[60].

Pour enrayer le pourriel, l'Australie mise aussi sur la mobilisation de solutions technologiques. Par exemple, l'ACMA est à mettre en place un projet pour enrayer les réseaux de zombies en Australie, qui sont actuellement le véhicule idéal de prolifération des pourriels (Zombie-hunting project)[61].

L'ACMA rend également disponible le bouton (« reporting button ») SpamMATTERS[62]. Une fois téléchargé sur l'ordinateur de l'usager, ce bouton permet simultanément et d'un seul coup de souris d'éliminer et de rapporter un pourriel à l'ACMA. Le pourriel est envoyé à une base de données où il est automatiquement analysé pour retracer son origine. Cette initiative permet à l'ACMA d'identifier plus facilement les campagnes de pourriels qui émergent et de récolter des informations sur des crimes reliés au pourriel comme l'hameçonnage, la fraude de type « Nigeria » et le « mule scams[63] ».

L'ACMA travaille en partenariat avec l'industrie : fournisseurs de services Internet, opérateurs de réseaux mobiles, compagnies de télémarketing et compagnies de logiciels. Par exemple, dans une démarche de corégulation prévue dans le *Telecommunications Act 1997*[64], l'ACMA a travaillé en consultation avec l'Internet Industry Association (IIA), organisme représentatif de l'industrie, dans le but d'élaborer un code de conduite à l'intention des fournisseurs de services Internet et de courriel. Le code[65] exige des fournisseurs de services Internet et de courriel de fournir à leurs abonnés des choix de filtres anti-pourriel, des informations sur la façon de traiter le pourriel et un mécanisme de traitement des plaintes.

---

57 Ex : contenu frauduleux : Australian Competition and Consumer Commission (ACCC) ou Australian Securities and Investment Commission (ASIC) ; violation de la vie privée : Office of the Federal Privacy Commissioner. Ces organismes peuvent aussi recevoir les plaintes directement.

58 ACMA, *Spam-Frequently Asked Questions,* http://www.acma.gov.au/WEB/STANDARD//pc=PC_1793. Par exemple, l'Australian Competition and Consumer Commission (ACCC), l'Australian High Tech Crime Centre (AHTCC, Federal Police), la Telecommunications Industry Ombudsman (TIO), l'Australian Securities and Investmesnts Commission (ASIC), l'Office of the Federal Privacy Commissioner (OFPC).

59 ACMA, *Spam Act 2003: A Practical Guide for Business*, http://www.acma.gov.au/webwr/consumer_info/frequently_asked_questions/spam_business_practical_guide.pdf.

60 ACMA, *Fighting Spam in Australia-A Consumer Guide*, http://www.acma.gov.au/webwr/consumer_info/spam/consumer_information/spam_consumerguide.pdf. L'Australian Government Department for Communications, Information Technology and the Arts a préparé un document d'information sur le hameçonnage: *Phishing-Don't taket he bait! Avoid being caught by fraudulent email*.

61 ACMA, *Australian zombie-hunting program launched*, 7 novembre 2005, MR 41/2005, http://www.acma.gov.au/WEB/STANDARD//pc=PC_100266.

62 ACMA, *ACMA launches « one click » spam reporting button,* media releases, 30 mai 2006, MR 62/2006, http://www.acma.gov.au/WEB/STANDARD//pc=PC_100598.

63 C'est le recrutement d'internautes crédules qui servent d'intermédiaires locaux pour tranférer des fonds illégalement acquis par hameçonnage.

64 Le *Telecommunications Act 1997* renferme des dispositions complétant le *Spam Act 2003*. Ces dispositions visent le pourriel, principalement pour le développement, l'enregistrement et la mise en vigueur de codes et de normes de l'industrie, d'une façon volontaire ou à la demande de l'ACMA.

65 Internet Industry Association, *Internet Industry Spam Code of Practice-A Code for Internet and Email Service Providers*, Co-Regulation in Matters Relating to Spam Email (Consistent with the Requirements of the Spam Act 2003 and Telecommunications Act 1997 to the Extent it Relates to the Spam Act), December 2005, Version 1.0.www.iia.net.au.

Le code indique comment traiter les sources de pourriels présentes sur les réseaux des fournisseurs de service Internet et leur suggère des meilleures pratiques (*best practices*) pour renforcer leur réseaux contre le pourriel et ses fléaux comme les zombies. L'ACMA a enregistré ce code et les obligations énoncées sont en vigueur depuis le 16 juillet 2006[66]. Ce code s'applique aux 689 fournisseurs de services Internet de l'Australie ainsi qu'aux fournisseurs de services de courriel offrant leurs services en Australie tels Hotmail et Yahoo.

Toujours en vertu du *Telecommunications Act 1997*, un comité formé de représentants de l'industrie du e-marketing, de groupes de consommateurs et d'autorités gouvernementales ont développé le *Australian eMarketing Code of Practice* qui établit les lignes directrices pour l'envoi de messages électroniques commerciaux en conformité avec le *Spam Act 2003*[67]. Enregistré le 16 mars 2005, ce code est obligatoire et relève de l'autorité de l'ACMA.

La coopération internationale est un volet de la lutte contre le pourriel en Australie. Par exemple, en septembre 2006, l'ACMA lançait une enquête sur un résident australien accusé d'avoir envoyé plus de 2 milliards de messages électroniques non sollicités dans le monde qui proposaient des produits Viagra[68]. L'enquête a été lancée suite à une information fournie par l'OPTA (l'organisme anti-pourriel des Pays-Bas). En effet, les autorités néerlandaises, après une perquisition chez un opérateur Internet, ont découvert qu'un australien était à l'origine de cet acte. L'ACMA travaille étroitement avec les organismes internationaux dans cette affaire.

L'ACMA Anti-Spam Team travaille aussi en collaboration avec des instances anti-pourriel étrangères pour partager leurs connaissances. Le gouvernement australien a également conclu des accords anti-pourriel avec d'autres pays, travaille avec l'Union internationale des télécommunications et l'OCDE pour développer des approches multilatérales pour réduire le pourriel.

Rebecca Bolin remarque que la stratégie australienne est largement tributaire de l'action de l'organisme gouvernemental de réglementation. Or, elle relève que l'ACMA avait, en début de l'année 2006, enjoint 350 entreprises de mettre fin au pourriel, a imposé des amendes à quelques unes et accusé une seule devant les tribunaux[69]. Mais pour plusieurs, les « lois anti-pourriel de l'Australie sont considérées comme les meilleures »[70]. La stratégie australienne semble en effet porter fruits. Depuis la mise en vigueur du *Spam Act 2003*, le pourriel originant de l'Australie a considérablement réduit. L'Australie est passée de la 10ième position en avril 2004 à la 25ième en juin 2006 (données Sophos)[71].

1.2 Europe

En Europe, deux directives encadrent la prospection par courriel[72]. D'abord la directive 95/46/CE du 24 octobre 1995[73] dispose qu'une opération de prospection par courriel par un organisme établi au sein de

---

66 ACMA, *ACMA registers Internet industry code on spam*, 28 mars 2006, MR34/2006, http://www.acma.gov.au/WEB/STANDARD//pc=PC_100488.

67 *Australian eMarketing Code of Practice*, mars 2005, http://www.acma.gov.au/webwr/telcomm/industry_codes/codes/australian%20emarketing%20code%20of%20practice.pdf.

68 ACMA, *ACMA executes search warrant for alleged major breaches of Spam Act*, 12 septembre 2006, MR 100/2006, http://www.acma.gov.au/web/STANDARD//pc%3DPC_100759.

69 Rebecca BOLIN, "Opting Out of Spam: A Domain level Do-Not-Spam Registry", [2006] 24 *Yale Law & Policy Rev.*, 399-435, p. 421.

70 Selon le Groupe de travail sur le pourriel, *Comparaison des mesures internationales de lutte contre le pourriel*, mai 2005.

71 ACMA, *Spam information for the media*, http://www.acma.gov.au/ACMAINTER.1638528:STANDARD::pc=PC_2861.

72 Les pourriels frauduleux et trompeurs sont aussi des pratiques illégales en vertu des règles existantes de l'UE sur la publicité mensongère et les pratiques commerciales déloyales (Directive 84/450/CEE sur la publicité mensongère).

l'Union doit respecter les règles suivantes : il doit informer les personnes, dès la collecte de leur adresse électronique, de l'utilisation ou de la cession à un tiers de l'adresse à des fins de marketing et il doit mettre à la disposition des personnes, un droit d'opposition. Par exemple, la pratique de récolte d'adresses de courriels (collecte automatique de données à caractère personnel) sur des lieux publics d'Internet, automatisée ou non à l'aide d'un logiciel, est illégale en vertu de cette directive.

L'article 13 de la directive 2002/58/CE sur la protection de la vie privée et les communications électroniques[74], adoptée en juillet 2002, introduit dans l'ensemble de l'Union européenne le principe du consentement préalable de la personne en matière de prospection commerciale. Elle interdit l'envoi de communications commerciales non sollicitées par courrier électronique ou par un autre système de messagerie électronique dans toute l'Union européenne, sauf si la personne a donné son consentement préalable ou dans le cadre limité de relations client-fournisseur existantes. Il est aussi interdit de dissimuler l'identité de l'expéditeur pour le compte duquel la communication a été effectuée et le message doit indiquer une adresse de réponse valide pour s'opposer à l'envoi de messages ultérieurs.

Plusieurs États membres de l'Union Européenne ont transposé cette directive en droit national, dont la France et les Pays-Bas.

1.2.1 France

Selon le Groupe de réflexion sur le spam de l'OCDE, la France offre un bon exemple d'approche globale et cohérente au phénomène du pourriel et à ses divers enjeux, particulièrement en ce qui concerne la cybersécurité et la protection du consommateur, avec la *Loi pour la confiance dans l'économie numérique*[75].

L'article 22 de la *Loi pour la confiance dans l'économie numérique* pose le principe du consentement préalable. L'utilisation des adresses de courriel dans les opérations de prospection commerciale est soumise au consentement préalable des personnes concernées. Il est interdit d'adresser aux personnes physiques des messages de nature commerciale par courrier électronique, par SMS ou par MMS sans avoir obtenu préalablement leur consentement[76]. Le consentement doit être libre, spécifique et informé[77]. Si la personne y a consenti, elle doit avoir la possibilité à tout moment de s'opposer à l'envoi de messages (modalités de désinscription) et doit être informée de l'identité de l'expéditeur ou de la personne pour lequel le message a été envoyé. Une dérogation est prévue au principe de consentement préalable lorsque la personne a déjà été contactée à l'occasion d'une vente ou d'une prestation de service : la prospection commerciale sera permise sans permission préalable pour des produits ou des services analogues. L'entreprise doit quand même offrir la possibilité de s'opposer à recevoir de la publicité de sa part.

---

73 Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, JO L 281 du 23 novembre 1995.

74 Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (Directive « vie privée et commerce électronique »), JO L 201 du 31 juillet 2002.

75 Loi no 2004-575 du 21 juin 2004. L'article 22 vient définir les articles L. 34-5 du Code des postes et des communications électroniques et L. 121-20-5 du Code de consommation; OCDE, *Rapport du Groupe de réflexion sur le spam de l'OCDE : Boîte à outils anti-spam de politiques et mesures recommandées,* 19 mai 2006, note 33, DSTI/CP/ICCP/SPAM/(2005)3/FINAL.

76 Une amende de 750 euros par message expédié est prévue pour le non-respect du principe de consentement préalable. Le consentement préalable n'est pas exigé lorsque le message est adressé à une personne morale.

77 La CNIL recommande que le consentement soit donné à l'aide d'une case à cocher mais non par le biais d'une case pré-cochée. CNIL, *SPAM: L'état du droit en France*, <http://www.cnil.fr/index.php?id=1272>

La Commission nationale de l'informatique et des libertés (CNIL) veille, pour ce qui concerne la prospection directe utilisant les coordonnées d'une personne physique, au respect des dispositions de cet article en application des compétences qui lui sont reconnues par la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (Loi Informatique et Libertés). À cette fin, elle peut notamment recevoir, par tous moyens, les plaintes relatives à des infractions aux dispositions de l'article.

La prospection par courrier électronique demeure soumise à la législation sur la protection des données en ce qui concerne la collecte. Les adresses de messagerie utilisées à des fins de prospection doivent avoir été collectées de manière loyale (information préalable sur l'utilisation de l'adresse électronique à de telles fins et droit de s'opposer à cette utilisation). Par exemple, la collecte d'adresses de courrier électronique dans des espaces publics de l'Internet (sites web, forums de discussion, annuaires) sans la connaissance des personnes concernées est une collecte déloyale en vertu de la Loi Informatique et Libertés[78].

Certaines pratiques délictuelles reliées au pourriel peuvent aussi contrevenir à des dispositions du Code pénal relatives aux atteintes aux systèmes de traitement automatisé de données (ex : utilisation du matériel informatique à l'insu des personnes, « mailbombing »). La distribution et l'emploi d'espiogiciels, et plus généralement, toute activité consistant à collecter, par des moyens informatiques installés sur le poste informatique des personnes concernées et à leur insu, des informations à caractère personnel ou concernant leur équipement, peut être constitutif d'un délit à la loi n° 88-19 du 5 janvier 1988 (loi Godfrain) qui garantit la sécurité des systèmes informatiques en punissant l'accès ou le maintien frauduleux dans un système informatique[79].

La France a également mis en place des partenariats public/privé. Le 10 juillet 2003, le Gouvernement français a annoncé la création d'un groupe de concertation et d'action contre le spam dont l'objectif est de favoriser la concertation entre les acteurs publics et privés de la lutte contre le spam et la coordination de leurs actions, en France comme à l'international. Le *Groupe de contact des acteurs de la lutte contre le spam*, animé par la Direction du développement des médias (DDM) a pour objectif de faciliter et d'accompagner la mise en œuvre d'actions concrètes contribuant à résorber le « spam », dans ses causes comme dans ses effets. Ce Groupe a *entrepris de mettre en place plusieurs groupes de travail thématiques ainsi que de créer un centre de ressources français sur le spam dont les missions incluront notamment le recueil des plaintes des utilisateurs contre les «spammeurs»*[80]. Le Groupe travaille entre autres sur un projet de réouverture d'une «boîte à spam », projet mené en 2002 par la CNIL et qui a permis l'établissement de premières analyses statistiques sur ce phénomène en France. Ce nouveau projet, le SignalSpam se veut un outil logiciel de signalement, de recueil et d'analyse des pourriels reçus par les usagers français[81].

Le Forum des droits sur l'Internet, créé avec le soutien des pouvoirs publics, est un organisme de concertation multiacteur responsable de la corégulation de l'Internet en France. Ses missions sont l'information et la sensibilisation du public et la concertation entre les pouvoirs publics, les entreprises et

---

78 CNIL, *Spam : L'état du droit en France*, www.cnil.fr.

79 Voir Forum des droits sur l'Internet, *Recommandation-Les publiciels et espiogiciels*, 11 juillet 2006, http://www.forum internet.org/recommandations/lire.phtml?id=1094. Le droit des contrats peut également offrir une solution au pourriel. Au niveau contractuel, les fournisseurs d'accès Internet peuvent priver d'accès leurs clients identifiés comme polluposteurs en vertu des conditions générales d'utilisation de leur service ou de la nétiquette qui condamne la pratique du pollupostage. Voir TGI Rochefort-sur-mer, 28 février 2001 où on a reconnu une telle solution en vertu de l'article 1135 du Code civil.

80 CNIL, http://www.cnil.fr/index.php?1266.

81 Direction du développement des médias, *La réouverture de la "boîte à spam",* 21 septembre 2005, http://www.ddm.gouv.fr/article.php3?id_article=369. Le site SignalSpam est ouvert depuis juillet 2006 (http://www.signal-spam.fr). Il est actuellement un centre de ressources et d'information pour les utilisateurs afin de se prémunir contre le pourriel. Au cours du premier trimestre de 2007, il devrait offrir aux utilisateurs de signaler automatiquement les pourriels dont ils sont victimes et de suivre leur signalement.

les utilisateurs sur la question des règles et usages de ce nouvel environnement. Dans le cadre de ses missions, le Forum s'est intéressé aux différentes menaces et fraudes sur Internet (ex : publiciels et espiogiciels), soit en sensibilisant le public ou en formulant des recommandations et interprétations destinés aux éditeurs de logiciels, aux utilisateurs et aux pouvoirs publics[82].

La mobilisation des pays francophones (Nord-Sud) est un élément de renforcement dans la lutte contre le pourriel. La France, le Maroc, la Belgique et l'Institut francophone des nouvelles technologies de l'information et de la formation (INTIF-OIF) ont organisé un premier atelier francophone de lutte contre le pourriel en mars 2006, réunissant 14 pays participants[83].

Les autorités françaises croient aussi qu'il est nécessaire d'intégrer une dimension internationale pour lutter efficacement contre le phénomène du pourriel. Le gouvernement français participe activement à plusieurs forums internationaux et européens où « l'on traite de la coopération judiciaire, de l'échange d'informations et des bonnes pratiques en matière de spam : Commission européenne, OCDE, UIT, ASEM, APEC »[84]. La France est également partie à diverses conventions bilatérales ou multilatérales susceptibles de s'appliquer à la lutte contre le pourriel.

1.2.2 Pays-Bas

Aux Pays-Bas, et ce depuis 2004, l'article 11.7 de la *Loi sur les télécommunications* réglemente les communications électroniques non sollicitées et introduit le régime de consentement préalable en matière de prospection, conformément à la directive européenne[85]. La loi prévoit aussi que le message doit révéler l'identité de l'expéditeur et fournir une adresse de réponse valide pour les demandes de refus subséquents. L'OPTA, l'autorité indépendante de régulation des postes et des communications, est responsable de l'application de la loi. D'autres lois, comme celle relative à la protection des données personnelles, complètent les mesures de protection contre le pourriel.

Dès la première année de la mise en vigueur de la loi, la lutte anti-pourriel a constitué une priorité pour l'OPTA[86]. L'OPTA a mis sur pied un site web (www.spamklacht.nl) qui fournit des renseignements sur l'interdiction de pourriel et reçoit les plaintes des citoyens. Ces plaintes (plus de 20,000 en février 2007) sont une source d'information pour les enquêtes menées par l'OPTA. En février dernier, l'OPTA imposait une amende de 75,000 euros à un polluposteur néerlandais, la plus haute à ce jour, pour avoir contrevenu à l'interdiction de pourriel[87]. L'OPTA collabore aussi avec les autorités étrangères de

---

82 Voir Forum des droits sur l'Internet, *De quelques dangers en "ing"*, 28 septembre 2006, <http://www.foruminternet.org/actualites/lire.phtml?id=1112>, où on présente certaines fraudes développées sur l'Internet (phishing, pharming, IP spoofing, sniffing, spamming, scamming, bombing, metatagging, Googlebombing, happyslapping, typosquatting, cybersquatting, dotsquatting) ; Forum des droits sur l'Internet, *Recommandation-Les publiciels et espiogiciels*, 11 juillet 2006, < http://www.foruminternet.org/recommandations/lire.phtml?id=1094>. Le Forum a aussi un service d'information, le site DroitDuNet.fr, où il publie des fiches pratiques sur ces différents dangers.

83 Direction du développement des médias, *Succès du premier atelier francophone de lutte contre le spam*, 28 mars 2006, < http://www.ddm.gouv.fr/article.php3?id_article=1050>

84 Direction du développement des médias, *Le gouvernement français s'engage dans la lutte contre le « spam »*, http://www.ddm.gouv.fr/article.php3?id_article=606.

85 Groupe de travail sur le pourriel, *Comparaison des mesures internationales de lutte contre le pourriel*, mai 2005.

86 OPTA, *Annual report and market monitor 2005*, pp. 31-32, <http://www.opta.nl/download/jaarverslag%5F2005%5Finteractive%5Fwebsite%5Fen%2Epdf>.

87 OPTA, *OPTA: EUR 75.000 fine for spammer*, Press releases, 2 février 2007, < http://www.opta.nl/asp/en/newsandpublications/pressreleases/document.asp?id=2126 >.

réglementation, européennes et américaines, par des échanges d'information ou des campagnes de sensibilisation[88].

Il a été possible de réduire le pourriel originant des Pays-Bas de 85% au moyen des poursuites engagées par l'OPTA, et ce en y consacrant seulement 5 personnes à plein temps et 570,000 euros d'équipement[89]. Les efforts et les moyens investis par les Pays-Bas en matière de lutte contre le pourriel sont cités en exemple par la Commission européenne. La Commission constate qu'« investir ne serait-ce que modérément dans la lutte antipourriel peut aussi donner des résultats significatifs »[90].

1.3 États-Unis

Pas moins de trente-huit états américains ont adopté des législations anti-pourriel[91] qui consacrent généralement l'existence d'un droit d'opposition à la réception d'un message. Ces lois contiennent aussi des exigences concernant l'étiquetage des messages et réglementent les messages trompeurs et la transmission d'information. Certains états, comme la Californie et le Delaware, ont plutôt adopté l'approche du consentement préalable[92].

La législation fédérale sectorielle sur la réglementation des valeurs mobilières a été intensément utilisée afin de combattre les pratiques de pourriel impliquant des informations relatives à des produits financiers proposés au public. Entre 1995 et 2006, la Commission américaine des valeurs mobilières, la Security and Exchange Commission, a intenté plus de 500 poursuites judiciaires relativement à des activités se déroulant sur Internet, dont plusieurs visaient les polluposteurs ou autres activités de fausses représentations effectuées via Internet[93].

En janvier 2004 entrait en vigueur une loi fédérale, le *Controlling the Assault of Non-Solicited Pornography and Marketing Act* ou le CAN-SPAM Act, dont la mise en oeuvre est sous la responsabilité de la Federal Trade Commission (FTC). Cette loi a préséance « sur les dispositions des lois anti-pourriel des états qui réglementent précisément l'utilisation des messages électroniques commerciaux, mais non sur les lois qui interdisent les affirmations fausses ou trompeuses dans les messages électroniques commerciaux »[94].

Le CAN-SPAM Act s'applique au courriel commercial dont le but premier est la publicité ou la promotion d'un produit ou d'un service commercial. La loi prévoit un droit d'opposition a posteriori à recevoir des courriers électroniques. Ce régime se veut respectueux de la liberté d'expression. Il autorise les commerçants à faire de la prospection commerciale par voie électronique en l'absence de refus des

---

88 OPTA, *First year's fight against spam yields positive results: Growing collaboration with American regulator*, Press release, 6 mars 2005, < http://www.opta.nl/asp/en/newsandpublications/pressreleases/document.asp?id=2260>.

89 Commission européenne, *Lutte contre le pourriel, les espiogiciels et les logiciels malveillants: les États membres doivent mieux faire d'après la Commission*, Press release, 27 novembre 2006, < http://europa.eu >; OPTA, *Annual report and market monitor 2005*, p. 32, <http://www.opta.nl/download/jaarverslag%5F2005%5Finteractive%5Fwebsite%5Fen%2Epdf>.

90 Commission des communautés européennes, *Communication de la Commission au Parlement européen, au Conseil , au Comité économique et social européen et au Comité des régions sur la lutte contre le pourriel, les espiogiciels et les logiciels malveillants,* 15 novembre 2006, COM(2006) 688 final, p. 3.

91 Tiré de National Conference of State Legislatures, *State Laws Relating to Unsolicited Commercial or Bulk E-mail (SPAM),* < http://www.ncsl.org/programs/lis/legislation/spamlaws02.htm>

92 John REED STARK et Carolyn E. KURR, "Using the Securities and Exchange Commission's Statutory Weaponry to Combat Spam", [2006] 37 *University of Toledo Law Rev.*, 271-305, p. 276.

93 John REED STARK et Carolyn E. KURR, "Using the Securities and Exchange Commission's Statutory Weaponry to Combat Spam", [2006] 37 *University of Toledo Law Rev.*, 271-305, p. 282.

94 Clinique d'intérêt public et de politique d'Internet du Canada, *Un droit privé d'action prévu par la loi contre les polluposteurs au Canada : Contexte canadien, leçons apprises et répercussions des diverses approches*, Rapport présenté au Groupe de travail sur le pourriel d'Industrie Canada, 17 décembre 2004, p. 12.

destinataires du message et moyennant certaines conditions. Les commerçants peuvent faire l'envoi de messages jusqu'à une éventuelle opposition des destinataires, c'est-à-dire lorsque le destinataire signale sa faculté de refuser la réception de messages.

La loi exige que le message contienne un dispositif de retrait (opt-out) et une adresse de retour valide de l'expéditeur pour recevoir les demandes de retrait. L'envoi de courriels commerciaux à un destinataire qui s'est désabonné est interdite. La loi interdit aussi les informations de transmission de messages trompeurs (utilisation d'en-têtes faux ou d'intitulés trompeurs dans la ligne « objet ») et la publicité mensongère. La loi n'exige pas que le message comporte une quelconque indication sur la nature du message, sauf si celui-ci contient du matériel pornographique explicite[95].

Un droit privé d'action est prévu pour le fournisseur de services Internet mais non pour un particulier[96]. La cueillette d'adresses par l'utilisation d'un générateur d'adresses et les attaques par dictionnaire aggravent les peines encourues. La loi autorise en outre la possibilité d'établir un registre « Do-Not-E-Mail » par la FTC. Ce registre, inspiré du registre « Do-Not-Call » implanté pour le télémarketing, permettrait de se joindre à une liste de personnes ne désirant pas recevoir de sollicitation par courrier électronique. Mais le FTC a fait savoir que ce registre serait difficilement réalisable[97].

Dès sa mise en vigueur, la loi fédérale a fait l'objet de nombreuses critiques. Par dérision, la loi a été renommée « You can spam » Act par ceux qui croient que la loi a plutôt légalisé le pourriel; les polluposteurs envoient des contenus frauduleux sous des dehors qui respectent la législation[98].

Une des critiques les plus importantes est que la loi fédérale a préséance (« *preempt* ») sur les dispositions plus sévères des lois anti-pourriel des états, comme par exemple la loi de la Californie, qui a adopté une approche de consentement préalable et un droit privé d'action. L'approche de la loi fédérale, soit le consentement présumé du destinataire jusqu'à son opposition, est considérée inefficace par plusieurs. La loi servirait les intérêts de l'industrie du marketing et de la publicité en plaçant la charge de traitement et les coûts sur les épaules du consommateur[99]. La loi fédérale a d'ailleurs reçu le soutien de la Direct Marketing Association. L'approche du consentement préalable était largement préconisée par les associations américaines de consommateurs et les internautes puisque le consommateur choisit alors de qui il veut recevoir de la prospection commerciale.

De même, une quinzaine de législations des états exigent l'étiquetage des messages publicitaires par la mention ADV ou autre, ce qui donne la possibilité au consommateur de filtrer ses messages sans avoir à les ouvrir. Le CAN-SPAM Act « écarte les causes d'action fondées sur l'étiquetage et le consentement, ce

---

95 C'est la FTC qui détermine si le contenu est licite ou non.

96 À noter que les sanctions à la CAN-SPAM Act sont les suivantes :une amende de 250$ par infraction, jusqu'à concurrence de 2 millions$ pour non-conformité non intentionnelle, ainsi que d'une amende pouvant atteindre 6 millions$ pour infraction intentionnelle, assortie de dommages-intérêts exemplaires. Pour les cas les plus graves, des peines d'emprisonnement jusqu'à cinq ans sont prévues. Tiré de Groupe de travail sur le pourriel, *Comparaison des mesures internationales de lutte contre le pourriel*, mai 2005.

97 Dans un rapport de 2004, la FTC, doutant de l'application effective de la liste, « recommandait plutôt de concentrer les efforts de la lutte anti-spam sur la création d'un système performant d'authentification des adresses électroniques qui permettrait d'empêcher les spammeurs de cacher leur routage en vue d'échapper aux filtres anti-spam des fournisseurs d'accès et à l'application de la loi. », Direction du développement des médias, *Le « spam »-Le cadre juridique-La législation des Etats-Unis en matière de « spam »*, <http://www.ddm.gouv.fr/article.php3?id_article=603>.

98 Adam HAMEL, "Will the CAN-SPAM Act of 2003 Finally Put a Lid on Unsolicited E-Mail", (2004-2005) 39 *New England Law Review* 961, 997.

99 W. Parker BAXTER, "Has Spam Been Canned? Consumers, Marketers, and the Making of the CAN-SPAM Act of 2003, (2005) 8 *NYU Journal of Legislation and Public Policy*, p. 169, 172.

qui ne laisse que la possibilité d'intenter des actions pour transmission de renseignements trompeurs en vertu des lois des États »[100].

Par contre, les défenseurs du CAN-SPAM Act font valoir qu'étant donné l'existence de différentes lois pour chacun des états américains, une loi fédérale uniforme est la solution appropriée pour régler les problèmes de juridiction. On prétend également que la loi favorise le commerce, notamment le commerce électronique. Ce texte est l'aboutissement d'un conflit existant entre les acteurs du marché et les défenseurs des libertés individuelles. Surtout, l'interdiction d'utiliser des en-têtes faux ou des intitulés trompeurs dans la ligne « objet » est considérée comme un progrès pour la prévention de la fraude puisque deux-tiers des pourriels contenait une telle falsification d'information[101]. De plus, l'accent est mis sur la mise en application de la loi; d'importants fournisseurs de services Internet ont poursuivi des polluposteurs et des sanctions très lourdes ont été prononcées contre eux. Certains constatent :

> *Il semble que moins d'un an après l'entrée en vigueur de la CAN-SPAM Act, les critiques diminuent au fur et à mesure que les poursuites commencent à augmenter. Les observateurs semblent constater maintenant que l'application de la loi prend du temps et qu'il faut souvent innover lors de la collecte et de l'interprétation des éléments de preuve technologiques. Il y a une courbe d'apprentissage, et il faut un certain temps pour que les mesures prises arrivent à maturité.*[102]

Plusieurs études suggèrent que le phénomène du pourriel n'a pas été freiné malgré la mise en vigueur de la loi et les nombreuses poursuites intentées[103].

1.4 Canada

Bien que le pourriel a été identifié comme un enjeu majeur du développement d'Internet, la politique du gouvernement fédéral, et notamment d'Industrie Canada a été celle du laisser-faire fondée sur le crédo à l'égard de la capacité du secteur privé agissant seul à enrayer le phénomène. Les autorités canadiennes ont été lentes à réagir au phénomène du pourriel. Ce n'est qu'en 1999 qu'Industrie Canada a publié une première prise de position sur le pourriel. Ce document célébrait les soi-disant vertus du marché compétitif et des choix des consommateurs et considérait qu'il s'agissait d'appliquer les lois générales afin de combattre le phénomène. Toutefois, aucune politique concrète ne fut mise de l'avant afin de favoriser l'application concertée des dispositions susceptibles de trouver application à l'égard du pourriel[104].

En janvier 2003, Industrie Canada publie un document de discussion sur le pourriel. On y soulève pour la première fois, la perspective d'une législation spécifique sur le pourriel. Face à la montée des critiques à l'égard de la politique jovialiste d'Industrie Canada au sujet d'Internet, le gouvernement s'interroge sur les

---

100 Clinique d'intérêt public et de politique d'Internet du Canada, *Un droit privé d'action prévu par la loi contre les polluposteurs au Canada : Contexte canadien, leçons apprises et répercussions des diverses approches*, Rapport présenté au Groupe de travail sur le pourriel d'Industrie Canada, 17 décembre 2004, p. 12. John REED STARK et Carolyn E. KURR, "Using the Securities and Exchange Commission's Statutory Weaponry to Combat Spam", [2006] 37 *University of Toledo Law Rev.*, 271-305, p. 276.

101 Lilly ZHANG, "The CAN-SPAM Act: An Insufficient Response to the Growing Spam Problem", (2005) 20 *Berkeley Technology Law Journal* 301, 322; Rebecca BOLIN, "Opting Out of Spam: A Domain Level Do-Not-Spam Registry", (2006) 24 *Yale L. & Pol'y Rev.* 399, 414.

102 Groupe de travail sur le pourriel, *Comparaison des mesures internationales de lutte contre le pourriel*, mai 2005.

103 Voir les études citées dans: Lilly ZHANG, "The CAN-SPAM Act: An Insufficient Response to the Growing Spam Problem", (2005) 20 *Berkeley Technology Law Journal* 301, 325. Sur la perception du pourriel par les usagers, voir *CAN-SPAM a year later*, PIP Senior Research Fellow Deborah Fallows (202-419-4500), april 2005.

104 Michael GEIST, *Untouchable?: A Canadian Perspective on the Anti-Spam Battle*, version 1.1, May 2004, p. 6.

approches les plus efficaces pour contenir le pourriel[105]. Par la suite, des projets de lois ont été déposés au Parlement à l'initiative de parlementaires. Ces projets sont demeurés sans suite[106].

Le 11 mai 2004, le gouvernement du Canada annonce la mise sur pied d'un Groupe de travail spécial sur le pourriel pour coordonner la mise en œuvre du *Plan d'action anti-pourriel pour le Canada*[107], plan d'action exhaustif visant à réduire le volume des messages électroniques commerciaux non sollicités. Présidé par Industrie Canada, le Groupe de travail réunit des experts et des intervenants-clés représentant les fournisseurs de service Internet, les entreprises canadiennes qui utilisent le courriel à des fins commerciales légitimes et les consommateurs.

Dans son rapport intitulé *Freinons le pourriel : Créer un Internet plus fort et plus sécuritaire*, le Groupe de travail sur le pourriel convient que la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDÉ), la *Loi sur la concurrence* et le *Code criminel* sont des outils potentiellement utilisables pour lutter contre diverses facettes du pourriel. Cependant, le Groupe de travail note les difficultés de mise en application des lois : ressources limitées des organismes d'application, priorités conflictuelles limitant leur capacité d'intervention, pénurie d'experts-enquêteurs pour entreprendre des poursuites, sanctions inefficaces pour décourager les véritables contrevenants. Il souligne que ces dispositions législatives « ne peuvent être utilisées avec suffisamment de certitude pour contrer efficacement les méthodes et les moyens des polluposteurs, les intrusions plus agressives et envahissantes, ni les nouvelles menaces à la sécurité du réseau Internet »[108].

Le Groupe de travail recommande l'adoption d'une loi spécifique, neutre technologiquement, traitant du pourriel et des infractions liées au pourriel et aux nouvelles menaces et la modification des lois actuelles au besoin, des sanctions appropriées, un centre de responsabilité pour la surveillance et la coordination des politiques et des dispositions favorisant l'application des lois et la tenue d'enquêtes à l'échelle internationale. Dans le sillage des travaux du Groupe de travail, ont été publiés des documents de bonnes pratiques à l'intention des intervenants majeurs de l'industrie[109] et une campagne bilingue d'éducation des internautes canadiens a été mise sur pied[110].

Depuis le rapport du Groupe de travail sur le pourriel, aucune action concrète a été entreprise. Par exemple, l'article 41 de la *Loi sur les télécommunications*[111] qui permet au CRTC d'intervenir à l'égard du

---

105 INDUSTRIE CANADA, *Télémercatique: Offrir un choix au consommateur et créer des possibilités d'affaire*, document de discussion, janvier 2003, http://e-com.ic.gc.ca/epic/site/ecic-ceac.nsf/fr/gv00189f.html.

106 Voir: CANADA, SÉNAT, Projet de loi S-23, *Loi visant à empêcher la diffusion sur l'Internet de messages non sollicités*, 2e session, 37e législature, première lecture, 17 septembre 2003. Le 20 octobre 2004, le projet de loi fut réintroduit, voir Projet de loi S-15, *Loi visant à empêcher la diffusion sur l'Internet de messages non sollicités*, Première session, 38e législature, première lecture, 20 octobre 2004.

107 Industrie Canada, *Un plan d'action anti-pourriel pour le Canada*, mai 2004, < http://strategis.ic.gc.ca/epic/site/ecic-ceac.nsf/fr/h_gv00246f.html >.

108 Rapport du Groupe de travail sur le pourriel, *Freinons le pourriel-Créer un Internet plus fort et plus sécuritaire*, mai 2005, p. 14, < http://www.e-com.ic.gc.ca/epic/site/ecic-ceac.nsf/fr/h_gv00317f.html >.

109 *Pratiques exemplaires recommandées pour le marketing par courriel*, Groupe de travail sur le pourriel, Sous-groupe sur la validation du courriel commercial, Mai 2005, < http://e-com.ic.gc.ca/epic/site/ecic-ceac.nsf/fr/h_gv00348f.html >; *Pratiques exemplaires recommandées pour les fournisseurs de services Internet et autres exploitants de réseaux,* Groupe de travail sur le pourriel, Sous-groupe sur la gestion des technologies et des réseaux, mai 2005, http://e-com.ic.gc.ca/epic/site/ecic-ceac.nsf/fr/gv00347f.html.

110 Il s'agit de la campagne "Arrêtez le pourriel ici" qui met l'accent sur trois conseils: protégez votre ordinateur, protégez votre adresse électronique, protégez-vous; < http://arretezlepourrielici.ca/ >.

111 Art. 41 de la *Loi sur les télécommunications* (L.C. 1993, c. 38) : « Le Conseil 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 ».

pourriel sur Internet est demeuré lettre-morte. Il faut rappeler que le CRTC maintient une politique de non-intervention à l'égard d'Internet depuis son Ordonnance d'exemption sur les « nouveaux médias » de 1999[112].

Entre temps, les défenseurs du droit à la vie privée fédéraux, provinciaux et territoriaux se sont unis pour lutter contre la fraude, tel le vol d'identité[113]. En effet, le vol d'identité est considéré comme le crime du XXI[e] siècle. En 2006, près de 7 800 personnes ont signalé le vol de leur identité auprès du groupe anti•fraude PhoneBusters et les pertes financières s'élevaient à plus de 16 millions de dollars; et, cela ne représente probablement que 5 % des données réelles[114].

La commissaire à la protection de la vie privée du Canada et ses homologues ont convenu que pour être efficaces, les mesures contre le vol d'identité devaient être menées sur plusieurs fronts. Des sanctions plus sévères, pénales ou autres, pour mieux protéger les renseignements personnels, la mise en place de mesures de sécurité les plus efficaces pour protéger la vie privée de la part des entreprises, la sensibilisation et l'éducation des usagers [115] sont des exemples de mesures proposées.

Citant Spamhaus, où le Canada est classé au sixième rang des dix plus gros producteurs de pourriels, ils soulignent aussi l'importance de prendre des mesures pour endiguer l'énorme flux de pourriel:

> *Pourtant, à ce jour, le gouvernement fédéral n'a mis en œuvre aucune des recommandations émises par son groupe de travail sur le pourriel. Le Canada est maintenant le seul pays du G-8 qui ne dispose pas de loi antipourriel.*[116]

Et au fur et à mesure que les pays adoptent des lois strictes sanctionnant le pourriel, certains craignent que le Canada devienne un véritable refuge pour les polluposteurs s'il ne fait rien[117].

2. L'approche dite de « boîte à outils »

Étant donné la nature ouverte et décentralisée d'Internet, de nombreux pays reconnaissent que la lutte contre le pourriel, l'hameçonnage et les logiciels espions doit être envisagée comme un problème mondial. Il n'y a pas de solution unique et les pouvoirs publics et le secteur privé doivent agir de concert sur plusieurs plans.

---

112 Voir : CRTC, *Ordonnance d'exemption relative aux entreprises de radiodiffusion de nouveaux médias,* Avis public CRTC 1999-19, 17 décembre 1999, http://www.crtc.gc.ca/archive/FRN/Notices/1999/PB99-197.HTM

113 Commissariat à la protection de la vie privée du Canada, « Les défenseurs du droit à la vie privée s'unissent pour lutter contre la fraude », *Communiqué*, 1er mars 2007, http://www.privcom.gc.ca/id/release_070301_f.asp. Le Bureau de la concurrence s'est aussi joint à cet effort de concertation : Bureau de la concurrence, « Les Canadiens doivent riposter afin de faire obstacle à la fraude », *Communiqué de presse*, 1er mars 2007, < http://www.competitionbureau.gc.ca/internet/index.cfm?itemID=2283&lg=f>.

114 Cités dans Commissariat à la protection de la vie privée du Canada, « Les défenseurs du droit à la vie privée s'unissent pour lutter contre la fraude », *Communiqué*, 1er mars 2007, http://www.privcom.gc.ca/id/release_070301_f.asp.

115 À cette même occasion, la commissaire à la vie privée a publié des fiches d'information, destinées au public, décrivant divers types d'attaques frauduleuses et des moyens de se protéger contre elles. Commissariat à la protection de la vie privée du Canada, « Vos renseignements personnels sont une mine d'or pour le vol d'identité. Protégez-vous contre les fraudeurs », 1er mars 2007, < http://www.privcom.gc.ca/id/index_f.asp>.

116 Commissariat à la protection de la vie privée du Canada, « Les défenseurs du droit à la vie privée s'unissent pour lutter contre la fraude », *Communiqué*, 1er mars 2007, http://www.privcom.gc.ca/id/release_070301_f.asp.

117 Voir « Le Canada parmi les pires délinquants », *La Presse*, Section affaires, 14 mars 2007, pp.2-3, citant Michael Geist.

L'OCDE a réuni des experts pour constituer un Groupe de réflexion chargé de mettre en place un cadre pour lutter contre le spam en intégrant diverses solutions pluridisciplinaires. Ce groupe a retenu le concept de « boîte à outils » anti-spam :

> […] *reposant sur le principe selon lequel il faut mobiliser de façon ordonnée plusieurs éléments différents afin de favoriser le développement de stratégies et solutions de lutte contre le spam – techniques, réglementaires et d'application de la loi – et faciliter la coopération internationale face à ce problème.*[118]

La Boîte à outils contribue à la définition de stratégies anti-pourriel cohérentes aux échelons nationaux et internationaux et propose un ensemble de politiques et de mesures constituant des éléments clés d'un cadre global d'action publique pour s'attaquer au problème du pourriel.

Ainsi, « une approche multiple, de type "boîte à outils" », et mettant à contribution différents intervenants, approche similaire à celle qui a été préconisée par le Groupe de travail canadien, est considérée comme étant la plus efficace pour lutter contre le pourriel et résoudre d'autres problèmes en ligne[119].

L'approche « boîte à outils » est également préconisée en Europe. La Commission des communautés européennes présentait en 2004 une communication qui répertorie une série d'actions nécessaires pour compléter la réglementation de l'Union européenne et faire passer dans la réalité l'interdiction de pourriel[120]. On reconnaît que la législation à elle seule ne peut mettre fin au pourriel et que tous les acteurs concernés (États membres, autorités compétentes, consommateurs, utilisateurs d'Internet, entreprises) doivent jouer leur rôle. Ces mesures se complètent mutuellement; elles sont axées sur l'application effective des règles édictées par les États, des solutions techniques et de l'autorégulation mise en œuvre par les entreprises. Ces mesures sont complétées par des initiatives de sensibilisation des usagers et la coopération internationale.

En 2006, dans une nouvelle communication sur la lutte contre le pourriel, les espiogiciels et les logiciels malveillants, la Commission reconnaissait le caractère changeant des menaces. Non seulement la quantité de pourriel aurait considérablement augmenté au cours des cinq dernières années, mais il a de plus « cessé d'être une simple nuisance et devient peu à peu une activité de nature frauduleuse et délictueuse » avec le recours au courriels hameçons et la diffusion d'espiogiciels. Les actions prises par les États membres sont insuffisantes pour faire face à cette évolution. La Commission conclut :

> *Il faut intensifier les efforts pour faire appliquer la loi afin d'arrêter ceux qui l'enfreignent sciemment. Pour compléter les activités visant au respect de la loi, d'autres actions doivent être menées par les entreprises. Une coopération s'impose au niveau national, tant au sein de l'administration qu'entre l'administration et les entreprises. La Commission développera le dialogue et la coopération avec les pays tiers et étudiera aussi la possibilité de soumettre de nouvelles propositions législatives, de même qu'elle entreprendra des actions de recherche pour*

---

118 OCDE, *Rapport du Groupe de réflexion sur le spam de l'OCDE : Boîte à outils anti-spam de politiques et mesures recommandées,* 19 mai 2006, p. 18, DSTI/CP/ICCP/SPAM/(2005)3/FINAL.

119 Groupe de travail sur le pourriel, *Freinons le pourriel-Créer un Internet plus fort et plus sécuritaire*, Rapport du Groupe de travail sur le pourriel, Mai 2005, p. 29.

120 Commission des communautés européennes, *Communication de la Commission au Parlement européen, au Conseil , au Comité économique et social européen et au Comité des régions sur les communications commerciales non sollicitées ou "spam",* 22 janvier 2004, COM(2004) 28 final; Étienne WERY, «La Commission européenne déclare la guerre totale au spam :elle dévoile un plan d'attaque pluri-annuel, *Droit et Nouvelles technologies*, 30 janvier 2004, http://www.droit-technologie.org/1_2.asp?actu_id=883.

> *renforcer encore la protection de la vie privée et la sécurité dans le secteur des communications électroniques.*[121]

La Commission recommandait aux États membres de promouvoir activement le recours à la boîte à outils de l'OCDE sur l'application des législations contre le pourriel.

Les tendances dans la pratique internationale montrent une prédilection pour l'approche « boîte à outils » proposée par le Groupe de réflexion sur le spam de l'OCDE (19 mai 2006). Cette approche, résumée et présentée ici, suppose la mobilisation concertée de huit éléments interdépendants.

2.1 Une réglementation anti-pourriel

L'approche « boîte à outils » suppose l'existence de dispositions législatives anti-pourriel. C'est l'une des conditions nécessaires à la lutte efficace contre ce fléau mais ce n'est pas en soi suffisant.

Le Groupe de réflexion sur le spam de l'OCDE croit qu'il est essentiel d'élaborer une législation anti-pourriel, concise et simple, qui fixe les orientations claires et sans ambiguïté sur ce qui est autorisé et ce qui ne l'est pas, avec un régime de sanctions effectif et des modes adéquats d'administration de la preuve, et qui facilite la mise en place de partenariats internationaux de lutte contre le pourriel.

D'abord, il faut cerner le *champ d'application de la loi*, c'est-à-dire définir la base technologique du « spam ». La loi peut cibler les problèmes actuels et viser des technologies spécifiques de messages. Par exemple, la loi australienne vise les messages commerciaux électroniques non seulement par courriel, mais aussi par téléphone mobile (SMS), multimédia (MMS) et par la messagerie instantanée (IM). Une loi anti-pourriel peut aussi opter pour une approche législative technologiquement neutre qui demeurerait pertinente sur le long terme, en tenant compte de l'évolution des technologies de communications. Comme le souligne le rapport de l'OCDE, la législation doit être suffisamment flexible pour inclure les nouvelles formes de pourriel permises par une technologie de communication mais en même temps, il faut garder à l'esprit que toute action réglementaire sur une technologie de messagerie a des impacts non seulement sur les messages indésirables mais aussi sur les envois légitimes.[122]

Les législations anti-pourriel reposent généralement sur un même principe : les courriels à caractère commercial ne peuvent être envoyés qu'aux personnes et organisations qui consentent à recevoir ces messages. Les législations anti-pourriel se distinguent selon le *type de consentement* visé.

Comme le souligne le rapport de l'OCDE[123], une grande partie du débat sur le consentement s'est focalisé autour de l'opposition des modèles *opt-in* (consentement préalable : approche européenne) vs *opt-out* (droit de refus : approche américaine), alors qu'aujourd'hui, des approches plus complexes ou plus subtiles sont retenues (approche australienne). Les méthodes utilisées distinguent entre consentement explicite, consentement implicite, consentement présumé ou une combinaison de ces concepts.

Le consentement explicite est celui où l'individu donne activement son consentement à une action (ex : formulaire où on consent à l'envoi ultérieur de messages commerciaux, case à cocher où on indique notre volonté de recevoir des messages commerciaux, etc.). Le consentement implicite est déduit de l'attitude

---

121 Commission des communautés européennes, *Communication de la Commission au Parlement européen, au Conseil , au Comité économique et social européen et au Comité des régions sur la lutte contre le pourriel, les espiogiciels et les logiciels malveillants,* 15 novembre 2006, COM(2006) 688 final, pp. 12-13.

122 OCDE, *Rapport du Groupe de réflexion sur le spam de l'OCDE : Boîte à outils anti-spam de politiques et mesures recommandées,* 19 mai 2006, DSTI/CP/ICCP/SPAM/(2005)3/FINAL, p. 29.

123 OCDE, Groupe de réflexion sur le spam, *La réglementation anti-spam*, 24 novembre 2005, DSTI/CP/ICCP/SPAM/(2005) 10/FINAL, p. 18.

du destinataire ou de ses relations commerciales antérieures avec l'expéditeur (client, partenaire commercial, abonné, etc)[124]. Dans les législations basées sur le consentement présumé ou droit de retrait, comme aux USA, *il y a présomption de consentement tant que le destinataire n'a pas retiré son consentement, par exemple en se « désabonnant » ou en inscrivant son adresse électronique sur une liste « ne pas poster » lorsque la loi prévoit cette possibilité*[125] .

Le Groupe de réflexion sur le spam relève l'émergence d'approches hybrides ou circonstancielles du consentement comme en Australie où dans certaines situations, la loi exige un consentement explicite et dans d'autres, un consentement implicite suffit, lorsqu'il peut être déduit de la conduite ou d'une relation commerciale ou autre antérieure. Par exemple, si une personne publie en ligne ou dans un annuaire son adresse électronique dans le cadre de son travail, elle est supposée avoir consenti à recevoir des messages ayant un lien avec son activité professionnelle[126]. Ces approches, plus complexes, créent davantage de consensus entre les groupes anti-pourriel et l'industrie de marketing en ligne.

Un des éléments fondamentaux d'une législation anti-pourriel fondée sur le consentement est d'offrir la possibilité au destinataire de révoquer son consentement. Une *fonction de « désabonnement »* doit inclure une adresse de réponse valide permettant au destinataire d'indiquer qu'il ne désire plus recevoir de messages. La loi doit prévoir un délai pour que l'expéditeur obtempère à la demande et des sanctions s'il ne cesse pas l'envoi de messages après le délai imparti. Encore là, le Groupe de réflexion reconnaît les limites dans l'application d'une telle disposition pour les polluposteurs « professionnels ». [127]

Une législation, pour enrayer le « spam » en tant que véhicule de virus, de hameçonnage ou de messages frauduleux, doit interdire l'envoi de messages électroniques dont les *informations d'identité ou d'origine* sont falsifiées. Il s'agit là, selon le Groupe de réflexion sur le spam, d'une des dispositions essentielles, mais en même temps, des plus difficiles à appliquer puisque « si l'expéditeur a masqué ou falsifié les informations de l'en-tête, il est difficile à identifier pour une autorité de police »[128]. De là l'importance de compléter et renforcer l'approche législative en dotant les autorités policières d'expertise technique, en facilitant la recevabilité de la preuve physique et financière pour l'application des lois anti-pourriel et en engageant des poursuite contre les contrevenants.

Une législation anti-pourriel peut également choisir d'interdire *l'envoi de masse* en fixant le nombre de messages au-delà duquel les messages sont considérés comme du pourriel[129]. Elle peut aussi imposer l'utilisation de *l'étiquetage* spécifique dans l'en-tête ou dans le sujet du message pour identifier certaines catégories de messages comme la publicité (ADV) ou les contenus réservés aux adultes (ADLT). Quoique facilitant les systèmes de filtrage, cette option présente plusieurs limites, la plus importante étant que les polluposteurs invétérés ne se plient à cette règle.

---

124 OCDE, Groupe de réflexion sur le spam, *La réglementation anti-spam*, 24 novembre 2005, DSTI/CP/ICCP/SPAM/(2005) 10/FINAL, p. 20.

125 OCDE, Groupe de réflexion sur le spam, *La réglementation anti-spam*, 24 novembre 2005, DSTI/CP/ICCP/SPAM/(2005) 10/FINAL, p. 20.

126 OCDE, Groupe de réflexion sur le spam, *La réglementation anti-spam*, 24 novembre 2005, DSTI/CP/ICCP/SPAM/(2005) 10/FINAL, p. 20.

127 OCDE, *Rapport du Groupe de réflexion sur le spam de l'OCDE : Boîte à outils anti-spam de politiques et mesures recommandées,* 19 mai 2006, DSTI/CP/ICCP/SPAM/(2005)3/FINAL, p. 32. De tels dispositifs de désabonnement sont prévus dans les lois américaine, australienne et dans la directive européenne.

128 OCDE, *Rapport du Groupe de réflexion sur le spam de l'OCDE : Boîte à outils anti-spam de politiques et mesures recommandées,* 19 mai 2006, DSTI/CP/ICCP/SPAM/(2005)3/FINAL, p. 33.

129 OCDE, Groupe de réflexion sur le spam, *La réglementation anti-spam*, 24 novembre 2005, DSTI/CP/ICCP/SPAM/(2005) 10/FINAL, p. 22 et suivantes. On reconnaît que cette option est arbitraire car tous les messages envoyés en masse ne sont pas nécessairement du pourriel et un message unique non sollicité peut être considéré comme du pourriel.

Comme le constate le Groupe de réflexion sur le spam, une campagne de pourriel n'est plus limitée à une manœuvre entre un polluposteur et un destinataire. Un ensemble d'intermédiaires peut s'interposer entre la personne (souvent via un ordinateur contrôlé par un cheval de Troie) qui est physiquement responsable de l'envoi et celle qui décide et bénéficie de cet envoi. Une législation devrait sanctionner les personnes qui prennent part à la manœuvre, i.e. la personne physique qui envoie le message mais aussi celle qui en retire un gain financier[130]. En terme de répression, il est plus facile d'identifier celui qui bénéficie de la manœuvre que celui qui l'envoie effectivement. De même, l'utilisation de *logiciels collecteurs d'adresses ou d'attaques par dictionnaire* liée à l'envoi de pourriel devrait être interdite.

L'utilisation délictuelle des ressources informatiques protégées doit être interdite[131]. En effet, il a été constaté que les polluposteurs font appel à de nouvelles stratégies pour envoyer leurs messages ou pour en falsifier l'origine, tels les « botnets » et les réseaux de zombies. Cependant, constate le Groupe de réflexion, de nombreux pays ont une loi touchant ce délit ou ont mis en œuvre l'article 2 de la Convention du Conseil de l'Europe sur la cybercriminalité qui couvre *l'accès illicite* à un système informatique.

D'abord considéré comme une technique de marketing agaçante, le pourriel est de plus en plus envisagé comme vecteur de manœuvres frauduleuses comme l'hameçonnage, la fraude et la diffusion de virus, de vers ou de logiciel espions. C'est alors le contenu du message qui est trompeur ou frauduleux ou qui porte *atteinte à la sécurité*. Généralement, ces délits sont couverts par les lois générales concernant la lutte contre la fraude ou la pornographie ou la protection du consommateur. Le Groupe de réflexion souligne que certains pays, comme la France, ont cependant préféré modifier ces normes afin de tenir compte des nouvelles menaces sur Internet[132]. La Convention sur la cybercriminalité est également un outil international pour répondre d'une façon coordonnée et harmonisée à ce fléau.

Enfin, comme toute activité conduite sur Internet, le pourriel pose des difficultés d'application des lois nationales. Comme le constate le Groupe de réflexion, il est difficile d'imposer la législation interne à un message de pourriel provenant de l'extérieur du territoire du destinataire, de même les autorités nationales n'ont pas toujours compétence sur un message de pourriel en provenance de leur territoire mais envoyé vers un autre pays[133]. Des éléments de *compétence extraterritoriale* peuvent être prévus dans une loi anti-pourriel pour que les mesures soient réellement applicables par les tribunaux nationaux. Par exemple, une loi anti-pourriel doit prévoir que les messages émis depuis la juridiction ou à destination de celle-ci sont couverts par la loi ainsi que les messages dont l'expédition a été commandée à l'intérieur de la juridiction. Dans la mise en œuvre, une telle législation doit aussi « permettre des accords internationaux en la matière, et faciliter l'application transnationale au niveau opérationnel (échange d'informations, coopération dans les enquêtes)»[134]. Par exemple, plusieurs régulateurs intensifient leurs efforts et se sont entendus sur un cadre de coopération internationale relative à l'application des lois anti-pourriel, le Plan d'action de Londres[135].

Le Groupe de réflexion reconnaît les limites de l'approche législative et la nécessité de la compléter avec d'autres outils, entre autres des pouvoirs d'investigation et d'exécution suffisants pour les autorités

---

130 OCDE, *Rapport du Groupe de réflexion sur le spam de l'OCDE : Boîte à outils anti-spam de politiques et mesures recommandées,* 19 mai 2006, DSTI/CP/ICCP/SPAM/(2005)3/FINAL, p. 34.

131 OCDE, *Rapport du Groupe de réflexion sur le spam de l'OCDE : Boîte à outils anti-spam de politiques et mesures recommandées,* 19 mai 2006, DSTI/CP/ICCP/SPAM/(2005)3/FINAL, p. 35.

132 OCDE, *Rapport du Groupe de réflexion sur le spam de l'OCDE : Boîte à outils anti-spam de politiques et mesures recommandées,* 19 mai 2006, DSTI/CP/ICCP/SPAM/(2005)3/FINAL, p. 36 et note 33.

133 OCDE, *Rapport du Groupe de réflexion sur le spam de l'OCDE : Boîte à outils anti-spam de politiques et mesures recommandées,* 19 mai 2006, DSTI/CP/ICCP/SPAM/(2005)3/FINAL, p. 37.

134 OCDE, *Rapport du Groupe de réflexion sur le spam de l'OCDE : Boîte à outils anti-spam de politiques et mesures recommandées,* 19 mai 2006, DSTI/CP/ICCP/SPAM/(2005)3/FINAL, p. 38.

135 Voir la section 2.8 *La coopération mondiale*, dans cette deuxième partie du rapport.

compétentes, de l'information au consommateur et des codes de conduite et de pratiques exemplaires pour les fournisseurs de services Internet et les associations professionnelles qui soient compatibles avec la législation.

2.2 La répression du pourriel

L'application et la mise en œuvre de la législation, particulièrement la promptitude de la répression et l'application des sanctions, sont très importantes dans un contexte où les polluposteurs agissent très rapidement et peuvent transférer leurs opérations au besoin[136].

Plusieurs législations sectorielles en vigueur dans les pays peuvent s'appliquer à un aspect ou à un autre du pourriel : lois sur la protection de la vie privée, sur la protection du consommateur, sur les fraudes et la sécurité informatique, sur la pornographie, sur les contenus faux ou mensongers etc. Plusieurs organismes nationaux, avec des priorités et des pouvoirs différents, sont susceptibles de s'occuper de pratiques liées au pourriel. Le Groupe de réflexion sur le spam de l'OCDE croit qu'il faut agir sur la coordination nationale en renforçant la coopération inter-organismes et désigner un organisme pour assurer la liaison nécessaire et mettre en commun leur information et leurs ressources[137].

Les autorités d'exécution doivent aussi disposer, selon le Groupe de réflexion, de pouvoirs suffisants de perquisition et de saisie des éléments de preuve électroniques et appliquer les sanctions avec diligence et célérité[138]. Les sanctions doivent être suffisamment sévères pour décourager les polluposteurs et en fonction de la gravité des délits (avertissement, injonction, amendes administratives, civiles ou pénales et dans certains cas l'emprisonnement). Étant donné que le préjudice subi par le destinataire de pourriel est difficile à évaluer, une loi peut mettre en place un droit de recours privé lui permettant d'obtenir réparation.

Comme déjà mentionné, la répression du pourriel passe par la coopération et la mise en commun de l'information étant donné les difficultés liées à la collecte et à la préservation de la preuve lorsque le pourriel traverse les frontières. Cette coopération peut prendre la forme d'accords bilatéraux, de mécanismes tel le Plan d'action de Londres qui crée un réseau multilatéral de répression internationale du pourriel, de projets qui encouragent l'échange d'informations et la coordination entre les secteurs public et privé, de création de réseau de contacts des autorités anti-pourriel etc. Évidemment, cela doit être complété par une coopération transnationale en matière de répression du pourriel. [139]

---

136 OCDE, *Rapport du Groupe de réflexion sur le spam de l'OCDE : Boîte à outils anti-spam de politiques et mesures recommandées,* 19 mai 2006, DSTI/CP/ICCP/SPAM/(2005)3/FINAL, p. 41.

137 OCDE, *Rapport du Groupe de réflexion sur le spam de l'OCDE : Boîte à outils anti-spam de politiques et mesures recommandées,* 19 mai 2006, DSTI/CP/ICCP/SPAM/(2005)3/FINAL, pp. 41-42.

138 Le Groupe de réflexion note, à la page 42, que la Convention sur la cybercriminalité propose un cadre procédural pour les enquêtes dans ce domaine et contient des dispositions sur la préservation, la perquisition et la saisie de preuves de nature électronique (*Convention sur la cybercriminalité*, STCE n° 185, < http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CL=FRE>)

139 Son cités, entre autres, les mécanismes et initiatives d'application transfrontière des lois suivants: L'initiative Spotspam, issue d'un partenariat public/privé, vise à construire une base de données facilitant les enquêtes et l'application transfrontière de la loi en matière de pourriel. Le Réseau de contact des autorités anti-spam (CNSA), créé par la Commission européenne pour échanger les meilleures pratiques en matière d'application transfrontière des lois, a établi une procédure pour faciliter le traitement transfrontière des plaintes relatives au pourriel. Un formulaire de transmission de plainte relative au pourriel a été élaboré par les autorités du Plan d'action de Londres et le CNSA pour faciliter la transmission d'une demande d'enquête d'une autorité à l'autre. L'OCDE a aussi adopté, en avril 2006, une recommandation relative à la coopération transfrontière dans l'application des législations contre le pourriel invitant les autorités chargées d'appliquer la loi à s'échanger de l'information et à collaborer. Ces deux derniers documents sont reproduits aux annexes 1 et 5 du rapport du Groupe de réflexion sur le spam. OCDE, *Rapport du Groupe de réflexion sur le spam de l'OCDE : Boîte à outils anti-spam de politiques et mesures recommandées,* 19 mai 2006, DSTI/CP/ICCP/SPAM/(2005)3/FINAL, p. 45.

2.3 Les initiatives anti-pourriel du secteur privé

Une législation anti-pourriel peut manquer de la flexibilité requise pour tenir compte de la rapidité des progrès technologiques selon le Groupe de réflexion sur le spam[140]. Elle doit être jumelée à des initiatives d'autorégulation engagées par des acteurs du secteur privé, comme les fournisseurs d'accès Internet (ex : code de conduite et conditions générales d'utilisation, pratiques exemplaires de sécurité des réseaux, outils éducatifs et informations aux clients, mise à disposition de filtres anti-pourriel, mesures techniques etc). Les fournisseurs d'accès Internet, par la position qu'il occupent, jouent un rôle important dans la lutte anti-pourriel et plusieurs *pensent que le problème des « botnets » et des ordinateurs « zombies » peut être résolu, ou tout au moins limité, en mettant en oeuvre les meilleures pratiques en matière de sécurité, en appliquant des CGU* [conditions générales d'utilisation] *et en formant les internautes à tirer parti des outils à leur disposition pour protéger leurs ordinateurs*[141].

Les banques, institutions financières et autres opérateurs en ligne doivent également élaborer des politiques, des pratiques exemplaires harmonisées de communication par courrier électroniques et agir à plusieurs niveaux pour prévenir la fraude par hameçonnage (ex : méthodes et normes de communication d'entreprise pour les sites web, activités de blocage destinées à faire obstacle à l'hameçonnage, éducation et sensibilisation des clients quant aux types de communications susceptibles d'être acheminées par voie électroniques).

Les diverses associations professionnelles, qui représentent les intérêts soit des sociétés de marketing direct, des cyberentreprises, des sociétés de logiciels, des fournisseurs d'accès Internet etc. ont un rôle actif à jouer dans la lutte anti-pourriel. Elles sont actives pour défendre les intérêts communs, mettre en place les meilleures pratiques, faciliter la coopération et faire face de façon concertée à un problème touchant le service faisant l'objet de leurs activités.

Par exemple, les associations de marketing direct, dont les sociétés ont recours à l'envoi massif de courriel et doivent se conformer aux législations anti-pourriel, ont élaboré des codes de conduite et des pratiques exemplaires qui offrent une garantie de respect des dispositions législatives applicables pour ceux qui y adhèrent[142].

Également le Messaging Anti-Abuse Working Group (MAAWG) (Groupe de travail contre les abus des messageries électroniques) est une coalition mondiale qui regroupe des sociétés de télécommunications et des fournisseurs d'accès Internet qui se voue à éliminer les abus de messageries en encourageant des solutions techniques, la collaboration entre les professionnels et l'expression d'opinion auprès des pouvoirs publics. Dans le cadre des travaux du Groupe de réflexion sur le spam de l'OCDE, le MAAWG et le BIAC[143] ont proposé un ensemble de pratiques exemplaires à l'intention des fournisseurs de services

---

140 OCDE, *Rapport du Groupe de réflexion sur le spam de l'OCDE : Boîte à outils anti-spam de politiques et mesures recommandées,* 19 mai 2006, DSTI/CP/ICCP/SPAM/(2005)3/FINAL, pp. 46-54.

141 OCDE, *Rapport du Groupe de réflexion sur le spam de l'OCDE : Boîte à outils anti-spam de politiques et mesures recommandées,* 19 mai 2006, DSTI/CP/ICCP/SPAM/(2005)3/FINAL, p. 47.

142 Au Canada, voir le *Code de déontologie et les normes de pratiques* de l'Association canadienne du marketing, < http://www.the-cma.org/french/?WCE=C=47|K=225885#13>. Par exemple, les agents de marketing doivent promouvoir des pratiques responsables et transparentes de gestion des renseignements personnels d'une manière conforme aux dispositions de la Loi fédérale sur la protection des renseignements personnels et les documents électroniques ou de la loi provinciale qui s'applique et qui sont détaillées dans le code. Ce code s'applique au marketing par courriel et à la collecte en ligne de données. Le Sous-groupe sur la validation du courriel commercial, mis sur pied par le Groupe de travail sur le pourriel du gouvernement canadien, a élaboré une série de pratiques exemplaires fondées sur les divers codes existants et destinées à servir de référence pour l'usage du courriel à des fins de marketing ; Voir Appendice C, *Pratiques exemplaires recommandées pour le marketing par courriel*, dans Rapport du Groupe de travail sur le pourriel, *Freinons le pourriel-Créer un Internet plus fort et plus sécuritaire*, mai 2005, < http://www.e-com.ic.gc.ca/epic/site/ecic-ceac.nsf/fr/h_gv00317f.html>.

143 Le BIAC (Business and Industry Advisory Committee) est le comité consultatif économique et industriel auprès de l'OCDE. Cet organisme indépendant est le représentant officiel du milieu des affaires des pays membres de l'OCDE. <www.biac.org>.

d'accès Internet et des opérateurs de réseaux. Ces pratiques représentent « un ensemble de principes volontaires élaborés par les milieux des affaires dont la finalité est de renforcer la sécurité des infrastructures des réseaux dans la lutte contre le spam »[144].

Le MAAWG s'est aussi associé à l'Anti-Phishing Working Group (APWG), pour élaborer des pratiques exemplaires, de nature technique et commerciale, pour combattre l'hameçonnage à l'intention des fournisseurs de services Internet et de courriels[145]. Mentionnons que le Anti-Phishing Working Group (APWG) est une association professionnelle (institutions financières, fournisseurs de services Internet, développeurs de logiciels etc.) dont l'objectif est de faire échec au vol d'identité et à la fraude résultant du problème croissant de l'hameçonnage et de la falsification de courriels. [146]

Dans la même foulée au Canada, dans le cadre des travaux du Groupe de travail sur le pourriel, des pratiques exemplaires techniques ont été élaborées et recommandées pour les fournisseurs de services Internet et les autres exploitants de réseaux afin de réduire le volume de pourriel[147].

2.4 Les solutions techniques

L'utilisation et l'administration rationnelles d'un éventail d'outils et de technologies anti-pourriel (filtrage et autres) peut réduire considérablement le volume de pourriel. Selon le Groupe de réflexion sur le spam de l'OCDE, la technologie est un élément de la stratégie globale anti-pourriel, au même titre que les mesures publiques, les pratiques et la sensibilisation[148].

2.5 L'information et la sensibilisation

L'utilisateur, qui est le destinataire du pourriel et la victime potentielle, a le contrôle sur son ordinateur et sur son information personnelle. L'information et la sensibilisation de l'utilisateur sont des éléments importants d'une stratégie anti-pourriel étant donné que même un très faible taux de réponse à un pourriel peut être profitable pour un polluposteur. L'utilisateur doit être suffisamment informé et sensibilisé afin de faire face aux menaces d'Internet.

Comme le souligne le Groupe de réflexion sur le spam, les activités d'éducation et de sensibilisation doivent s'adresser, non seulement à l'utilisateur individuel, mais aussi aux grandes entreprises, aux PME, aux établissements d'enseignement et doivent « créer une culture de la sécurité, et [...] encourager une utilisation responsable du cyberespace »[149].

Concernant les particuliers, les autorités publiques peuvent organiser des campagnes d'information et de sensibilisation du public pour les éduquer sur les risques associés aux activités sur Internet et les moyens de s'en protéger. Par exemple, des ressources pédagogiques de différents pays sont mises à la disposition

---

144 OCDE, *Rapport du Groupe de réflexion sur le spam de l'OCDE : Boîte à outils anti-spam de politiques et mesures recommandées,* 19 mai 2006, *Annexe II: Pratiques exemplaires préconisées par le BIAC et le MAAWG à l'intention des fournisseurs d'accès Internet et opérateurs de réseaux*, p. 90, DSTI/CP/ICCP/SPAM/(2005)3/FINAL.

145 MAAWG, *Global Best Practices to Fight Online "Phishing" Crime Jointly Approved By APWG & MAAWG*, 25 juillet 2006, < http://www.maawg.org/news/MAAWG060725.pdf>

146 Anti-Phishing Working Group (APWG),< http://www.antiphishing.org/>.

147 Appendice B, *Pratiques exemplaires recommandées pour les fournisseurs de service Internet et les autres exploitants de réseaux*, dans Rapport du Groupe de travail sur le pourriel, *Freinons le pourriel-Créer un Internet plus fort et plus sécuritaire*, mai 2005, < http://www.e-com.ic.gc.ca/epic/site/ecic-ceac.nsf/fr/h_gv00317f.html>.

148 OCDE, *Rapport du Groupe de réflexion sur le spam de l'OCDE : Boîte à outils anti-spam de politiques et mesures recommandées,* 19 mai 2006, DSTI/CP/ICCP/SPAM/(2005)3/FINAL, p. 54.

149 OCDE, *Rapport du Groupe de réflexion sur le spam de l'OCDE : Boîte à outils anti-spam de politiques et mesures recommandées,* 19 mai 2006, DSTI/CP/ICCP/SPAM/(2005)3/FINAL, p. 8 et pp. 69-74.

d'organismes via la Boîte à outils anti-spam de l'OCDE. Les fournisseurs d'accès Internet peuvent utiliser leurs canaux de communication avec leurs clients (pages web, politiques d'utilisation acceptable) pour les informer sur les façons d'éviter le pourriel, l'usage de filtres, les modalités pour signaler les cas de pourriel etc.

Et, comme le souligne le rapport du Groupe de réflexion sur le spam, « l'éducation des destinataires est aussi importante que celle des expéditeurs »[150]. Par exemple, en matière de hameçonnage, une solution implique la mise en œuvre de mesures techniques pour limiter le fléau, l'élaboration d'initiatives d'éducation et de sensibilisation des consommateurs mais aussi un effort des opérateurs en ligne pour établir des pratiques claires de communication par courrier électronique avec leurs clients.

2.6 Les partenariats en coopération contre le pourriel

Une stratégie anti-pourriel doit être intégrée dans un cadre de partenariat public/privé. Les mesures anti-pourriel (ex : les pratiques exemplaires) seront efficaces s'il y a coopération des secteurs public/privé i.e. si l'ensemble des acteurs les ont élaborées, les ont acceptées et les considèrent adaptées à leurs besoins[151].

Les partenariats public/privé facilitent souvent l'éducation, la sensibilisation et l'échange d'informations et de données sur les cas de pourriels transfrontières. La coopération entre les secteurs public et privé sous-tend l'ensemble des initiatives anti-pourriel. Comme le souligne le Groupe de réflexion sur le spam « des partenariats stratégiques comme ceux qui se mettent en place dans les différents groupes de travail créés aux échelons national et international sont un outil fondamental pour améliorer la communication et mieux comprendre les besoins, les attentes et les problèmes réciproques et, ce faisant, permettre un renforcement de la coopération et de l'engagement mutuel. »[152] Par exemple, le Plan d'action de Londres, qui crée un réseau multilatéral de répression internationale du pourriel, est un partenariat public/privé « particulièrement dynamique » dont l'un des objectifs est de « faciliter les contacts entre les services chargés de faire respecter les mesures, de promouvoir l'échange d'informations dans les actions transnationales et d'intensifier la coopération avec les FAI et autres opérateurs privés »[153].

2.7 La mesure du pourriel

La mesure du pourriel, par les autorités publiques et les acteurs privés nationaux, est un élément important pour évaluer l'évolution du phénomène, l'impact des différentes initiatives ou efforts de répression, réglementaires ou autres, et les ajustements qui doivent être apportés[154].

Dans le cadre des travaux du Groupe de réflexion sur le spam de l'OCDE, le MAAWG (Messaging Anti-Abuse Working Group) a élaboré un programme de métrologie du courrier électronique, une méthode de mesure de la quantité de pourriels qui circulent dans le réseau.

---

150 OCDE, *Rapport du Groupe de réflexion sur le spam de l'OCDE : Boîte à outils anti-spam de politiques et mesures recommandées,* 19 mai 2006, DSTI/CP/ICCP/SPAM/(2005)3/FINAL, p. 16.

151 OCDE, *Rapport du Groupe de réflexion sur le spam de l'OCDE : Boîte à outils anti-spam de politiques et mesures recommandées,* 19 mai 2006, DSTI/CP/ICCP/SPAM/(2005)3/FINAL, p. 16.

152 OCDE, *Rapport du Groupe de réflexion sur le spam de l'OCDE : Boîte à outils anti-spam de politiques et mesures recommandées,* 19 mai 2006, DSTI/CP/ICCP/SPAM/(2005)3/FINAL, p. 76.

153 OCDE, *Rapport du Groupe de réflexion sur le spam de l'OCDE : Boîte à outils anti-spam de politiques et mesures recommandées,* 19 mai 2006, DSTI/CP/ICCP/SPAM/(2005)3/FINAL, p. 76.

154 Voir OCDE, *Rapport du Groupe de réflexion sur le spam de l'OCDE : Boîte à outils anti-spam de politiques et mesures recommandées,* 19 mai 2006, DSTI/CP/ICCP/SPAM/(2005)3/FINAL, pp. 78-81.

2.8 La coopération mondiale

La coopération mondiale (partenariats-mécanismes bilatéraux ou multilatéraux, échange d'informations-) est primordiale pour la mise en place harmonisée et l'application généralisée de mesures anti-pourriel afin de contrer ce phénomène. Ainsi, le Sommet mondial sur la société de l'information tenu à Genève en 2003, puis à Tunis en 2005, a appelé à une action concertée afin de lutter contre les diverses formes de fléaux d'Internet dont le pourriel.

Ainsi, le paragraphe 41 de l'*Agenda de Tunis pour la société de l'information* déclare que :

> ***Nous sommes résolus à traiter efficacement*** *le problème toujours plus préoccupant du spam.* ***Nous prenons note*** *des cadres multilatéraux et multi-parties prenantes de coopération régionale et internationale qui existent afin de lutter contre le spam, par exemple, la stratégie antispam de l'APEC, le Plan d'action de Londres, le Mémorandum d'accord Séoul-Melbourne sur la lutte contre le spam et les activités menées par l'OCDE et l'UIT dans ce domaine.* ***Nous demandons*** *à toutes les parties prenantes d'adopter des mesures sur plusieurs fronts pour lutter contre ce phénomène: sensibilisation des utilisateurs et des entreprises; mise en place d'une législation appropriée ainsi que de services et de mécanismes adaptés pour la faire appliquer; poursuite de la mise au point de mesures techniques et d'autoréglementation; bonnes pratiques; coopération internationale.*[155]

Dans cet esprit, l'Organisation de coopération économique Asie-Pacifique (APEC), le Réseau de contact européen des autorités anti-spam (CNSA), le Plan d'action de Londres, l'Union internationale des télécommunications (UIT), l'OCDE de même que le Seoul-Melbourne Anti-Spam Group ont mis sur pied le « stopspamalliance.org ». Le site « stopspamalliance.org » assure le réseautage entre les principales initiatives mondiales de lutte contre les diverses formes de pourriel. On y tient une veille sur les initiatives législatives et les autres mécanismes mis en place et surtout sur les activités de répression des pratiques nuisibles. Par exemple, la Boîte à outils et les diverses pratiques exemplaires élaborées par le Groupe de réflexion sur le spam de l'OCDE sont ainsi mises à la disposition de l'ensemble des pays.

Les formes plus élaborées de coopération passent par des formules bilatérales souples qui, sans aller jusqu'à créer des obligations impératives pour les États, engagent les participants à s'entraider dans la répression des pratiques nuisibles, à partager des informations et des technologies[156]. Ainsi, les autorités des États-Unis et de l'Union européenne ont convenu de coopérer dans l'application des mesures de lutte contre le pourriel.

D'autres initiatives, qui se veulent plus pratiques, fonctionnent selon des modes informels. Ainsi, le Plan d'action de Londres[157], instituant un forum international des autorités de lutte contre le pourriel, rejoint des intervenants sur cinq continents dont 62 agences de lutte anti-pourriel dans plus de 30 pays, comme les États-Unis, la Chine et le Nigeria. Tous les organismes qui souhaitent contribuer à la lutte internationale contre le pourriel peuvent s'associer au Plan d'action de Londres. Il leur suffit d'accepter

---

155 Deuxième phase du SMSI (16-18 novembre 2005, Tunis), *Agenda de Tunis pour la société de l'information*,WSIS-05/TUNIS/DOC/6 (rev. 1), <http://www.itu.int/wsis/documents/doc_multi.asp?lang=fr&id=2267|0 >.

156 Meyer POTASHMAN, "International Spam Regulation & Enforcement: Recommendations Following the World Summit on the Information Society," [2006] 29 *Boston College International & Comparative Law Rev.,* 323, p. 345.

157 Les projets concrets du Plan d'action de Londres incluent la sensibilisation des grandes entreprises et des fournisseurs d'accès Internet grâce à des opérations d'éducation comme "Opération Zombies", l'échange de bonnes pratiques pour identifier les origines du pourriel, la facilitation et la mise en place de procédures de coopération entre les régulateurs, et entre les régulateurs et l'industrie et enfin, les opérations conjointes de lutte anti-pourriel comme des opérations de balayage de spam. Tirés de *Plan d'action de Londres*, < http://www.londonactionplan.org/?q=node/22>.

les lignes directrices du Plan d'action puis de contacter le secrétariat informel du Plan, soit l'Office of Fair Trading (OFT), qui est le bureau de la concurrence britannique. L'OFT soumet alors la description de l'organisme-candidat et ses activités aux autres signataires, et si aucune question ou objection n'est soulevée, l'organisme-candidat peut, sans autre formalité, devenir membre et prendre part aux activités. Les participants proviennent de secteurs variés comme les agences de protection de la vie privée, les agences de protection des consommateurs ou les agences de réglementation des télécommunications. De nombreuses sociétés commerciales d'envergure internationale ont également rejoint le Plan d'action de Londres.

De son côté, la Commission européenne a mis en place le Réseau de contact des autorités anti-spam (CNSA). Le réseau assure l'échange des meilleures pratiques et la coopération dans l'application transfrontières des lois. Il a, entre autres, établi un processus afin de faciliter le traitement transfrontière des plaintes relatives au pourriel. Ce réseau est également animé par l'Office of Fair Trading britannique.

D'autres organisations internationales comme l'Union internationale des télécommunications (UIT)[158] et l'Organisation de coopération économique Asie-Pacifique (APEC) ont mis sur pied des activités de lutte contre le pourriel ou ont élaboré des travaux liés à l'application des lois[159].

Enfin, les organisations du secteur privé jouent aussi un rôle important dans la lutte anti-pourriel à l'échelle mondiale. L'élaboration de pratiques exemplaires par le Messaging Anti-Abuse Working Group (MAAWG) et le Anti-Phishing Working Group (APWG) en est un exemple.

158 < http://www.itu.int/osg/spu/spam/>

159 Voir OCDE, Groupe de réflexion sur le spam, *Rapport sur l'application des lois antispam*, 30 août 2005, DSTI/CP/ICCP/SPAM(2004)3/FINAL, p. 31.

TROISIÈME PARTIE
ANALYSE DU CADRE RÉGLEMENTAIRE QUÉBÉCOIS DU POURRIEL, DE L'HAMEÇONNAGE ET DES LOGICIELS ESPIONS

Afin d'éviter de longues et inutiles répétitions, nous avons omis d'inclure dans ce texte les recours civils possibles. Retenons que la plupart des gestes énumérés ci-dessous sont susceptibles de constituer une faute au sens de l'article 1457 C.c.Q. et d'engager la responsabilité de leur auteur.

Deux tableaux placés à la fin de cette partie résument les lois applicables à ces gestes.

1. Le pourriel et l'hameçonnage

Les notions de pourriel et d'hameçonnage couvrent un vaste ensemble de situations. Les évolutions d'Internet transforment constamment les contextes dans lesquels se déroulent les diverses pratiques abusives ou malhonnêtes. De pratique simplement gênante, le pourriel est devenu un vecteur pour des activités frauduleuses comme l'hameçonnage : la réalité concrète de l'activité de même que ses conséquences peuvent emporter l'application de plusieurs dispositions ne portant pas au départ sur le pourriel en tant que tel. C'est pourquoi il faut se garder d'envisager le cadre réglementaire de ces phénomènes comme si cela visait des gestes bien délimités.

Tant qu'il n'y a pas de législations visant directement le pourriel et l'hameçonnage, ce sont des législations à portée générale ou réglementant des secteurs spécifiques d'activités qui ont vocation à s'appliquer à l'encontre de plusieurs gestes inhérents aux pratiques des polluposteurs et hameçonneurs.

1.1 La collecte d'adresses

Il est nécessaire pour les polluposteurs d'obtenir des listes d'adresses courriel valides afin de mener à bien leurs activités.

Au Québec, la *Loi sur la protection des renseignements personnels dans le secteur privé*[160] prévoit, à titre de principe, qu'une entreprise qui collecte des informations personnelles sur une personne physique doit le faire auprès de la personne concernée elle-même (art. 6). Dès lors, il est utile de se demander si une adresse courriel constitue un « renseignement personnel » au sens de la loi. L'article 2 de la *Loi sur la protection des renseignements personnels dans le secteur privé* définit qu'est un renseignement personnel « tout renseignement qui concerne une personne physique et permet de l'identifier ». Pour que la loi s'applique, le libellé de l'adresse courriel doit permettre d'identifier effectivement son propriétaire. Sinon, il sera difficile de soutenir qu'elle constitue, en elle-même un renseignement personnel. L'adresse pierre.trudel@umontreal.ca est, par exemple, un renseignement personnel protégé en vertu de cette loi. Cependant, une adresse du genre professeur@hotmail.com est un cas plus problématique, car elle ne fournit pas — en soi — suffisamment d'informations pour identifier son détenteur. Or, le pourriel est adressé aussi bien aux adresses détenues par des personnes individuelles qu'à des organisations.

C'est donc dans la mesure où elle implique la collecte d'un renseignement personnel que la collecte d'adresses de courriel est visée par les lois sur la protection des renseignements personnels. Mais alors il faut distinguer si l'adresse est mise à la disposition du public à toutes fins ou si la mise à la disposition du public de l'adresse n'est effectuée que dans le cadre d'une activité restreinte.

160 L.R.Q., c. P-39.1.

Par exemple, dans une plainte dont a été saisie la Commissaire à la vie privée du Canada, l'employeur du plaignant était d'avis que les adresses de courriel de son personnel constituaient de l'information commerciale. Bien que l'employeur pouvait, en des circonstances très exceptionnelles, permettre à un employé de supprimer son adresse de courriel, il exigeait que ses employés publient leur adresse de courriel, conformément à son modèle d'affaires et à son attente voulant que les employés soient facilement accessibles. L'employeur s'attendait également à ce que les entreprises ou les organisations obtiennent sa permission avant de communiquer avec son personnel pour des fins qui ne sont pas liées à la promotion des intérêts de l'employeur[161].

1.1.1 La collecte auprès d'un tiers

En vertu de la *Loi sur la protection des renseignements personnels dans le secteur privé,* une entreprise ne peut communiquer, sans le consentement de l'intéressé, les renseignements recueillis à un tiers ou les utiliser à des fins non pertinentes par rapport à l'objet du dossier (art. 13). De plus, l'entreprise doit limiter sa cueillette aux informations nécessaires à l'objet du dossier et l'effectuer par des moyens licites (art. 5). En vertu de l'article 22 de la *Loi sur la protection des renseignements personnels dans le secteur privé*, il demeure possible qu'une entreprise communique légalement une adresse protégée par la loi. En effet, cet article prévoit que l'entreprise pourra communiquer à un tiers une liste nominative si elle respecte les trois conditions suivantes :

1- cette communication est prévue dans un contrat comportant une stipulation qui oblige le tiers à n'utiliser ou ne communiquer la liste ou le renseignement qu'à des fins de prospection commerciale ou philanthropique;

2- avant cette communication, lorsqu'il s'agit d'une liste nominative de ses clients, de ses membres ou de ses employés, elle a accordé aux personnes concernées l'occasion valable de refuser que ces renseignements soient utilisés par un tiers à des fins de prospection commerciale ou philanthropique;

3- cette communication ne porte pas atteinte à la vie privée des personnes concernées.

On constate qu'il est difficile pour une entreprise de fournir à un polluposteur une liste d'adresses courriel sans engager sa responsabilité. Ajoutons que lorsque la personne intéressée accepte la communication dans le cadre d'un concours ou d'un sondage rémunéré, l'entreprise devra tout de même s'assurer d'avoir obtenu son « véritable » consentement, ce qui — dans la pratique — n'est pas toujours assuré. Ces difficultés découlent en grande partie du fait que, bien souvent, on a perdu de vue la raison d'être de la protection des données personnelles. D'une finalité de protéger la vie privée, on est passé à celle de donner suite à un plus ou moins mythique « droit de veto » de la personne sur les informations la touchant. Le consentement, qui était au départ un moyen d'assurer au sujet la maîtrise nécessaire sur les renseignements relevant de sa vie privée, est devenu une fin en soi, quitte à ce qu'il soit perverti ou banalisé afin de contourner les rigidités résultant d'une conception parfois trop englobante de la protection des données personnelles. C'est ainsi que s'est répandu sur Internet, la pratique de requérir de l'usager qu'il consente…. à toutes sortes d'usages dans des contrats que personne ne prend le temps ou n'a le courage de lire. Le droit de la protection des données a été ramené à une simple obligation d'exiger un clic de la part de l'usager ! Cette approche formaliste qui repose sur le mythe du consentement soi-disant libre et éclairé montre ses limites. Les pourriels peuvent à toutes fins pratique être transmis sans limites à tous ceux qui ont consenti. Ce qu'il faut assurer, c'est la protection effective des données personnelles et non ramener cette obligation à celle d'obtenir le consentement de la personne concernée.

---

161 *Courriels non sollicités pour fins de marketing* http://www.privcom.gc.ca/cf-dc/2005/297_050331_01_f.asp. Dans cette situation, la Commissaire a considéré que la collecte de cette adresse n'était pas licite aux termes de l'article 2; principe 4.3; alinéas 7(1)d) et 7(2)c.1); principes 4.1 et 4.1.3 de la *Loi sur la protection des renseignements personnels et les documents électroniques.* Voir aussi, "Récentes poursuites reliées au pourriel" dans *Freinons le pourriel, Rapport du Groupe de travail sur le pourriel*, Ottawa, mai 2005, p. 13.

1.1.2 La collecte automatisée

Si les dispositions de la *Loi sur la protection des renseignements personnels dans le secteur privé* peuvent effectivement inquiéter les firmes de marketing direct qui organisent des sondages « bidon » ou qui font appel à d'autres astuces pour obtenir des adresses, il faut reconnaître qu'une bonne partie (voire même la majorité) des polluposteurs ne s'en préoccupent guère, étant donné qu'ils recueillent les adresses à l'aide de moyens informatiques automatisés. En l'absence de jurisprudence à ce sujet, il est difficile de déterminer si la *Loi sur la protection des renseignements personnels dans le secteur privé* s'applique à la collecte d'informations publiquement disponibles à l'aide de « crawlers » (des micro-programmes qui parcourent le Web à la recherche d'adresses). Il ne faut pas oublier en outre que la loi ne s'applique qu'à l'occasion de l'exploitation d'une entreprise (au sens de l'art. 1525 C.c.Q.). Le polluposteur-criminel n'est donc pas forcément visé par celle-ci.

Pour sa part, Michael Geist a soutenu que l'article 342.1 du *Code criminel*[162] concernant l'utilisation non autorisée d'ordinateur interdit ce genre de pratiques. Mais, compte tenu du principe d'interprétation restrictive des textes créateurs d'infractions, il n'est pas certain que le texte de l'infraction puisse supporter une si large interprétation.

En plus d'utiliser des « crawlers », les polluposteurs font également appel à des attaques par dictionnaire dans l'optique de recueillir des adresses courriel. À cet égard, il serait possible d'argumenter que ce genre d'attaques est un méfait interdit par l'article 430 (1.1) c) du *Code criminel* dans la mesure où elles « gêne[nt] l'emploi légitime des données » (le courriel, en l'espèce). Une attaque si intense qu'elle ralentit le serveur courriel serait un bon exemple de méfait au sens de l'art. 430. L'article 342.1 (1) c) peut également recevoir application si l'ordinateur d'un tiers est usurpé pour commettre le méfait.

1.2 L'expédition des messages

1.2.1 Le caractère non sollicité de l'envoi

Pour l'instant, le simple fait d'envoyer un message courriel non sollicité n'est pas, en soi, interdit par les lois québécoises et fédérales. Toutefois, l'article 41 de la *Loi sur les télécommunications*[163] accorde au CRTC un pouvoir de réglementation sur le caractère non sollicité du pourriel, mais ce pouvoir n'a pas encore été utilisé à ce jour par l'organisme.

Cela étant dit, il est à remarquer qu'au Québec, l'article 24 de la *Loi sur la protection des renseignements personnels* dans le secteur privé accorde à la personne sollicitée grâce à une liste nominative le droit d'en être retirée (*opt-out*).

1.2.2 L'usurpation des ressources informatiques d'autrui

Plus souvent qu'autrement, les moyens employés pour procéder à l'envoi de pourriel sont contraires à la loi. Afin de masquer leur identité, les polluposteurs vont généralement envoyer leurs pourriels à l'aide d'installations informatiques qui ne leur appartiennent pas. Or, l'article 342.1 du *Code criminel* interdit l'utilisation non autorisée d'un ordinateur (que ce soit par le piratage d'un réseau d'entreprise ou par la transformation d'un PC en « zombie »). Les logiciels facilitant ce genre d'activités illicites sont également interdits selon l'article 342.2 du *Code criminel*, qui concerne la possession de moyens permettant

---

162 L.R. 1985, c. C-46. Michael GEIST, *Untouchable?: A Canadian Perspective on the Anti-Spam Battle*, version 1.1, May 2004, p. 27.

163 L.R. 1985, c. T-3.4.

l'utilisation non autorisée d'ordinateur. Mais ceci ne serait pas un vol de service de télécommunication en vertu de l'article 326.1 du *Code criminel* car selon l'arrêt *R*. c. *McLaughlin*, [1980] 2 R.C.S. 331, un ordinateur ne constitue pas une « installation de télécommunication ».

1.2.3 La manipulation du champ « De : »

L'article 24 de la *Loi sur la protection des renseignements personnels dans le secteur privé* précise que lorsqu'une entreprise contacte des personnes à partir d'une liste nominative, elle doit s'identifier. La pratique courante des polluposteurs de substituer leur adresse réelle par une adresse fictive ou appartenant à une autre entreprise y est donc assurément contraire.

Il est aussi probable que la manipulation de l'adresse d'où provient un courriel soit interdite par le *Code criminel*. En effet, l'article 372 (1) prévoit qu'est « coupable d'un acte criminel et passible d'un emprisonnement maximal de deux ans quiconque, avec l'intention de nuire à quelqu'un ou de l'alarmer, transmet ou fait en sorte ou obtient que soit transmis, par lettre, télégramme, téléphone, câble, radio ou autrement, des renseignements qu'il sait être faux ». Lorsqu'un polluposteur ment à propos de l'origine de ses messages, il transmet un faux renseignement et le fait dans le dessein de nuire à la personne qui reçoit le pourriel. L'emploi de l'expression « ou autrement » donne ouverture à une interprétation de la disposition qui y inclut les faux renseignements transmis par courriel.

Des dispositions en matière de protection du consommateur pourraient également interdire la manipulation du champ « De : » dès lors que l'on considère le mensonge sur l'identité comme constituant une fausse représentation. Les articles 238 c)[164], 242[165] et 219[166] de la *Loi sur la protection du consommateur* et les articles de la 52[167] et 74.01[168] de la *Loi sur la concurrence* portent sur ce type de pratiques. Toutefois, il n'est pas assuré que toutes les offres faites par courriel peuvent être qualifiées de contrats de consommation au sens de la LPC.

1.3 Le contenu des messages

1.3.1 Fausses représentations

Il est communément admis que les produits annoncés par pourriel correspondent rarement à leur description. Les dispositions de protection du consommateur mentionnées plus haut peuvent également s'appliquer à l'égard de ces offres frauduleuses. Dans les cas plus graves, l'article 408 du *Code criminel* pourrait même trouver application. Cet article dispose que commet une infraction quiconque, avec l'intention de tromper ou de frauder le public ou toute personne, passe d'autres marchandises ou services pour et contre les marchandises et services qui ont été commandés ou utilise, à l'égard de marchandises ou services, une désignation qui est fausse sous un rapport essentiel.

De façon plus particulière, la *Loi sur les aliments et drogues* réglemente strictement la vente — très populaire sur Internet — de produits pharmaceutiques. Le fait, par exemple, de vendre de fausses pilules

---

164 Art. 238c) LPC : "Aucun commerçant, fabricant ou publicitaire ne peut faussement, par quelque moyen que ce soit, déclarer comme sien un statut ou une identité."

165 Art. 242 LPC : "Aucun commerçant ne peut, dans un message publicitaire, omettre son identité et sa qualité de commerçant".

166 Art. 219 LPC: "Aucun commerçant, fabricant ou publicitaire ne peut, par quelque moyen que ce soit, faire une représentation fausse ou trompeuse à un consommateur."

167 Art. 52 de la *Loi sur la concurrence*: « Nul ne peut, de quelque manière que ce soit, aux fins de promouvoir directement ou indirectement soit la fourniture ou l'utilisation d'un produit, soit des intérêts commerciaux quelconques, donner au public, sciemment ou sans se soucier des conséquences, des indications fausses ou trompeuses sur un point important. »

168 Des indications fausses ou trompeuses constituent des pratiques interdites en vertu de cet article.

de Viagra est interdite à l'article 9 de cette loi. En vertu de cet article, « il est interdit d'étiqueter, d'emballer, de traiter, de préparer ou de vendre une drogue — ou d'en faire la publicité — d'une manière fausse, trompeuse ou mensongère ou susceptible de créer une fausse impression quant à sa nature, sa valeur, sa quantité, sa composition, ses avantages ou sa sûreté. ». Les lois sur la profession de pharmacien peuvent également trouver application.

1.3.2 Offres de contrats à distance

Un pourriel peut comporter une offre de contrat à distance au sens des dispositions des articles 54.1 et suivants de la *Loi sur la protection du consommateur*[169]. Selon l'article 54.1 2e alinéa, un commerçant est réputé faire une offre de conclure le contrat dès lors que sa proposition comporte tous les éléments essentiels du contrat envisagé, qu'il y ait ou non indication de sa volonté d'être lié en cas d'acceptation et même en présence d'une indication contraire. L'article 54.4 de la *Loi sur la protection du consommateur* indique un ensemble de renseignements que le commerçant doit divulguer avant la conclusion du contrat à distance. Les messages à caractère commercial adressés à un consommateur qui ne se conforment pas à ces exigences sont donc susceptibles de donner lieu à des poursuites.

1.3.3 Virus, vers, chevaux de Troie, etc.

Aux termes des articles 342.1 et 430 (1.1) du *Code criminel*, il est interdit d'envoyer par courriel tout programme malicieux qui vise à prendre contrôle ou à gêner l'utilisation d'un ordinateur personnel. Les dommages occasionnés par l'infection peuvent constituer un méfait sur les données au sens de l'article 430 (1.1).

1.3.4 Fraudes « pump and dump »

Certains pourriels peuvent s'inscrire dans l'organisation d'un stratagème appelé fraude « pump and dump ». Jean-Pierre Cloutier explique que :

> *L'astuce pour les fraudeurs consiste d'abord à acheter un certain volume d'actions d'un titre boursier dormant ou coté en cents (penny stock), puis par un pourriel prenant la forme d'une recommandation d'achat de susciter de l'intérêt pour le titre dans le but d'en faire artificiellement gonfler le prix (pump) et, par la suite, une fois atteint le seuil souhaité de liquider rapidement le portefeuille (dump) et d'encaisser la marge. Évidemment, la vente en bloc du portefeuille des fraudeurs fait s'effondrer le titre et les investisseurs qui ont mordu à l'arnaque subissent des pertes*[170].

La *Loi sur les valeurs mobilières* dispose, à son article 195.2, que constitue « une infraction le fait d'influencer ou de tenter d'influencer le cours ou la valeur d'un titre par des pratiques déloyales, abusives ou frauduleuses ». Cette disposition vise certainement le phénomène des fraudes « pump and dump » qui circulent très couramment par pourriel. L'article 204 de la loi prévoit qu'en cas de violation de l'article 195.2, la personne trouvée coupable est passible d'une amende pouvant atteindre cinq millions de dollars. Une amende d'une telle ampleur est susceptible de produire un effet dissuasif important.

Il existe en outre un recours criminel contre le polluposteur qui participe à une fraude « pump and dump ». L'article 382 du *Code criminel* porte sur les manipulations frauduleuses d'opérations boursières et vise ce type de fraudes qui, vu sa complexité, mérite d'être cité en entier :

---

169 Ces dispositions, aux termes de l'article 18 de la *Loi modifiant la Loi sur la protection du consommateur et la Loi sur le recouvrement de certaines créances*, L.Q. 2006 c. 48, doivent entrer en vigueur à la date ou aux dates fixées par le gouvernement mais au plus tard le 15 décembre 2007.

170 Le pourriel « pump and dump », Jean-Pierre Cloutier le blogue, 20 janvier 2007, < http://cyberie.qc.ca/jpc/2007/01/le-pourriel-pump-and-dump.html >.

> *382. Est coupable d'un acte criminel et passible d'un emprisonnement maximal de dix ans quiconque, par l'intermédiaire des facilités d'une bourse de valeurs, d'un* curb market *ou d'une autre bourse, avec l'intention de créer une apparence fausse ou trompeuse de négociation publique active d'une valeur mobilière, ou avec l'intention de créer une apparence fausse ou trompeuse quant au prix courant d'une valeur mobilière, selon le cas :*
>
> *a) fait une opération sur cette valeur qui n'entraîne aucun changement dans la propriété bénéficiaire de cette valeur;*
>
> *b) passe un ordre pour l'achat de la valeur, sachant qu'un ordre sensiblement de même importance, à une époque sensiblement la même et à un prix sensiblement semblable pour la vente de la valeur, a été ou sera passé par ou pour les mêmes personnes ou des personnes différentes;*
>
> *c) passe un ordre pour la vente de la valeur, sachant qu'un ordre sensiblement de même importance, à une époque sensiblement la même et à un prix sensiblement semblable pour l'achat de la valeur, a été ou sera passé par ou pour les mêmes personnes ou des personnes différentes.*

On remarque que ce sont les paragraphes b) et c) qui interdisent ces fraudes. Mais en l'absence de jurisprudence, il est difficile d'émettre une opinion définitive à ce sujet. Quoi qu'il en soit, il serait toujours possible de poursuivre les auteurs de l'opération en vertu de l'article 380 du *Code criminel* qui interdit de manière générale la fraude.

1.3.5 Hameçonnage

L'hameçonnage est une fraude lourde de conséquences qui implique une pluralité de gestes; plusieurs dispositions du *Code criminel* permettent de poursuivre les personnes qui en sont auteurs ou complices.

Il va de soi que l'hameçonnage est interdit en vertu de l'article 380 du *Code criminel* qui prévoit une interdiction de nature générale de la fraude. L'utilisation de faux prétextes, une prétendue « mise à jour du compte », par exemple, afin de nuire à une personne en l'amenant à divulguer des informations personnelles et bancaires est interdite par l'article 372 (1).

L'usurpation d'une marque ou de l'image corporative d'une société, afin de faire croire que le courriel provient d'une source de confiance, constitue une infraction en vertu de l'article 406 du *Code criminel* (contrefaçon d'une marque de commerce) et cette pratique est également visée par l'article 7 de la *Loi sur les marques de commerce*.

L'utilisation des informations transmises par la victime peut bien sûr faire aussi l'objet de poursuites criminelles, fondée sur les articles 403, 342 et 362 du *Code criminel* qui interdisent respectivement le vol d'identité, l'utilisation non autorisée d'un numéro de carte de crédit et l'escroquerie (ex. obtenir un prêt sous un faux nom).

2. Les logiciels espions

Les logiciels espions sont ceux qui sont installés sur un ordinateur sans l'accord de son possesseur légitime[171]. C'est essentiellement une installation non consentie (2.1) qui une fois accomplie, peut donner lieu à des comportements dommageables (2.2) et à des effets pervers (2.3).

171 Daniel B. GARRIE, Alan F. BLAKELEY, Matthew J. ARMSTRONG, "The Legal Status of Spyware", (2006) 59 *Federal Comm. L.J.,* 161.

2.1 Installation non consentie

Le caractère non consenti des espiogiciels en fait des phénomènes visés aussi bien par les dispositions du Code criminel que les principes de droit civil relatifs à la protection de la vie privée.

D'abord, l'article 342.1 du *Code criminel* interdit à toute personne de placer un programme informatique sur l'ordinateur d'autrui sans avoir reçu préalablement son autorisation (car il s'agit d'une manière d'obtenir « les services d'un ordinateur »). Dans l'hypothèse où le logiciel est installé sans l'autorisation de l'utilisateur, ce n'est pas l'auteur comme tel du logiciel qui engage sa responsabilité criminelle, mais bien la personne qui a initié l'installation du logiciel en l'absence de consentement. L'utilisation des techniques d'installation « invisibles » (« *drive-by install* ») exploitant une vulnérabilité du système d'exploitation ou du navigateur Web est par conséquent interdite en vertu de 342.1. Il en va de même pour le rattachement de logiciels espions à des fichiers échangés sur des réseaux d'échange entre pairs (P2P) ou à un logiciel-appât.

Ensuite, au plan civil, l'article 36 du Code civil prévoit que :

> *Peuvent être notamment considérés comme des atteintes à la vie privée d'une personne les actes suivants :*
>
> *1° Pénétrer chez elle ou y prendre quoi que ce soit*[172] *;*
>
> *2° Intercepter ou utiliser volontairement une communication privée,*[173]
>
> *3° Capter ou utiliser son image ou sa voix lorsqu'elle se trouve dans des lieux privés,*[174]
>
> *4° Surveiller sa vie privée par quelque moyen que ce soit*[175] *;*

Les auteurs et distributeurs de logiciels espions doivent donc s'assurer que la procédure d'installation de leurs logiciels soit conditionnée par un consentement libre et éclairé. À cet égard, et même s'il peut y avoir de légères différences quant à la notion de consentement entre le droit criminel et le droit civil, les principes établis quant à la qualité du consentement par les articles 1399 à 1401 du *Code civil du Québec* constituent la référence. À ce stade de l'analyse, il demeure important de ne pas confondre le consentement à l'installation du logiciel et le consentement à la cueillette d'informations personnelles.

---

172 *Société Radio-Canada c. Courtemanche*, (C.A., 1999-06-07), SOQUIJ AZ-99011442, J.E. 99-1250, [1999] R.J.Q. 1577, REJB 1999-12880; *Doyon c. Ducharme*, (C.Q., 1999-12-20), SOQUIJ AZ-00036099, B.E. 2000BE-156, [2000] R.L. 366; *Propriétés Parc Vertu c. Jebara*, (C.Q., 2003-01-20), SOQUIJ AZ-50166114, J.E. 2003-694, [2003] J.L. 186, REJB 2003-38832; *Syndicat canadien de la fonction publique, section locale 302 c. Verdun (Ville de)*, (C.A., 2000-02-09), SOQUIJ AZ-50069143, J.E. 2000-379, D.T.E. 2000T-164, [2000] R.J.Q. 356, [2000] R.J.D.T. 38, (2000), 186 D.L.R. (4th) 89 (Que. C.A.), REJB 2000-16403

173 *Cadieux* c. *Service de Gaz naturel Laval Inc.*, [1991] R.J.Q. 2490 (C.A.); *Roy* c. *Saulnier*, [1992] R.J.Q. 2419 (C.A.) et *167782 Canada Inc.* c. *Tenneco Canada Inc.*, J.E. 94-1817 (C.S.) ; R. c. Solomon, (C.M., 1992-09-28), SOQUIJ AZ-92031314, J.E. 92-1573, [1992] R.J.Q. 2631, 16 C.R. (4th) 193, 77 C.C.C. (3d) 264 (sur l'expectative de confidentialité avec un téléphone cellulaire)

174 *Cohen* c. *Queenswear International Ltd.*, [1989] R.R.A. 570 (C.S.) (utilisation d'une photo sur les emballages d'un produit); *Torrito* c. *Fondation Lise T. pour le respect du droit à la vie et à la dignité des personnes lourdement handicapées*, [1995] R.D.F. 429 (C.S.); *Dion* c. *3576523 Canada inc.*, (C.Q., 2001-03-01), SOQUIJ AZ-50190072, [2001] R.L. 253; *Pelletier* c. *Ferland*, (C.S., 2004-07-07), SOQUIJ AZ-50261329, J.E. 2004-1576, [2004] R.R.A. 944, REJB 2004-66848; *176100 Canada inc.* c. *Réseau des Appalaches FM ltée*, (C.S., 2001-03-14), SOQUIJ AZ-50084537, J.E. 2001-877, [2001] R.J.Q. 1011, [2001] R.R.A. 503 (rés.), REJB 2001-24168 (atteinte à la vie privée d'un animateur de radio)

175 *Maheux* c. *Boutin*, (C.Q., 1995-11-27), SOQUIJ AZ-96031018, J.E. 96-136, [1996] R.R.A. 265 (rés.), EYB 1995-85020; *Syndicat des chauffeurs de la Société de transport de la Ville de Laval (CSN)* c. *Ferland*, (C.A., 2001-01-31), SOQUIJ AZ-01019038, J.E. 2001-526, D.T.E. 2001T-235, [2001] J.Q. No. 447 (Q.L.), REJB 2001-22753.

2.2 Comportements dommageables

Les espiogiciels servent à accomplir des actes de surveillance et autres gestes intrusifs.

2.2.1 Le profilage marketing

L'article 5 de la *Charte des droits et libertés de la personne* garantit à toute personne le droit à la protection de sa vie privée. Ce principe est repris dans le *Code civil du Québec* à son chapitre troisième « Du respect de la réputation et de la vie privée ». La *Loi sur la protection des renseignements personnels dans le secteur privé* met en œuvre le régime de protection des renseignements personnels lors de l'exploitation d'une entreprise.

Il faut comprendre que le consentement à l'installation du programme auquel est joint le logiciel espion ne peut, à lui seul, autoriser l'éditeur du logiciel à recueillir des informations personnelles auprès de l'utilisateur. Les éléments de cette cueillette doivent faire l'objet de clauses spécifiques au sein même du contrat de licence ou être clairement divulgués lors de la procédure d'installation selon l'article 6 de la *Loi sur la protection des renseignements personnels dans le secteur privé.* Parce que ces contrats sont des contrats d'adhésion, un simple lien du type « Consulter notre politique relative à la vie privée à http://www.entreprise.com/vieprivee » est insuffisant, car la clause externe ne lie pas les parties dans un contrat d'adhésion si son contenu n'a pas été porté à la connaissance de l'adhérent (art. 1435 C.c.Q.).

Même si la définition de renseignement personnel à l'article 2 de *Loi sur la protection des renseignements personnels dans le secteur privé* semble claire, il n'est pas aisé de déterminer ce qui constitue, en matière technologique, un tel renseignement. L'adresse IP et l'historique de navigation, deux informations souvent transmises par les logiciels espions, permettent-ils vraiment d'identifier la personne physique? Généralement, on pourrait croire que non. Est-ce une question de circonstances? Y-a-t-il des exceptions?

Prenons le cas de l'utilisateur qui remplit en ligne un formulaire d'abonnement à un site de réseautage social. L'exemple n'est pas théorique, compte tenu de la popularité de ces sites et de la vague « Web 2.0 ». Si le webmestre du site en question a choisi la méthode « GET » pour transmettre le formulaire au serveur, l'URL soumise puis enregistrée dans l'historique de navigation risque de contenir des informations personnelles au sens de la loi (exemple fictif : www.communaute.qc.ca/inscription?prenPierre"& nom="Trudel"&employeur="UdeM").

Comme il est difficile de prévoir, ce serait une pratique souhaitable que les entreprises effectuant du « profilage » marketing obtiennent le consentement de l'utilisateur quant à la communication de ses renseignements personnels, et ce, même si l'entreprise prétend dresser des profils de manière anonyme. Ces firmes de marketing sont très au fait des difficultés que soulève l'envoi de formulaires quant au caractère anonyme de l'historique de navigation d'une personne.

2.2.2 L'interception des communications

Les logiciels espions les plus agressifs agissent souvent comme enregistreurs de frappe, c'est-à-dire qu'ils notent toutes les touches du clavier sur lesquelles l'utilisateur a appuyé. L'atteinte à la vie privée est ici flagrante : le logiciel espion peut transmettre à un tiers le fichier journal d'une session de clavardage, par exemple.

Bien que les dispositions du chapitre « Du respect de la réputation et de la vie privée » du *Code civil du Québec* soient générales, le second paragraphe de l'article 36 prévoit explicitement que l'interception d'une communication privée peut constituer une violation du droit à la vie privée. L'interception des communications d'un ordinateur est également interdite par le *Code criminel* à l'article 342.1 (1) b); on traite d'interception de « toute fonction d'un ordinateur » frauduleusement et sans apparence de droit.

2.2.3 Usurpation de revenus publicitaires

Dans la première partie de ce rapport, nous avons vu que certains logiciels espions remplacent les bandeaux publicitaires d'un site Web fort achalandé par des publicités ciblées émanant de leur développeur. Il va de soi que plusieurs recours civils, dont le recours en responsabilité extracontractuelle, sont possibles dans un tel cas et permettent au maître du site Web affecté d'obtenir réparation.

De plus, le *Code criminel*, à son article 380 (1), interdit d'employer un « moyen dolosif » pour « frustrer » toute personne de « quelque bien, service, argent ou valeur ». Si l'objet de l'infraction est inférieur ou égal à 5000 $, la personne prise en défaut est coupable d'un acte criminel ou d'une infraction punissable sur déclaration de culpabilité par procédure sommaire. Lorsque la valeur de la fraude dépasse 5000 $, il s'agit forcément d'un acte criminel.

2.2.4 Fausses alertes de sécurité

Un autre procédé dolosif employé par les développeurs de logiciels espions est de faire apparaître, de manière intempestive, de faux avis très alarmistes incitant l'utilisateur à se procurer un logiciel de sécurité proposé par l'éditeur du logiciel espion (ex. pare-feu, antivirus et, ironiquement, un anti-espiogiciel). L'analyse que nous avons faite plus haut de l'article 380 du *Code criminel* reçoit également application en l'espèce. Qui plus est, il serait également possible d'argumenter qu'une « information fausse » a été transmise dans le but de nuire à la victime de l'arnaque au sens de l'article 372 (1).

Évidemment, prétendre à tort que le PC d'une personne est infecté d'un dangereux virus constitue une fausse représentation au sens de la *Loi sur la protection du consommateur* (art. 219) et de la *Loi sur la concurrence* (art. 52 et 74.01). Notons que la vente du produit de sécurité devra, entre autres, avoir été conclue entre l'éditeur du logiciel espion et l'internaute victime pour être considérée comme un contrat de consommation.

2.3 Effets

Si les logiciels-espions sont de plus en plus connus, c'est surtout à cause de leurs effets pervers sur l'ordinateur qui en est l'hôte. Compte tenu de toutes les fenêtres de publicité qu'ils affichent, l'utilisateur développe rapidement l'impression que l'interface graphique de son système d'exploitation a été « envahie ». Il est également en mesure de constater les nombreux ralentissements et pannes que leur installation en trop grand nombre provoque. Pour les utilisateurs, la seule solution se limite souvent à embaucher un technicien informatique pour qu'il restaure la configuration d'origine du PC.

Ces effets des logiciels espions peuvent constituer un méfait sur les données au sens de l'article 430 (1.1) c), car ils empêchent, interrompent ou gênent l'emploi légitime des données.

Tableau 1 - Lois applicables au pourriel et à l'hameçonnage

La plupart des gestes identifiés ci-dessous sont susceptibles de constituer une faute au sens de l'article 1457 C.c.Q. et d'engager la responsabilité de leur auteur.

Les lois fédérale et québécoise sur la protection des renseignements personnels ne s'appliquent que lorsque le libellé de l'adresse courriel permet d'identifier son propriétaire. Par exemple, pierre.trudel@umontreal.ca est un renseignement personnel protégé en vertu de ces lois, mais pas coolgirl@hotmail.com (art. 2 de la *Loi sur la protection des renseignements personnels dans le secteur privé*). Il ne faut pas oublier en outre que la loi québécoise ne s'applique qu'à l'occasion de l'exploitation d'une entreprise (au sens de l'art. 1525 C.c.Q.). Le polluposteur-criminel n'est donc pas forcément visé par celle-ci.

COLLECTE D'ADRESSES	EXPÉDITION	CONTENU
Voir section 1.1.1, p. 56 **VENTE OU ACHAT D'UNE LISTE NOMINATIVE SANS LE CONSENTEMENT DE L'INTÉRESSÉ À DES FINS DE PROSPECTION COMMERCIALE OU PHILANTHROPIQUE** *Loi sur la protection des renseignements personnels dans le secteur privé*, art. 22. ► Par dérogation aux principes établis aux articles 6 et 13. ► L'art. 22 affirme qu'une liste nominative peut être constituée d'une adresse technologique (courriel). Ainsi, il s'applique donc à toutes les adresses de courrier électronique, peu importent qu'elles identifient ou non leur détenteur.	**VOIR SECTION 1.2.1, P. 57** **ENVOI NON SOLLICITÉ** *Loi sur les télécommunications*, art. 41. ► Accorde au CRTC un pouvoir de réglementation sur le pourriel. Ce pouvoir n'a pas encore été exploité à ce jour.	**VOIR SECTION 1.3.1, P. 58** **FAUSSES REPRÉSENTATIONS VISANT À PROMOUVOIR UN PRODUIT OU UN SERVICE** *Code criminel*, art. 408 (substitution frauduleuse). *Loi sur la concurrence*, art. 52 (sanction criminelle) et 74.01 (sanction administrative). *Loi sur la protection du consommateur*, art. 219. (fausses représentations) *Loi sur les aliments et drogues*, art. 9 (fraude).
VOIR SECTION 1.1.2, P. 57 **ATTAQUES PAR DICTIONNAIRE ET DE « FORCE BRUTE »** *Code criminel*, art. 430 (1.1) c) (Méfait) ► Certains affirment que l'art. 342.1 interdit les attaques par dictionnaire. ► Pour être plus précis l'art. 430 (1.1) c) peut interdire ce genre d'attaques dans la mesure où elles « gêne[nt] l'emploi légitime des données » (le courriel, en l'espèce). Une attaque si intense qu'elle ralentit le serveur courriel serait un bon exemple de méfait au sens de l'art. 430. ► L'art. 342.1 (1) c) peut également recevoir application si l'ordinateur d'un tiers est utilisé pour commettre le méfait.	**VOIR SECTION 1.2.2, P. 57** **USURPATION DES RESSOURCES INFORMATIQUES D'AUTRUI** (Piratage d'un réseau d'entreprise, transformation d'un PC en « zombie »). *Code criminel*, art. 342.1 (utilisation non autorisée d'ordinateur) ► L'art 326 (1) b) (vol de service de télécommunication) ne s'applique pas, car, selon *R.* c. *McLaughlin*, [1980] 2 R.C.S. 331, un ordinateur n'est pas une « installation de télécommunication ».	**VOIR SECTION 1.3.4, P. 59** **FRAUDES « PUMP AND DUMP »** *Code criminel*, art. 382 b) (manipulations frauduleuses d'opérations boursières). *Code criminel*, art. 380 (2) (fraude). *Loi sur les valeurs mobilières*, art. 195.2 (influencer frauduleusement le cours d'un titre) ► Voir l'art. 204 pour déterminer la sanction.

COLLECTE D'ADRESSES	EXPÉDITION	CONTENU
VOIR SECTION 1.1.2, P. 57 **BALAYAGE DU WEB** *Loi sur la protection des renseignements personnels dans le secteur privé*, art. 4-6. ► L'article 342.1 du *Code criminel* portant sur l'utilisation non autorisée d'ordinateur pourrait s'appliquer. Mais il n'est pas certain que sa rédaction puisse donner lieu à un interdit de balayer le Web à la recherche d'adresses courriel.	VOIR SECTION 1.2,3, P. 58 **TRAFICAGE DU CHAMP « DE : »** *Code criminel*, art. 372 (1) (faux messages) ► La portée de l'article 372 (1) est assez large pour rendre superflue une mise à jour de l'article 371. Il nécessite toutefois une intention de nuire à la personne. *Loi sur la protection des renseignements personnels dans le secteur privé*, art. 24 (obligation de s'identifier). *Loi sur la concurrence*, art. 52 (sanction criminelle) et 74.01 (sanction administrative). ► Si on considère le mensonge sur l'identité comme constituant une fausse représentation. *Loi sur la protection du consommateur*, art. 238 c), 242 et 219 (fausses représentations).	VOIR SECTION 1.3.5, P. 60 **HAMEÇONNAGE** *Code criminel*, art. 380 (interdiction générale de frauder). *Code criminel*, art. 403 (vol d'identité) *Code criminel*, art. 342 (utilisation non autorisée du numéro de carte de crédit) *Code criminel*, art. 362 (escroquerie) *Code criminel*, art. 372 (1). (utilisation de faux prétextes pour amener une personne à divulguer ses renseignements personnels.)
	Voir section 1.2.1, p. 57 **REFUS DE RETIRER UNE PERSONNE D'UNE LISTE NOMINATIVE (OPT-OUT)** *Loi sur la protection des renseignements personnels dans le secteur privé*, art. 24.	VOIR SECTION 1.3,5, P. 60 **USURPATION DE MARQUE, DE L'IMAGE CORPORATIVE** *Code criminel*, art. 406. *Loi sur les marques de commerce*, art. 7.
	LOGICIELS FACILITANT LE POURRIEL *Code criminel*, 342.2	VOIR SECTION 1.3.3, P. 59 **VIRUS, VERS ET CHEVAUX DE TROIE** *Code criminel*, art. 342.2 et 430 (1.1)

Tableau 2 - Lois applicables aux logiciels espions

NOTE : La plupart des gestes énumérés ci-dessous sont susceptibles de constituer une faute au sens de l'article 1457 C.c.Q. et d'engager la responsabilité de leur auteur.

INSTALLATION	COMPORTEMENT	EFFETS
VOIR SECTION 2.1, P. 61 **INSTALLATION NON CONSENTIE (SITES WEB MALICIEUX, FICHIERS CONTAMINÉS, ETC.)** *Code criminel*, art. 342.1 (utilisation non autorisée d'ordinateur) *Code civil du Québec*, art. 36	VOIR SECTION 2.2.1, P. 62 **CUEILLETTE D'INFORMATIONS PERSONNELLES, PROFILAGE MARKETING** *Loi sur la protection des renseignements personnels dans le secteur privé*, art. 4-6, 12-15 et 22-25. *Code civil du Québec*, art. 37.	VOIR SECTION 2.3, P. 63 **ENVAHISSEMENT DE L'INTERFACE GRAPHIQUE, PANNES ET RALENTISSEMENTS LIÉS À LA PRÉSENCE DE LOGICIELS ESPIONS** *Code criminel*, art. 430 (méfait sur les données). *Code civil du Québec*, art. 1457 et 1458 (responsabilité civile).
VOIR SECTION 2.1, P. 61 **INSTALLATION AU CONSENTEMENT « BOITEUX »** *Code civil du Québec*, art. 1399 à 1401 ► Pour juger la validité du consentement à l'installation du logiciel.	VOIR SECTION 2.2.2, P. 62 **INTERCEPTION DES COMMUNICATIONS (KEYLOGGING)** *Code criminel*, art. 342.1. ► Certains auteurs affirment que l'art. 184 ne peut recevoir application, étant donné qu'il exige que la communication soit faite entre deux personnes et non entre une personne et un ordinateur. *Charte des droits et libertés de la personne,* art. 5. *Code civil du Québec*, art. 35 et 36.	

INSTALLATION	COMPORTEMENT	EFFETS
	VOIR SECTION 2.2.3, P. 63 **APPROPRIATION DES COMMISSIONS D'AUTRUI** *Code criminel*, art. 380.	
	VOIR SECTION 2.2.4, P. 63 **FAUSSES ALERTES DE SÉCURITÉ AFIN DE VENDRE UN PSEUDO ANTI-VIRUS** *Code criminel,* art. 380 et 372 (1). *Loi sur la concurrence*, art. 52 (sanction criminelle) et 74.01 (sanction administrative). *Loi sur la protection du consommateur*, art. 219. ► Si la vente de produit de sécurité est réalisée entre le consommateur et le développeur du logiciel espion responsable de la fausse représentation.	

QUATRIÈME PARTIE
LA MISE EN OEUVRE DE L'APPROCHE « BOÎTE À OUTILS » EN CONTEXTE QUÉBÉCOIS : MODULER ET GÉRER LES RISQUES

À côté des graves menaces terroristes, le pourriel peut être perçu par certains comme un inconvénient qu'il faut apprendre à endurer! Devant le caractère insaisissable du phénomène, plusieurs peuvent en venir à penser qu'il est préférable d'attendre que le « marché » trouve une solution. De telles attitudes pouvaient se comprendre lorsque le pourriel se limitait à d'agaçants envois de publicité non sollicitée. Mais de plus en plus, il est un vecteur pour des activités qui peuvent être beaucoup plus dommageables. L'on constate combien le pourriel constitue un élément des stratégies de fraudeurs qui font de l'hameçonnage. Les méfaits à l'encontre des systèmes informatiques sensibles peuvent figurer au nombre des actions terroristes. C'est pourquoi il est plus difficile qu'auparavant de postuler que la non-intervention de l'État serait la meilleure option. Mais on reconnaît également que le phénomène du pourriel et des fléaux qui l'accompagnent ne se résoudra pas uniquement par l'adoption d'une loi. Il faut plutôt mobiliser un réseau de ressources travaillant de concert.

Le pourriel est un phénomène typique à Internet : sa régulation doit forcément tenir compte des caractéristiques du cyberespace. On ne peut espérer réussir dans la lutte au pourriel et autres fléaux en se limitant seulement à prendre des mesures qui pourraient convenir à l'égard des réalités qui se situent en dehors du cyberespace.

Or, le cyberespace n'est pas un environnement qui se réglemente comme l'espace physique. Construit essentiellement par la technique, Internet est une réalité qui paraît échapper à plusieurs points de repère sur lesquels s'appuie habituellement la réglementation étatique. Dans le cyberespace, la réglementation émanant de l'État n'est pas la seule à assurer les équilibres. La régulation étatique doit concourir avec les autres normativités à assurer les équilibres à l'égard des multiples activités qui se déroulent dans le cyberespace. De plus, le phénomène du pourriel, de l'hameçonnage et des espiogiciels connaît des évolutions souvent fulgurantes : tel un virus, ces fléaux connaissent des mutations qui peuvent rendre dérisoire une législation ou une stratégie pour en contrer la progression qui auraient été fondées sur les pratiques observables à un moment donné.

C'est pourquoi il est opportun d'envisager la stratégie de régulation du pourriel et autres fléaux au moyen d'une approche de « boîte à outils » comportant en elle-même une capacité d'adaptation rapide aux mutations. Une telle approche vise essentiellement à gérer les risques d'Internet. Pourriel, hameçonnage et espiogiciels sont des fléaux qui augmentent les risques associés à Internet. Internet étant configuré en un réseau ouvert, il est impossible de postuler qu'une intervention spécifique pourra à elle seule faire disparaître la totalité des pratiques et comportements risqués. Il faut donc une approche conséquente avec ces caractéristiques inhérentes d'Internet, capable d'assurer un suivi des évolutions et de garantir l'adaptation des actions de lutte afin de répondre vraiment aux fléaux avant qu'ils causent trop de dégâts.

1. Des risques à gérer

Ceux qui prennent part à des activités dans le cyberespace le font avec plus ou moins d'intensité selon qu'ils ont ou non conscience qu'ils auront à supporter plus ou moins de risques. L'encadrement normatif des pratiques nuisibles sur Internet peut s'envisager dans le cadre d'une approche de modulation et de gestion des risques.

Dans son acception générale, le risque peut être envisagé comme un objet social. Yvette Veyret observe que « le risque objet social se définit comme la perception du danger. Le risque n'existe que par rapport à

un individu, à un groupe social ou professionnel, une communauté, une société qui l'appréhende (…) et le traite par des pratiques spécifiques. Il n'y a pas de risque sans une population ou un individu qui perçoit et pourrait subir ses effets. »[176] Le risque n'existe pas dans le vide : il découle forcément d'un contexte sociétal donné.

Une fois reconnu, le risque emporte des obligations de précautions. Le risque juridique découle en effet des situations où la violation des droits d'autrui est susceptible de se produire. Même s'ils sont différents, il y a une étroite proximité entre le risque technologique et le risque juridique : lorsque le risque technologique est avéré, il naît presque toujours une obligation d'en tenir compte et de se comporter de façon conséquente. Le risque juridique peut aussi découler de la possible non-conformité à une loi ou à une autre sorte d'obligation également applicable. Le risque juridique, en toute hypothèse, résulte des situations dans lesquelles la responsabilité d'une personne peut être mise en cause.

L'État ou un autre acteur peut agir afin d'augmenter les risques de certains comportements ou activités ou réduire les risques associés à une conduite saine. Par exemple, lorsque l'État adopte une loi sévère contre certaines pratiques, cela accroît les risques associés à celles-ci. À l'égard des usagers qui se livrent à des activités légitimes, l'État peut baliser, voire limiter les risques.

Dans un pareil contexte, une stratégie contre le pourriel, l'hameçonnage et les espiogiciels s'envisage comme un ensemble de mesures conçues de manière à se renforcer les unes et les autres afin de limiter les risques des internautes qui s'adonnent à des activités licites. En somme, la stratégie doit se déployer en réseau : imposer des règles aux acteurs et inciter ces derniers à relayer ces exigences à tous ceux à l'égard desquels ils exercent une influence.

Dans une logique de risques, les mesures étatiques seront plus efficaces si elles sont assorties de politiques dynamiques de surveillance et de poursuites dans les cas où cela est possible. Il s'agit alors de faire en sorte que les risques découlant de ces lois soient relayés vers tous ceux qui mènent des activités illicites.

Dans un réseau, les acteurs gèrent leurs risques. Chacun de ceux qui sont en mesure d'imposer leur volonté disposent d'une capacité d'accroître les risques des autres. Ainsi, un État peut imposer des devoirs aux citoyens qui se trouvent sur son territoire. Ces derniers auront alors à gérer leurs risques découlant de ces obligations. Ils chercheront à s'assurer que leurs partenaires agissent en conformité avec les obligations auxquelles ils sont eux-mêmes tenus et à l'égard desquelles leur responsabilité peut se trouver engagée.

En somme, le système de régulation vise à rétablir les équilibres entre les risques et les précautions. Il doit fonctionner de façon à inciter l'ensemble des acteurs à minimiser les risques qui relèvent de situations sur lesquelles ils sont effectivement en mesure d'avoir une prise, et à accroître le plus possible les risques des acteurs qui choisissent d'avoir des comportements dommageables ou qui augmentent indûment les risques des usagers légitimes. C'est dans cette logique que s'inscrit nécessairement une politique intégrée de lutte contre le pourriel et les autres fléaux d'Internet.

2. Augmenter les risques associés aux pratiques nuisibles, diminuer les risques des usagers légitimes

Le pourriel et les autres pratiques nuisibles sont des risques d'Internet. La stratégie vise à réduire ou à transférer ces risques. Une politique intégrée de type « boîte à outils » doit viser à rééquilibrer les risques.

176 Yvette VEYRET, « Les risques », Dossier des images économiques du monde, FEDES, cité par Franck VERDUN, *La gestion des risques juridiques*, Paris, Éditions d'organisation, 2006, p. 11.

Il s'agit de rééquilibrer les risques causés aux usagers légitimes en augmentant les risques de ceux qui s'adonnent aux activités de pourriel, hameçonnage et espiogiciels ou en tirent profit.

L'approche dite de « boîte à outils » est essentiellement une régulation visant à accroître les risques de ceux qui se livrent aux pratiques nuisibles. L'approche suppose également d'appuyer les utilisateurs légitimes, les aider à se prémunir contre les pratiques nuisibles et par conséquent à limiter leurs risques à cet égard.

L'approche boîte à outils est fondée sur le recours à une pluralité de moyens : elle reconnaît que les interventions doivent être concertées. Elle reflète également le constat selon lequel la lutte contre les pratiques nuisibles ne saurait être l'apanage de la loi ou de la seule approche technique ou uniquement du marché : la loi peut être nécessaire afin de fixer le risque associé à une pratique nuisible au niveau approprié. On reconnaît également le caractère évolutif des activités risquées sur Internet et la nécessité d'une adaptation constante aux tendances.

Dans la conception traditionnelle, le risque juridique est une notion inusitée. Les juristes voient le risque dans tous les phénomènes qu'ils ont à examiner mais le fait qu'une sanction puisse découler de la transgression d'une règle n'est pas envisagé comme un risque en tant que tel par le juriste[177]. Par contre, dans une approche de gestion, le risque juridique apparaît plus clairement. Le gestionnaire envisage les règles de droit comme étant porteuses de risques. Celui qui, par hypothèse serait tenté de prendre part ou de tirer profit d'une activité de pourriel ou d'espionnage sur Internet doit savoir qu'une pareille décision est porteuse de risque lorsqu'elle est accomplie en territoire québécois.

Ainsi, dans un environnement en réseau, le risque juridique se présente comme comportant deux composantes : une ou des normes et un événement. C'est de la conjonction de la norme et de l'événement que découle le risque juridique.

La norme peut être énoncée dans une loi ou un règlement mais elle peut aussi découler d'un contrat ou d'une règle technique. Le propre de la norme, c'est qu'elle est susceptible d'être sanctionnée, c'est-à-dire qu'une conséquence adverse est susceptible de découler de la transgression. La transgression survient lors d'un événement. Il peut s'agir d'un acte affirmatif ou d'une omission qui a lieu dans un contexte concret. L'événement doit nécessairement être anticipé ou à tout le moins, sa survenance possible détectée. Le dommage qui peut découler de cet événement doit être évalué.

3. Une normativité qui s'énonce et s'applique en réseaux

Les enjeux d'Internet se posent dans un espace cadrant mal avec les référents fondés uniquement sur l'État territorial. Les normativités s'inscrivent dans un réseau complexe et en continuelle redéfinition. Un réseau est un ensemble de nœuds interconnectés et relayés[178]. Sans prétendre au déclassement du droit étatique, on ne peut ignorer que d'autres normativités contribuent autant, sinon plus que les lois étatiques, à définir les règles selon lesquelles les services sont créés, expérimentés, déployés et mis en marché[179].

177 Franck VERDUN, *La gestion des risques juridiques*, Paris, Éditions d'organisation, 2006, p. 20.

178 Manuel CASTELLS, *The Rise of Network Society*, 2nd ed., Oxford and Cambridge, Mass, Blackwell, 2000, p. 501.

179 Pour une revue du modèle réseautique d'analyse du droit voir : Thomas SCHULTZ, « La régulation en réseau du cyberespace », [2005] 55 *R.I.E.J.,* 31-90.

Pour connaître les normes qui ont vocation à régir un environnement raccordé à Internet, il faut identifier les nœuds au sein desquels s'élabore et s'énonce la normativité qui s'applique effectivement[180]. L'ensemble des normativités agissantes sur Internet peut être représenté selon un modèle réseautique. Internet peut être envisagé comme un univers constitué de nœuds et de relais de normativité qui sont tous en lien d'interinfluence. Les nœuds de normativité sont les endroits où les normes sont énoncées. Par exemple, un État énonce des lois qui seront obligatoires pour ceux qui sont situés sur son territoire. Les relais contribuent à la fois à mettre les nœuds de normativité en présence l'un de l'autre ou à les distancier. Par exemple, une entreprise régie par les lois du Québec devra, pour gérer adéquatement ses risques, exiger de ses co-contractants qu'ils assurent la protection des données personnelles. À leur tour, les co-contractants vont devoir s'assurer de respecter les exigences contractuelles tout en composant avec les normes techniques qui s'imposent à eux.

Dans le réseau, on observe des interrelations diversifiées entre les normes. Les normes sont proposées (voire imposées) dans divers nœuds de normativité; ces nœuds de normativité sont en concurrence ou en complémentarité avec d'autres. Les relais de la normativité assurent l'application effective des règles. Dans les relais s'explicitent et se diffusent les normativités et les conséquences de celles-ci.

On peut identifier plusieurs rapports entre les normativités. Dans la plupart des situations, on se trouvera en présence d'un rapport d'obligation : une loi est obligatoire à l'égard d'une personne située sur le territoire d'un État : cette dernière doit forcément relayer les obligations découlant de la loi. Dans d'autres situations, on sera appelé à considérer le rapport de relevance : par exemple, les directives européennes ont des effets non seulement sur le droit des pays membres mais aussi sur les obligations des acteurs situés dans des pays entretenant des relations importantes avec les ressortissants de cette entité. La régulation des usages sur Internet résulte donc souvent aussi bien du droit national du pays où l'on se trouve que du droit des ordres juridiques des entités en position d'exercer une influence sur les autres lieux d'élaboration de normes. Il en est de même des lois américaines : plusieurs sites y compris ceux qui sont exploités au Québec considèrent qu'il est de bonne pratique de se conformer à certaines lois américaines puisqu'ils ambitionnent de rejoindre des ressortissants de ce pays.

Des lieux de normativité produisent des normes ou des processus de coordination tandis que d'autres fonctionnent comme des espaces de négociation ou d'équilibrage appliquant des régulations dans un rapport de dialogue avec d'autres lieux de normativité. Par exemple, c'est souvent à la suite d'invitations de la part des organisations internationales que les États sont amenés à relayer des normes dans leurs législations. Par exemple, la *Convention sur la cybercriminalité*[181] a été mise de l'avant par les instances européennes et ouverte à la signature d'autres pays.

Les régulations peuvent découler de normativités technologiques, de normativités gestionnaires ou de normativités juridiques. Rien n'indique que la normativité juridique ou une autre logique normative soit invariablement en position dominante. Il y a en effet concurrence entre les diverses logiques en vertu desquelles se produisent les régulations : les logiques technologiques, celles du marché et les logiques du droit ne concordent pas toujours. Dans certaines situations, les référents juridiques demeurent absents des débats qui sont perçus comme relevant essentiellement d'une problématique de gestion ou d'agencement technique. Dans d'autres contextes, l'enjeu technique est fortement capté par les logiques juridiques.

---

180 Pierre TRUDEL, « Un 'droit en réseau' pour le réseau : le contrôle des communications et la responsabilité sur Internet », dans INSTITUT CANADIEN D'ÉTUDES JURIDIQUES SUPÉRIEURES, *Droits de la personne : Éthique et mondialisation,* Cowansville, Éditions Yvon Blais, 2004, pp. 221-262.

181 CONSEIL DE L'EUROPE, *Convention sur la cybercriminalité*, Budapest, 23 novembre 2001< http://conventions.coe.int/Treaty/fr/Treaties/Html/185.htm >

Les phénomènes associés au pourriel, à l'hameçonnage et aux espiogiciels se développent dans un environnement en réseau. Les polluposteurs profitent des forces mais aussi des faiblesses du réseau pour poser leurs gestes délictueux. La régulation destinée a faire face à ces fléaux doit donc se penser et s'appliquer en réseau. Il faut tisser un réseau de normes et de lieux de normativité qui agissent de façon concertée et qui se relaient mutuellement afin de limiter les risques qui découlent des actions délictueuses.

3.1 Renforcer les noeuds de normativité

Dans un modèle de réseau, les normativités sont pensées et exprimées dans divers lieux qui sont autant de noeuds de normativité.

Sur un territoire spécifique, le droit étatique constitue un nœud majeur de normativité : l'ensemble de ceux qui sont situés sur le territoire n'ont pratiquement pas le loisir d'ignorer la loi. Ils pourront toutefois être tentés de courir le risque de se trouver en situation de non-conformité avec une ou plusieurs lois s'ils ont le sentiment que ces lois sont peu appliquées ou que la volonté de les appliquer n'est pas apparente. On voit bien ici à quel point le cyberespace est un environnement dans lequel l'usager exerce une grande maîtrise. S'il a l'impression qu'il court peu de risques de se voir inquiété pour avoir ignoré les lois, il est plausible qu'il sera tenté prendre le risque de se livrer à une activité prohibée ou dommageable.

C'est pourquoi il est insuffisant à l'égard des activités se déroulant sur Internet à partir du territoire national de se limiter à adopter des lois si on n'est pas prêt à consacrer les énergies et les ressources pour les mettre effectivement en œuvre. Une telle situation peut même se révéler pire que le laisser-faire car elle peut comporter un risque de discréditer l'importance de la loi aux yeux de plusieurs usagers.

3.1.1 La mise à niveau des lois pénales et civiles

La mise à niveau des lois pénales et civiles suppose d'assurer l'ajustement des règles de droit aux contextes et pratiques. Ainsi, on visera à faire en sorte que les comportements analogues à ceux qui sont considérés comme contraires à l'ordre public ou dommageables hors du réseau soient visés par les textes lorsque commis au sein du réseau.

Pour la plupart des acteurs du cyberespace, la responsabilité au regard du droit d'un État ou de plusieurs se présente comme un ensemble de risques à gérer. Les personnes et entreprises doivent s'assurer que leurs pratiques sont conformes aux exigences des dispositions des lois susceptibles de trouver application et d'engager leur responsabilité. Ils chercheront à maîtriser les risques découlant de leurs activités en prenant les précautions susceptibles de garantir qu'elles s'en tiennent uniquement à un rôle compatible avec les responsabilités qu'elles sont prêtes à assumer.

Lorsqu'il existe des règles énoncées dans des textes de loi, les acteurs ont tendance à ajuster leurs pratiques de façon à limiter leurs risques de se retrouver en contravention avec celle-ci. Même si en elle-même, elle peut se révéler insuffisante, la loi est porteuse d'un effet symbolique : sa seule existence est comprise comme un message par la plupart des acteurs. Une loi qui est effectivement appliquée indique aux acteurs qu'il est préférable d'adopter un comportement exempt de pratiques nuisibles. C'est pourquoi il peut être opportun pour un État d'édicter des lois même si une partie des comportements visés sont peu susceptibles d'être effectivement sanctionnés par ces lois.

Mais le pourriel vise un ensemble diversifié de pratiques et de comportements. Par exemple, dans son *Rapport sur l'application des lois antispam*, le Groupe de réflexion sur le spam de l'OCDE constate que dans la plupart des situations, les pratiques pouvant être associées au pourriel vont relever tantôt d'une législation et d'un organisme chargé de son application, tantôt d'un autre organisme. Ainsi, au niveau fédéral canadien, le Bureau de la concurrence peut être compétent pour intervenir à l'égard de messages impliquant de la publicité trompeuse tandis que c'est le Commissaire à la vie privée qui pourra intervenir si la pratique reprochée consiste à avoir utilisé une adresse de courriel sans avoir obtenu le consentement

de la personne concernée. Dans l'affaire française Microsoft, c'est l'utilisation non autorisée d'une marque de commerce qui était reprochée au polluposteur[182].

C'est pourquoi la mise à niveau des lois doit, pour générer des résultats optimaux, concerner l'ensemble des situations pouvant être associées à des pratiques de pourriel. En plus, il faut garder à l'esprit que sur Internet, la normativité effective est fréquemment celle qui est énoncée dans les législations nationales et supra-nationales influentes. La prise en compte des législations nationales et supra-nationales influentes est nécessaire à la fois dans la conception des législations nationales et dans l'arrimage qui peut être envisagée avec les lois de juridictions des États exerçant plus d'influence sur le réseau.

La modification des lois relevant des divers champs d'activités susceptibles d'être concernés permet de disposer d'un vaste arsenal législatif qui peut être utilisé dans le cadre d'une stratégie concertée et intégrée. Comme le pourriel et autres fléaux d'Internet sont susceptibles de porter sur un ensemble varié de situations, des textes de lois à mettre à niveau peuvent se retrouver dans un vaste ensemble de domaines.

Le Canada est un État fédéral. La totalité des pouvoirs d'adopter des lois sont partagés entre le Parlement fédéral et les législatures des provinces. Dans leurs champs respectifs de compétences, les provinces et le Parlement fédéral peuvent adopter des lois portant sur l'une ou l'autre des facettes du phénomène du pourriel et fléaux connexes[183]. La transmission de pourriels, la mise en place de manœuvres de hameçonnage et l'installation d'espiogiciels sont des gestes qui sont visés par un ensemble de règles de droit qui existent déjà. Les comportements visés tombent en effet sous le coup de lois générales, comme le Code criminel ou l'article 1457 du Code civil qui prescrit que toute personne qui commet un acte fautif doit réparer le dommage qui en résulte. Un vaste ensemble de lois sectorielles peuvent trouver application selon le sujet abordé dans un message fautif.

C'est pourquoi le phénomène du pourriel, de l'hameçonnage et des espiogiciels pas plus d'ailleurs que le phénomène Internet dans sa globalité ne relèvent exclusivement ni du Parlement fédéral ni de l'Assemblée nationale. Aucun de ces deux ordres de gouvernement ne dispose de la totalité de la juridiction pour faire des lois sur ces phénomènes multiformes. Selon l'aspect visé, le Parlement ou la législature possèdera la compétence. Ainsi, les mesures qui créent des crimes ou celles qui constituent de la réglementation d'entreprises de télécommunications relèvent en principe du Parlement fédéral. D'autre part, les mesures relatives aux contrats, à la responsabilité civile, aux valeurs mobilières relèvent en principe de la législature provinciale. L'administration de la justice, y compris de la justice pénale, relève également, en principe, des provinces.

a) Lois criminelles

La mise à niveau des textes actuels édictant des infractions criminelles de même que la création de nouvelles incriminations permettraient de disposer d'un arsenal législatif mieux adapté. À cette fin, le Groupe fédéral de travail sur le pourriel a fait des recommandations.

---

182 Microsoft Corporation c/ E Nov Developpement, TGI Paris, 18 octobre 2006, *Juriscom.net* < http://www.juriscom.net/jpt/visu.php?ID=880 >. Dans cette décision, le tribunal estime que le fait d'utiliser à des fins de prospection commerciale une adresse e-mail qui reprend la marque d'un tiers dans son extension est susceptible d'en constituer un usage contrefaisant. Voir, Xavier JORELLE, « Le droit des marques entre dans la lutte contre le spam », *Juriscom.net*, 8-01-2007, < http://www.juriscom.net/actu/visu.php?ID=882 >

183 Karen NG, « Spam Legislation in Canada : Federalism, Freedom of Expression and the Regulation of the Internet », [2005] 2 *U. Ottawa L.& Tech. J.*, 447- 492.

Mais les polluposteurs opèrent sur de courtes périodes puis plient bagage[184]. Sans une politique assurant un relais adéquat des interdictions pénales, le risque d'être inquiété pour les polluposteurs paraît faible.

Les lois atteignent vite leurs limites. Les lois pénales sont généralement assujetties à de lourds fardeaux de preuve. En pratique, elles sont utilisées dans les situations où l'on dispose de preuves très solides.

b) Les règles de la responsabilité civile

Plusieurs recours sont fondés sur le droit privé. La plupart des gestes associés au pourriel, à l'hameçonnage et à l'usage des espiogiciels sont susceptibles de constituer des fautes civiles. L'application du principe général de la faute en responsabilité civile peut constituer une voie de recours fructueuse. Une stratégie intégrée de lutte devrait intégrer des moyens afin de mobiliser les recours civils qui pourraient éventuellement être entrepris à l'encontre de pratiques fautives et dommageables.

Au Québec, la responsabilité civile est fondée sur la faute. Celle-ci est définie par un procédé qui évite de déterminer a priori ce qui constitue un geste fautif[185]. La faute civile est définie comme un geste ou une omission que n'aurait pas commise une personne raisonnable placée en des circonstances similaires. Les « bons usages » généralement admis sur Internet peuvent constituer un facteur susceptible d'aider à déterminer si une personne a eu une conduite raisonnable[186].

Certains comportements associés au pourriel, aux espiogiciels et à l'hameçonnage ne sont habituellement pas ceux qu'ont les personnes raisonnables : ce sont assurément des comportements fautifs au sens du Code civil. La faute de violation de la vie privée vient spontanément à l'esprit à l'égard du pourriel, de l'hameçonnage et des espiogiciels. L'article 36 du Code civil du Québec énonce que peuvent être notamment considérés comme des atteintes à la vie privée d'une personne les actes suivants: intercepter ou utiliser volontairement une communication privée; surveiller sa vie privée par quelque moyen que ce soit et utiliser sa correspondance, ses manuscrits ou ses autres documents personnels.

En somme, plusieurs comportements associés à l'envoi de pourriels de même que les gestes dommageables qui les accompagnent pourraient constituer du harcèlement, ou même de l'abus de droit, deux situations constituant une faute au sens du Code civil.

Les recours en responsabilité sont largement conditionnés par les perspectives de gain que l'on peut en espérer. Sauf les situations où une entité tient à « faire un exemple », il est irréaliste de compter que les victimes de pourriel ou de hameçonnage intentent, sans aide, des recours en responsabilité civile à l'encontre de ceux qui auraient posé de tels gestes à leur égard.

c) Les législations sectorielles

Le pourriel peut comporter des pratiques visées par diverses lois sectorielles. La législation sur la concurrence, notamment les dispositions ayant trait à la publicité trompeuse et fausses représentations de même que la législation sur la protection des consommateurs peuvent s'appliquer à plusieurs

---

184 OCDE, *Rapport du Groupe de réflexion sur le spam de l'OCDE : Boîte à outils anti-spam de politiques et mesures recommandées,* 19 mai 2006, DSTI/CP/ICCP/SPAM/(2005)3/FINAL, p. 24.

185 L'article 1457 du Code civil renvoie au standard de la personne prudente et diligente. Il se lit comme suit :
1457. Toute personne a le devoir de respecter les règles de conduite qui, suivant les circonstances, les usages ou la loi, s'imposent à elle, de manière à ne pas causer de préjudice à autrui.
Elle est, lorsqu'elle est douée de raison et qu'elle manque à ce devoir, responsable du préjudice qu'elle cause par cette faute à autrui et tenue de réparer ce préjudice, qu'il soit corporel, moral ou matériel.
Elle est aussi tenue, en certains cas, de réparer le préjudice causé à autrui par le fait ou la faute d'une autre personne ou par le fait des biens qu'elle a sous sa garde.

186 Pierre TRUDEL, « La Lex electronica », dans Charles-Albert MORAND, *Le droit saisi par la mondialisation*, Bruxelles, Éditions Bruylant, 2001, 221, p. 242.

comportements caractéristiques du pouriel, de l'hameçonnage ou des espiogiciels. À l'égard de certains messages faisant la promotion de produits d'investissement, la législation sur les valeurs mobilières interdisant de proposer des valeurs mobilières (ou l'équivalent) au public est applicable. Enfin, la législation sur la protection des renseignements personnels sera fréquemment en cause.

Plusieurs gestes associés à ces fléaux tombent déjà sous le coup des lois générales. Mais il pourra être envisagé d'apporter des modifications à ces lois dans une perspective d'accroître les risques des polluposteurs. De telles modifications permettraient d'accentuer le message réprobateur à l'égard de ces pratiques. Il ne faut pas négliger l'effet dissuasif et symbolique des lois.

d) Une législation spécifiquement sur le pourriel

Les lois sont les véhicules privilégiés pour instituer les droits et les obligations. À l'époque post-moderne, la loi se présente davantage comme un énoncé de valeurs et principes généraux ayant vocation à être implantés dans une pluralité de situations. À l'égard de phénomènes complexes, la loi peut constituer un véhicule très efficace pour lancer un message dans l'espace social. L'effet d'annonce, le caractère symbolique attribué à la loi fait en sorte que c'est souvent un moyen de cristalliser une volonté d'encadrer un problème. La loi nomme les choses, identifie les objets qui doivent être régulés. En annonçant les objectifs à viser, elle indique la direction vers laquelle il faut tendre.

C'est pourquoi on pourrait trouver opportun d'adopter une loi sur le pourriel, l'hameçonnage et les espiogiciels même si plusieurs phénomènes associés à ces fléaux sont déjà largement pris en charge, comme on l'a vu, par les lois existantes. Évidemment, la loi peut énoncer des règles comportant des interdits spécifiques. Par exemple, le *Spam Act 2003* australien prohibe le recours à la collecte d'adresses de courriel de même que la fourniture et l'usage de logiciels à cette fin. Mais le message majeur de cette loi est de marquer une ferme volonté de prendre les moyens afin de réduire le pourriel en Australie

À l'égard des matières complexes et ayant un caractère changeant, la loi va souvent énoncer des objectifs à accomplir et indiquera des moyens afin d'y arriver[187]. Par exemple, à l'égard des fléaux d'Internet, un texte de loi peut énoncer certains principes comme celui de la préservation de l'intégrité des environnements de communication. La loi peut aussi identifier les mandats spécifiques des organismes au regard de la lutte contre le pourriel. La loi peut mettre en place une structure afin de favoriser les échanges entre les différents organismes qui sont susceptibles d'être concernés par les différents aspects des pratiques relatives au pourriel, à l'hameçonnage et aux espiogiciels.

Dans le cyberespace comme ailleurs, la personne ayant personnellement posé le geste fautif est évidemment la première à en assumer la responsabilité. La personne qui choisit de mettre en ligne une information ou se comporte de manière à exercer un contrôle sur la diffusion de celle-ci assume la responsabilité découlant de son caractère illicite ou délictueux. Ce principe demeure inchangé avec la *Loi concernant le cadre juridique des technologies de l'information*[188].

Mettre des informations en ligne, c'est assumer une fonction éditoriale. L'éditeur publie les informations. Publier signifie communiquer de l'information à des tiers en sachant que cette information sera lue, vue ou entendue. La publication s'effectuant de manière volontaire suppose une connaissance de la teneur de l'information transmise[189]. Dans le contexte d'Internet, la publication peut résulter de la transmission de fichiers, d'affichage de messages dans les sites de rencontres, de l'envoi d'un courriel ou encore par la

---

187 Charles-Albert MORAND, *Le droit néo-moderne des politiques publiques*, Paris, LGDJ, 1999, p. 189.

188 L.R.Q., c. C-1.1., voir, *Loi concernant le cadre juridique des technologies de l'information, texte annoté*, < http://www.msg.gouv.qc.ca/fr/enligne/loi_ti/index.asp >.

189 Loftus E. BECKER Jr., «The Liability of Computer Bulletin Board Operators for Defamation Posted by Others», (1989) 22 *Connecticut Law Review* 203-239, 217.

mise à disposition d'information dans des fichiers, des documents pouvant être transférés via le réseau. La personne qui pose le geste fautif est celle qui décide effectivement de le poser. Par contraste, la personne dont l'ordinateur aurait été illicitement détourné ne saurait être considérée comme ayant joué un rôle dans la transmission de matériel abusif.

Le champ d'application de la loi devrait être défini en termes neutres aussi bien au plan des gestes visés que de la technologie utilisée. Dans cet esprit, le recours à la notion de « document technologique » paraît constituer une avenue prometteuse. L'article 3 de la *Loi concernant le cadre juridique des technologies de l'information* définit ainsi la notion de document et de document technologique :

> ***3.*** *Un document est constitué d'information portée par un support. L'information y est délimitée et structurée, de façon tangible ou logique selon le support qui la porte, et elle est intelligible sous forme de mots, de sons ou d'images. L'information peut être rendue au moyen de tout mode d'écriture, y compris d'un système de symboles transcriptibles sous l'une de ces formes ou en un autre système de symboles.*
>
> ***(…)***
>
> *Les documents sur des supports faisant appel aux technologies de l'information visées au paragraphe 2° de l'article 1 sont qualifiés dans la présente loi de documents technologiques.*

Une avenue possible serait d'ajouter à la *Loi concernant le cadre juridique des technologies de l'information* des dispositions relatives aux usages abusifs des documents technologiques. La loi pourrait affirmer le principe selon lequel l'usage abusif, l'expédition abusive et la mise en place d'activités destinées à induire en erreur au moyen de documents technologiques constituent une faute civile donnant lieu à réparation. La loi devrait préciser que de tels gestes posés de façon intentionnelle donnent lieu à des dommages punitifs.

Une autre avenue serait d'insérer dans cette même loi une liste de pratiques associées au pourriel sur le modèle des pratiques abusives des articles 215 à 253 de la *loi sur la protection du consommateur*[190]

La lutte contre le pourriel et les fléaux qui y sont associés doit se concevoir en réseau. La coopération entre l'ensemble des acteurs n'est pas ici simplement souhaitable, c'est une condition de l'application efficace des mesures de lutte contre des phénomènes en métamorphose constante. Pour cette raison, une loi québécoise sur le pourriel et l'usage abusif des ressources Internet et des documents technologiques devrait préciser que le mandat de tout organisme exerçant des responsabilités à l'égard de l'un ou l'autre des gestes abusifs posés au moyen de documents technologiques doit se lire de manière à y inclure une habilitation à coopérer avec l'ensemble des entités, québécoises ou externes, qui interviennent dans la lutte contre l'un ou l'autre des gestes abusifs concernés.

Évidemment, il faudrait aussi préciser que des ressources seront mises à la disposition des organismes ayant à coopérer dans le cadre d'actions intersectorielles entreprises contre des pratiques abusives.

3.1.2 Les solutions technologiques

L'architecture technique s'entend de l'ensemble des éléments ou artefacts, tels les matériels, les logiciels, les standards et les configurations qui déterminent l'accès et les conditions d'utilisation des ressources technologiques. Plusieurs outils et solutions techniques peuvent être mobilisés afin de lutter contre certaines pratiques de pourriel.

---

190 L.R.Q., c. P40.1, Voir en général sur cette loi : Claude MASSE, *Loi sur la protection du consommateur, analyse et commentaires,* Cowansville, Éditions Yvon Blais, 1999.

Les objets techniques ont un effet régulateur se présentant suivant diverses formes[191]. La technologie alerte, habilite, permet, autorise, interdit. Par exemple, à l'égard du pourriel, des solutions technologiques existent afin de limiter le fléau. Des outils permettent de bloquer le pourriel au niveau du serveur de courriel du polluposteur. Il est possible de mobiliser des outils de blocage qui résident sur le serveur de l'entité réceptrice des messages. Enfin, il y a des outils contrôlés par les usagers eux-mêmes qui peuvent aider à bloquer le pourriel avant qu'il n'atteigne sa destination.

L'effet régulateur des éléments d'architecture peut être explicite. La volonté régulatrice peut être plus intense lorsque certains États imposent des contrôles sur les configurations techniques. L'effet régulateur peut être plus diffus : par exemple, les normes TCP/IP initiales visaient à constituer une architecture de réseau robuste. Il en est résulté un contexte favorable au développement d'un réseau décentralisé, Internet, qui est apparu par la suite peu accueillant à plusieurs initiatives régulatrices des États.

Comme une part significative des décisions relatives aux configurations techniques relèvent d'autorités non étatiques, le défi crucial est d'organiser l'arrimage entre ces forums qui définissent les règles, les instances de l'État et les activités spécifiques. Ce processus de relais est nécessaire afin d'assurer une cohérence entre la loi étatique et les limites et possibilités reconnues par les experts et les autres acteurs impliqués.

3.1.3 Les pratiques exemplaires

Si à l'origine le pourriel a été vite identifié comme une pratique inacceptable dans les énoncés de la « netiquette », on a rapidement constaté l'insuffisance de ces recommandations. Mais on convient de la nécessité de s'assurer de l'existence et de la diffusion appropriée de ce que les acteurs identifient comme étant de « bonnes pratiques » ou pratiques exemplaires afin de réduire les risques résultant du pourriel.

Les usages et pratiques se développent en général de façon graduelle et imperceptible, à la manière des règles jurisprudentielles. Les solutions apportées à chaque cas permettent de faire émerger graduellement les principes suivant lesquels les problèmes futurs seront résolus. De telles normes cèdent au droit étatique l'avantage de la stabilité et de la sécurité. Toutefois, les usages et pratiques ont l'avantage d'être plus près des participants. Leur évolution, plus rapide et mieux adaptée aux changements, représente l'expression d'un consensus sans cesse renouvelé.

Même si les usages et pratiques dans un champ d'activité donné sont souvent pris en compte et ainsi intégrés au droit étatique, l'intérêt de ce type de norme réside dans sa capacité à organiser de façon autonome les comportements et les transactions des membres d'une communauté. Le respect des usages et pratiques est, dans de telles circonstances, la condition essentielle de l'adhésion d'un participant à une communauté donnée. C'est à ces titres que les « bonnes pratiques » constituent une source de réglementation qui viendra souvent compléter les exigences plus formelles du droit étatique. En particulier, les « bonnes pratiques » sont souvent orientées vers les solutions afin de limiter les dégâts pouvant résulter des pratiques de pourriel.

Par exemple, un Sous-groupe du Groupe fédéral de travail sur le pourriel a élaboré des *Pratiques exemplaires recommandées pour les fournisseurs de services Internet et autres exploitants de réseaux*[192]. Le Sous-groupe a mis de l'avant une série de pratiques exemplaires techniques qu'il recommande dans le but de réduire le pourriel. Selon le Groupe, « De telles pratiques exemplaires représentent pour le Canada un modèle à partager à l'échelle internationale dans la lutte mondiale contre le pourriel. »

---

191 Joel REIDENBERG , « Lex Informatica », (1998) 76 *Texas Law Review*, 553-593; Lawrence LESSIG , « The Laws of Cyberspace » : http://cyber.law.harvard.edu/works/lessig/laws_cyberspace.pdf.

192 Groupe de travail sur le pourriel. Sous-groupe sur la gestion des technologies et des réseaux, mai 2005, http://www.e-com.ic.gc.ca/epic/site/ecic-ceac.nsf/fr/gv00347f.html .

Le défi est d'assurer la meilleure circulation possible de l'information à l'égard des pratiques exemplaires. C'est souvent à cette condition que ces dernières peuvent constituer un élément efficace d'une stratégie anti-pourriel.

3.1.4 Les normes mises de l'avant dans les forums internationaux

Les forums internationaux paraissent constituer le lieu le plus efficace de l'élaboration de méta-normes, celles qui sont exprimées sous forme de principes destinés à être relayés dans les législations nationales et dans les autres lieux d'élaboration de normativité. Tant les instances internationales conventionnelles que les associations non gouvernementales se présentent comme des lieux d'élaboration de méta-normes. Ce sont des lieux où l'on travaille à l'identification des dénominateurs communs.

C'est souvent dans les forums internationaux que sont établies les balises à caractère universel qui délimitent le licite et l'illicite. Afin de demeurer pertinentes face au rythme accéléré de l'évolution des pratiques de pourriel, ces instances doivent de plus en plus fonctionner en réseaux.

De plus, étant donné la nécessité de tenir compte d'un spectre très large de contextes dans lesquels la normativité aura à trouver application, les délibérations internationales donnent lieu à l'élaboration de principes se présentant comme ayant vocation à être relayés dans les ordres normatifs des États et des autres entités exerçant de l'influence.

Une stratégie complète de lutte au pourriel doit donc comporter une stratégie pour intervenir régulièrement au niveau des forums internationaux afin notamment d'assurer les relais des préceptes internationaux dans les pratiques québécoises.

3.2 Assurer les relais

Il importe d'identifier les processus par lesquels on obtient l'application effective[193] des règles dans un univers – tel Internet – présentant des coordonnées spatio-temporelles planétaires. Les relais sont les différents moyens par lesquels les acteurs reçoivent et appliquent effectivement les normes perçues par eux comme relevantes ou obligatoires.

Sur Internet, les règles que les usagers et autres acteurs considèrent relevantes ou obligatoires sont celles qui ont un impact sur les risques associés à leur activité. Par exemple, une entreprise qui décide d'être active sur Internet en mettant en place un site de transaction va nécessairement évaluer les lois et autres normes qu'elle doit suivre afin de minimiser ses risques. Elle considèrera relevantes, les règles qui sont effectivement susceptibles de trouver application à l'égard des activités qu'elle mène.

C'est ce phénomène qui explique que l'on ne se sent pas tenu d'être conforme aux exigences de toutes les lois de tous les pays de la planète lorsqu'on mène une activité sur Internet. En fait, on va considérer nécessaire d'être conforme uniquement aux lois qui sont susceptibles de trouver effectivement application à notre activité. Autrement dit, on s'assure de respecter les lois et autres normes qui peuvent effectivement nous être appliqués de façon significative. C'est généralement en faisant une évaluation des risques associés à la non-conformité avec les lois de pays avec lesquels on entretient ou prévoit entretenir des liens étroits que l'on identifie à quelles lois nationales il importe de se conformer lors de la réalisation d'une activité sur Internet. Par exemple, une entreprise située au Québec et envisageant de commercer aux États-Unis et en Europe ne se sentira pas obligée de se conformer aux lois du Népal même si son site est tout à fait susceptible d'être reçu sur le territoire népalais. À l'inverse, elle pourra trouver nécessaire de s'assurer d'être conforme aux lois québécoises, américaines et européennes.

---

193 On entend par effectivité, un degré suffisant de réalisation, dans les pratiques sociales, des règles énoncées. Voir sur cette notion : André-Jean ARNAUD (dir.) *Dictionnaire encyclopédique de théorie et de sociologie du droit*, 2e édition, Paris, L.G.D.J., 1993, p. 217.

Au niveau de l'activité de chacun des acteurs ou usager d'Internet, la gestion adéquate des risques suppose souvent d'anticiper les conflits et identifier de façon contextuée, comment seront relayées les exigences issues du droit ou des normativités qui, compte tenu des activités effectivement accomplies, risquent de trouver pratiquement application.

Par exemple, une entreprise devra se donner une politique afin de déterminer ce qui doit être fait lors de l'implantation de services sur Internet. Elle devra tenir compte de ce qui est tenu pour illicite dans le territoire dans lequel se trouvent ses infrastructures ou les lieux virtuels sur lesquels elle est en mesure d'exercer une activité significative. Pour évaluer les mesures à prendre, elle aura forcément à analyser les situations qui sont susceptibles de mettre en cause sa responsabilité.

Les relais rendent compte des processus de dialogue qui existent entre les divers pôles de normativité et entre les acteurs. Ces derniers ont forcément à prendre acte et à s'assurer qu'ils sont en conformité avec les règles qui sont impératives. Pour cela, ils devront les relayer à leurs partenaires et en combler les interstices afin d'en assurer une application concrète et effective.

3.2.1 Les stratégies de répression

Quelles que soient les mesures adoptées ou mises à niveau, les diverses règles doivent être appliquées dans le cadre d'une stratégie concertée. Des poursuites doivent être systématiquement entreprises afin de maximiser les effets dissuasifs. Dans certains cas, on tendra à maximiser l'effet de réconfort : rassurer les personnes victimes ou potentiellement susceptibles de le devenir.

L'un des relais majeurs entre les pôles de normativité et les acteurs est fourni par les régimes de responsabilité. Ceux qui prennent part à des activités sur Internet le font avec plus ou moins d'intensité selon l'ampleur de la responsabilité qu'ils auront à assumer et surtout le risque qu'ils courent d'avoir à répondre de leurs faits et gestes.

Pour la plupart des acteurs, la responsabilité au regard du droit d'un État ou de plusieurs se présente comme un ensemble de risques à gérer. Les personnes et entreprises doivent s'assurer que leurs pratiques sont conformes aux exigences des dispositions des lois susceptibles de trouver application et d'engager leur responsabilité.

Lorsqu'un préjudice est causé, l'on recherchera une sanction et une réparation. Alors, la normativité étatique sera souvent appelée en renfort. La responsabilité est le lieu où se joue le processus d'articulation entre les valeurs contradictoires que recèlent les droits et libertés. En départageant ce qui constitue un comportement fautif, les régimes de responsabilité contribuent à procurer les différentes hiérarchies et préséances entre les droits fondamentaux. Par exemple, un régime strict de responsabilité peut induire les acteurs à opter pour la mise en place de mesures et précautions.

3.2.2 Les initiatives du secteur privé

Plusieurs entreprises du secteur privé ont entrepris des actions afin de lutter contre les fléaux d'Internet. Une stratégie de lutte contre le pourriel suppose un arrimage avec les acteurs impliqués. Une politique de concertation avec les acteurs privés exerçant une influence est de nature à accentuer l'efficacité des mesures mises en place par un État. Pour optimiser les initiatives du secteur privé et des autres secteurs, il faut, dans toute la mesure du possible, promouvoir et valoriser les initiatives et bonnes pratiques mises en place ou expérimentées dans le secteur privé.

Les initiatives du secteur privé se retrouvent non seulement au niveau de la répression mais aussi en amont. Les pratiques contractuelles jouent un rôle significatif. Rappelons que c'est en invoquant une

disposition contractuelle qu'un tribunal ontarien a prononcé une sanction civile à l'encontre d'un polluposteur dans l'affaire *1267623 Ontario c. Nexx Online*[194].

La pratique contractuelle contribue largement à l'identification et au développement des usages élaborés par les multiples opérateurs d'Internet. Dans un environnement où la pratique contractuelle prend tant d'importance, le développement de guides et de contrats-types devient également un relais par lequel se traduisent concrètement les principes énoncés dans les lois et autres textes provenant d'autorités en mesure d'exercer une influence.

Une politique active de concertation autour de contrats-types peut constituer un jalon d'une stratégie intégrée de lutte au pourriel. Le contrat est l'outil de prédilection pour assurer le relais des obligations qui découlent des lois vers les parties qui sont en position d'y donner suite[195]. C'est aussi un moyen par lequel il est possible de transférer les risques découlant d'une activité. Par exemple, le contrat d'assurance procure un mécanisme de transfert de certains risques[196].

En fin de compte, une politique encourageant le développement de pratiques contractuelles visant à prévenir les comportement fautifs sur Internet contribue à relayer les principes normatifs exprimés dans les lois québécoises. Ce type de politique se définit souvent dans le cadre de processus de corégulation.

3.2.3 Les processus de corégulation

L'ensemble des risques associés au pourriel doivent être discutés et les solutions validées via un large spectre d'acteurs du secteur public, privé et communautaire: d'où l'intérêt des processus de corégulation. Les processus d'autorégulation et de corégulation[197] se révèlent d'importants relais des normativités encadrant les activités relatives à Internet. Par ces processus, on opère l'actualisation, l'adaptation et la particularisation des règles de droit considérées comme relevantes aux diverses activités prenant place sur Internet.

De tels processus peuvent s'envisager comme un cycle continu dans lequel les besoins et les exigences découlant des autres normativités, dont les lois étatiques, sont systématiquement discutés, évalués et ajustés de manière évolutive.

L'avènement d'un environnement en réseau dont Internet constitue l'archétype, a incité à mettre de l'avant le concept de corégulation. La généralisation d'Internet a engendré plusieurs réflexions sur le droit, la régulation et la réglementation. L'avènement d'un monde en réseau où les repères temporels et spatiaux semblent brouillés a stimulé l'intérêt pour les réflexions sur les normes et les divers facteurs encadrant les activités qui prennent place en tout ou en partie dans les réseaux ou dans les espaces virtuels qu'ils rendent possibles.

Le concept de corégulation a été mis de l'avant dès 1998 lors de la Conférence interministérielle de l'OCDE tenue à Ottawa qui souhaitait un « effective mix » d'interventions publique et privée afin de réguler le commerce électronique. Mais c'est en France que la notion de corégulation fera l'objet de travaux qui

---

194 [1999] O.J. n° 2246, voir : Marie-Hélène DESCHAMPS-MARQUIS, « Courriels indésirables, s'abstenir ! » *Juriscom.net*, octobre 1999, http://www.juriscom.net/int/dpt/dpt20.htm#note1.

195 Vincent GAUTRAIS, *L'encadrement juridique du contrat électronique international*, Bruxelles, Éditions Bruylant, 1998.

196 Richard V. ERICSON, Aaron DOYLE, Dean BARRY, *Insurance as Governance*, Toronto, University of Toronto Press, 2003, p. 8.

197 Jacques BERLEUR et Yves POULLET, « Quelles régulations pour l'Internet ? », dans Jacques BERLEUR, Christophe LAZARO et Robert QUECK, *Gouvernance de la société de l'information*, Bruxelles-Namur, Bruylant, Presses universitaires de Namur, 2002, pp. 133-151.

conduiront à une définition plus opératoire et à une mise en œuvre plus concrète du concept. Le Rapport du groupe dirigé par le député Christian Paul préconisait une approche de dialogue entre les acteurs.

La corégulation est moins une forme de normativité en tant que telle qu'un processus. Elle apparaît comme un espace où peut se construire un consensus entre les divers acteurs en mesure d'intervenir à divers titres dans la régulation. Bertrand DuMarais donne de la corégulation la définition suivante :

> *La co-régulation (ou terme plus explicite en anglais la policy cooperation…) s'analyse comme un lieu d'échange, de négociation entre les parties prenantes et les titulaires de la contrainte légitime et où se comparent les bonnes pratiques afin de les ériger en recommandations. Ce lieu peut également servir d'instance de médiation.*[198]

L'approche de corégulation est fondée sur la conviction qu'il est préférable de fonder la régulation d'Internet sur le partage des responsabilités entre les différents acteurs.

Une approche impliquant l'ensemble des acteurs favorise la mise en place d'une régulation beaucoup mieux acceptée et du coup plus efficace. Le caractère décentralisé d'Internet appelle une stratégie fondée sur un processus allant de bas vers le haut plutôt qu'une régulation imposée d'en haut. Une telle conception suppose des discussions ouvertes et équilibrées entre les intervenants du secteur public, de l'industrie et de la société civile. Ces discussions doivent mener à des solutions concrètes et pratiquement applicables par l'ensemble de ceux qui sont en mesure d'intervenir. Les règles peuvent prendre la forme de textes officiels comme des lois ou des règlements mais peuvent aussi emprunter la voie des guides de bonne conduite, des outils techniques ou des mises en garde.

Dans cet esprit, le réseau européen de corégulation de l'Internet met de l'avant un ensemble de recommandations pour une meilleure gouvernance de l'Internet. Ce réseau regroupe les organismes de corégulation d'Internet[199]. Il poursuit l'objectif de construire un réseau à l'échelle européenne sur les questions juridiques relatives à Internet. Il vise à organiser des débats entre les divers groupes d'intérêts et alimenter les diverses institutions communautaires européennes de suggestions sur des sujets relatifs à la régulation d'Internet.

Le mode d'opération d'un tel réseau est décentralisé. Le réseau n'a pas de hiérarchie : tous les organismes sont au même niveau. On opère de façon flexible. Pour certains membres, le réseau est un centre de ressources permettant l'échange et le partage d'information. Il permet d'être en contact continu sur des sujets d'intérêt. La densité et la configuration du réseau varient selon les demandes et selon les questions envisagées. Des groupes de travail sont mis sur pied et publient des recommandations. Le réseau se veut une structure ouverte, y compris à des entités non européennes.

Il pourrait être approprié d'envisager la possibilité de mettre en place, sur des modèles tels que le Forum français des droits sur l'Internet[200] ou le Oxford Internet Institute[201], un lieu d'échange voué à assurer les processus de corégulation en contexte québécois.

---

198 Bertrand DU MARAIS, « Autorégulation, régulation et co-régulation des réseaux, » dans Georges CHATILLON (éd.), *Le droit international de l'Internet*, Bruxelles, Bruylant, 2002, p. 296.

199 Il s'agit des organismes suivants : Confederation of European Computer User Associations, Forum per la tecnologia della informazione, Információs Társadalom-és Trendkutató Központ, Institutet för Rättsinformatik, Internet Watch Foundation, le Forum des droits sur l'Internet, ,l'Observatoire des droits de l'Internet l'Observatorium van de Rechten op het Internet, l'Oxford Internet Institute et l'Österreichisches Institut für angewandte Telekommunikation. Voir European Internet Coregulation Network, http://network.foruminternet.org/ .

200 Le Forum des droits sur l'Internet est un organisme formé selon la législation sur les associations, il regroupe des membres de l'industrie, du milieu de la recherche, du gouvernement et du monde associatif. Il s'est donné une mission de concertation et de veille. Voir: < http://www.foruminternet.org/ >.

3.2.4 L'éducation et la sensibilisation

Dans une approche fondée sur la gestion des risques d'Internet, le volet sensibilisation et éducation prend une importance considérable. Il faut en effet s'assurer que chaque usager est en mesure de reconnaître et de gérer à son niveau les risques. Dans un environnement ouvert tel qu'Internet, il est impossible de postuler qu'une entité quelconque est en mesure de se substituer à un usager pour reconnaître et gérer à sa place les risques.

Il faut également assurer l'information en continu sur les risques et fléaux d'Internet. Le caractère essentiellement évolutif de l'environnement interdit de postuler que les dangers sont connus et maîtrisés une fois pour toutes. Les nouvelles tendances, les « nouveaux trucs » doivent être identifiés et divulgués. Les stratégies les plus adéquates doivent être discutées et diffusées auprès des diverses catégories d'usagers.

Alors les politiques publiques doivent prévoir des moyens afin d'accroître le niveau de connaissance des usagers au sujet des risques d'Internet. Les sites procurant des informations à jour et adaptées aux différents besoins des internautes peuvent contribuer à prévenir plusieurs dommages[202].

3.2.5 La coopération nationale et internationale

Au plan national, il faut assurément mettre en place les conditions d'une étroite et quotidienne coopération entre l'ensemble des organismes ayant des responsabilités à l'égard des pratiques de pourriel et autres fléaux.

Au niveau intraquébécois, il importe d'assurer la mise en réseau des principaux organismes publics et privés qui exercent des responsabilités à l'égard de gestes associés au pourriel, hameçonnage et espiogiciels. Ainsi, l'Office de protection du consommateur (OPC), la Commission d'accès à l'information (CAI), les corporations professionnelles (pharmacie, médecine etc.), l'Autorité des marchés financiers (AMF) et les forces de police devraient être fortement incités à mettre en commun leurs informations afin de favoriser une lutte concertée. Une telle concertation doit également inclure les services concernés des entreprises privées qui ont un intérêt particulier au regard des pratiques abusives sur Internet.

Des voies équivalentes de coopération doivent être pratiquées avec les organismes fédéraux et ceux qui relèvent des autres provinces.

Du fait de la nature même d'Internet, tous reconnaissent la nécessité de la coopération internationale. Mais la volonté de coopérer est freinée par la multiplicité d'entités qui, au niveau de chaque État, exercent des responsabilités dans l'une ou l'autre des activités concernées par le pourriel.

La coordination interétatique est aussi freinée par le coût élevé des enquêtes et des mesures de répression. Plusieurs pays trouveront opportun de mettre des ressources en coopération uniquement à l'égard des pratiques causant des dommages significatifs[203].

---

201 Le Oxford Internet Institute est une entité universitaire. Il assure des tâches de recherche et anime des initiatives de concertation entre les divers acteurs d'Internet. Voir: < http://www.oii.ox.ac.uk/ >

202 Par exemple : « Conseils pour un Internet sécuritaire combattre le pourriel, les logiciels espions et l'hameçonnage » < http://arretezlepourrielici.ca/index.html>.

203 Meyer POTASHMAN, « International Spam Regulation & Enforcement : Recommendations Following the World Summit on the Information Society, » [2006] 29 *Boston College International & Comparative Rev.*, 322, pp. 344-345.

3.2.6 Le monitoring des tendances

L'évolution accélérée des pratiques sur Internet impose une capacité de veille assurant le relais des informations nécessaires pour maintenir constamment le niveau de vigilance nécessaire. Sans une capacité suffisante de monitoring, les mesures et stratégies mises en place risquent de devenir vite périmées.

CONCLUSION

S'il fut un temps où la lutte contre le pourriel pouvait s'envisager comme une mesure prescrivant aux entreprises d'obtenir la permission des internautes avant de leur expédier un message promotionnel, les choses ont radicalement changé. Le pourriel aujourd'hui et pour un avenir prévisible est une cible mobile pour les régulateurs. Les pratiques évoluent avec le développement des possibilités techniques et ne sont limités que par l'extraordinaire capacité d'imagination de tout esprit désireux de tromper. Face à ce redoutable défi, l'action doit être conçue en réseau : il faut des règles à la fois souples et exhaustives. Les règles, qu'elles proviennent de l'État, des entités privées ou des usages techniques doivent être tenues à jour et surtout efficacement relayées dans un réseau de l'ensemble des entités ayant mandat d'enrayer l'une et l'autre des facettes de ces fléaux.

Le souci de gérer les risques d'Internet motive et justifie un encadrement normatif conséquent, c'est-à-dire, une approche qui maximise les risques de ceux qui abusent et qui minimise ceux qui font un usage légitime des ressources du réseau. Un tel impératif est encore plus important lorsqu'il s'agit de lutter contre le pourriel et les fléaux qui y sont associés. Les normes sont élaborées afin de gérer les risques perçus ou avérés des pratiques du réseau.

Les caractéristiques d'Internet commandent une stratégie en réseau de lutte au pourriel mobilisant un ensemble de normativités. Les normes sont énoncées par un vaste ensemble d'instances publiques, privées, nationales ou internationales. Le modèle du réseau permet de rendre compte de la façon dont s'énoncent et s'appliquent les normativités. Ce modèle paraît plus adéquat que ceux qui postulent des institutions hiérarchisées comme lieu de d'énonciation et d'application de la normativité. Au sein des réseaux s'élaborent des principes qui doivent habituellement être relayés par d'autres lieux de normativité. D'où l'idée d'une régulation qui doit être relayée dans plusieurs vecteurs pour une effectivité optimale.

Les règles de droit et les autres normativités tendent de plus en plus à s'appliquer via un processus complexe de transferts de risques. Les groupes d'intérêts demandent la mise en place de normes pour contraindre les acteurs à prendre des mesures afin de limiter les risques d'Internet. Pour accentuer l'efficacité de telles revendications, ils viseront à créer des risques pour les décideurs qui s'aviseraient d'ignorer leurs revendications. Souvent, les organisations internationales seront mobilisées afin de reconnaître les risques et formuler des principes destinés à en assurer la prise en charge. Les instances gouvernementales, s'appuyant sur de tels principes, pourront formuler des règles plus ou moins contraignantes transférant ainsi aux acteurs - notamment les entreprises - la charge des risques. À leur tour, les acteurs chercheront, dans leurs pratiques contractuelles et les autres régulations sur lesquelles ils ont de l'influence, à transférer les risques.

Les principes mis en place par les régulateurs nationaux sont relayés par les normes mises en place par les acteurs. Les réseaux s'ajoutent ainsi aux lieux institutionnels que sont les États et les instances internationales[204]. De tels énoncés s'insèrent dans des processus de dialogue par lesquels se structurent les stratégies capables de répondre aux contextes engendrés par les objets techniques. Il en résulte des phénomènes de corégulation que les États doivent prendre en compte s'ils souhaitent prendre une part active à la lutte contre le pourriel.

Une stratégie efficace de lutte contre le pourriel, l'hameçonnage et les espiogiciels doit donc s'articuler dans l'ensemble du réseau de normativités que constitue désormais Internet. La législation et la réglementation étatique doivent certes être mises à niveau mais cela ne donnera rien s'il n'y a pas une stratégie concertée de suivi et d'application systématique des règles. Une telle stratégie doit

204 François OST et Michel de KERCHOVE, « De la pyramide au réseau ? Vers un nouveau mode de production du droit ?, (2000) 44 *Revue interdisciplinaire d'études juridiques*, 1- 82.

nécessairement impliquer l'ensemble des acteurs et être conçue de façon à être constamment mise à jour. Avant même d'envisager l'adoption de lois nouvelles, il conviendrait de mettre en place un réseau de vigilance ayant pour but d'appliquer les règles actuelles, notamment celles du droit commun aux situations découlant d'agissements menés sur le territoire du Québec. Les enseignements découlant du fonctionnement d'un pareil réseau permettraient l'élaboration d'une législation et de stratégies adaptées aux contextes changeants dans lesquels sévissent les pratiques de pourriel.

BIBLIOGRAPHIE SÉLECTIVE

Australian Communications and Media Authority (ACMA), *Fighting Spam in Australia-A Consumer Guide*, http://www.acma.gov.au/webwr/consumer_info/spam/consumer_information/spam_consumerguide.pdf.

Australian Communications and Media Authority (ACMA), *Spam Act 2003: A Practical Guide for Business*, http://www.acma.gov.au/webwr/consumer_info/frequently_asked_questions/spam_business_practical_guide.pdf.

Australian Communications and Media Authority (ACMA), *Spam-Junk email & messages*, http://www.acma.gov.au/WEB/STANDARD//pc=PC_2008.

Australian Communications and Media Authority (ACMA), *Australian eMarketing Code of Practice*, (2005), http://www.acma.gov.au/webwr/telcomm/industry_codes/codes/australian%20emarketing%20code%20of%20practice.pdf.

ACA, Australian Communications Authority, Australian Government, *Spam Act 2003: A Practical Guide for Business, National office for Information Economy*, February 2004.

AEEMA, *Spam Act 2003 Review: A legislative review of the operation of the Spam Act 2003 and related parts of the Telecommunications Act 1997 AEEMA Response*, February 1st, 2006.

ALONGI, E. A., "Has the U.S. Canned Spam?", (2004) 46 *Ariz. L. Rev.* 262.

ARORA, V., "The CAN-SPAM Act: An Inadequate Attempt to Deal with a Growing Problem", (2006) 39 *Colombia Journal of Law and Social Problems* 299.

AusCERT, *Spam Act 2003 Review: Submission from AusCERT*, (2006).

BAXTER, P.W, "Has Spam Been Canned? Consumers, Marketers, and the Making of the CAN-SPAM Act of 2003", (2005) 8 *NYU Journal of Legislation and Public Policy* 163.

BERLEUR, J. et Y. POULLET, « Quelles régulations pour l'Internet ? », dans Jacques BERLEUR, Christophe LAZARO et Robert QUECK, *Gouvernance de la société de l'information*, Bruxelles-Namur, Bruylant, Presses universitaires de Namur, 2002.

BOLIN, Rebecca, "Opting Out of Spam: A Domain Level Do-Not-Spam Registry", (2006) 24 *Yale L. & Pol'y Rev.* 399.

BUENAVENTURA, M.A, "Teaching Man to Fish: Why National Legislation Anchored in Notice and Consent Provisions is the Most Effective Solution to the Spyware Problem", (2006) 8 *Richmond Journal of Law & Technology* 1.

CALMAN, C., "Bigger Phish to Fry: California's Anti-Phishing Statute and its Potential Imposition of Secondary Liability on Internet Service Providers", (2006) 8 *Richmond Journal of Law & Technology* 1.

CAN-SPAM a year later, PIP Senior Research Fellow Deborah Fallows (202-419-4500), april 2005.

CASTELLS, Manuel, *The Rise of Network Society*, 2nd ed., Oxford and Cambridge, Mass, Blackwell, 2000.

Clinique d'intérêt public et de politique d'Internet du Canada, *Un droit privé d'action prévu par la loi contre les polluposteurs au Canada : Contexte canadien, leçons apprises et répercussions des diverses approches*, Rapport présenté au Groupe de travail sur le pourriel d'Industrie Canada, 17 décembre 2004.

Clinique d'intérêt public et de politique d'Internet du Canada, (CIPPIC), *FAQs and Resources-Spam*, < http://www.cippic.ca/en/faqs-resources/spam/ >

CNIL, *Spam : L'état du droit en France*, www.cnil.fr.

Commission des communautés européennes, *Communication de la Commission au Parlement européen, au Conseil , au Comité économique et social européen et au Comité des régions sur la lutte contre le pourriel, les espiogiciels et les logiciels malveillants*, 15 novembre 2006, COM(2006) 688 final.

Commission des communautés européennes, *Communication de la Commission au Parlement européen, au Conseil , au Comité économique et social européen et au Comité des régions sur les communications commerciales non sollicitées ou « spam »,* 22 janvier 2004, COM(2004) 28 final.

DANIEL, J.W, "Has Spam Been Fried? Why the CAN-SPAM Act of 2003 Can't: Regulation and Unsolicited Commercial Electronic Mail and the CAN-SPAM Act of 2003.", (2005-2006) 94 *Kentucky Law Journal* 363.

DESCHAMPS-MARQUIS, Marie-Hélène, « Courriels indésirables, s'abstenir ! » *Juriscom.net*, octobre 1999, http://www.juriscom.net/int/dpt/dpt20.htm#note1.

DRORI, O. « Commercial and non-commercial approaches to fighting SPAM », *Virus Bulletin Conference* (2005), http://www.commtouch.com/downloads/VB2005_Approaches_To_Fighting_Spam.pdf.

DU MARAIS, B., « Autorégulation, régulation et co-régulation des réseaux », dans Georges CHATILLON (éd.), *Le droit international de l'Internet*, Bruxelles, Bruylant, 2002, 296 p.

ERICSON, R.V., A. DOYLE, D. BARRY, *Insurance as Governance*, Toronto, University of Toronto Press, 2003.

European Internet Co regulation Network, http://network.foruminternet.org/ .

Ferris Research, "The Global Economic Impact of Spam" (2005).

FORD, R.A, "Preemption of State Spam Laws by the Federal CAN-SPAM Act", (2005) 72 *U. Chi. L. Rev.* 355

Forum des droits sur l'Internet*, De quelques dangers en « ing »*, 28 septembre 2006, http://www.foruminternet.org/actualites/lire.phtml?id=1112.

Forum des droits sur l'Internet, *Recommandation-Les publiciels et espiogiciels*, 11 juillet 2006, http://www.forum internet.org/recommandations/lire.phtml?id=1094.

GARRIE, Daniel B., Alan F. BLAKELEY, Matthew J. ARMSTRONG, "The Legal Status of Spyware", (2006) 59 *Federal Comm. L.J.*, 161.

GAUTRAIS, Vincent, *L'encadrement juridique du contrat électronique international*, Bruxelles, Éditions Bruylant, 1998.

GEIST, Michael, *Untouchable? : A Canadian Perspective on the Anti-Spam Battle*, version 1.1, May 2004.

Groupe de travail sur le pourriel, *Comparaison des mesures internationales de lutte contre le pourriel*, mai 2005.

Groupe de travail sur le pourriel, Rapport du Groupe de travail sur le pourriel, *Freinons le pourriel - Créer un Internet plus fort et plus sécuritaire*, Mai 2005, http://www.e-com.ic.gc.ca/epic/site/ecic-ceac.nsf/fr/h_gv00317f.html.

Groupe de travail sur le pourriel, Sous-groupe sur la gestion des technologies et des réseaux, *Pratiques exemplaires recommandées pour les fournisseurs de services Internet et autres exploitants de réseaux*, mai 2005, http://e-com.ic.gc.ca/epic/site/ecic-ceac.nsf/fr/gv00347f.html.

Groupe de travail sur le pourriel, Sous-groupe sur la validation du courriel commercial, *Pratiques exemplaires recommandées pour le marketing par courriel*, Mai 2005, http://e-com.ic.gc.ca/epic/site/ecic-ceac.nsf/fr/h_gv00348f.html.

HAMEL, Adam, "Will the CAN-SPAM Act of 2003 Finally Put A Lid On Unsolicited E-Mail?" (2004-2005) 39 *New England Law Review* 961.

HLADJK, Jörg, "Effective EU and US approaches to spam? Moves towards a co-ordinated technical and legal response", [2005] 10 *Communications Law*, 71-83 et 111-120.

IIA, Internet Industry Association, *Internet Industry Spam Code of Practice-A Code for Internet and Email Service Providers, Co-Regulation in Matters Relating to Spam Email* (Consistent with the Requirements of the Spam Act 2003 and Telecommunications Act 1997 to the Extent it Relates to the Spam Act), December 2005, Version 1.0.www.iia.net.au.

INDUSTRIE CANADA, « Télémercatique: Offrir un choix au consommateur et créer des possibilités d'affaire », document de discussion, janvier 2003, http://e-com.ic.gc.ca/epic/site/ecic-ceac.nsf/fr/gv00189f.html.

INDUSTRIE CANADA, *Un plan d'action anti-pourriel pour le Canada*, mai 2004, http://strategis.ic.gc.ca/epic/site/ecic-ceac.nsf/fr/h_gv00246f.html.

LEDBETTER, T.K, "Stopping Unsolicited Commercial E-Mail: Why the CAN-SPAM Act Is Not the Solution to Stop Spam", (2004-2005) 34 *Southwestern Law Review* 107

LESSIG, Lawrence, « The Laws of Cyberspace » : http://cyber.law.harvard.edu/works/lessig/laws_cyberspace.pdf.

LYNCH, J., "Identity Theft in Cyberspace: Crime Control Methods and Their Effectiveness in Combating Phishing Attacks", (2005) 20 *Berkeley Technology Law Journal* 259

MARKS, E.E., "Spammers Clog In-Boxes Everywhere: Will the CAN-SPAM Act of 2003 Halt the Invasion?", (2004) 54 *Case Western Reserve Law Review* 943

MOSHCHUK, A., et al., « A Crawler based study of Spyware on the Web », www.isoc.org/isoc/conferences/ ndss/06/proceedings/htmI/2006/papers/spycrawler.pdf, p.11.

NG, Karen, « Spam Legislation in Canada : Federalism, Freedom of Expression and the Regulation of the Internet », (2005) 2 *U. Ottawa L.& Tech. J.*, 447.

OCDE, Groupe de réflexion sur le spam, *La réglementation anti-spam*, 24 novembre 2005, DSTI/CP/ICCP/SPAM/(2005) 10/FINAL.

OCDE, Groupe de réflexion sur le spam, *Rapport sur l'application des lois antispam*, 30 août 2005, DSTI/CP/ICCP/SPAM/(2004) 3/FINAL.

OCDE, *Rapport du Groupe de réflexion sur le spam de l'OCDE : Boîte à outils anti-spam de politiques et mesures recommandées*, 19 mai 2006, DSTI/CP/ICCP/SPAM/(2005)3/FINAL, < http://www.oecd-antispam.org/IMG/pdf/Toolkit_2005_3_FINAL_FRE-2.pdf>

OCDE, Task Force on Spam, *Education and Awareness Raising*, 4 août 2005, DSTI/CP/ICCP/SPAM/(2005)4/FINAL.

OST, François et Michel de KERCHOVE, « De la pyramide au réseau ? Vers un nouveau mode de production du droit ?, (2000) 44 *Revue interdisciplinaire d'études juridiques*, 1- 82.

PINES, E., "Spyware Regulations: National Legislation Should Prompt Industry Self-Policing", (2004-2995) 38 *Loyola of Los Angeles Law Review* 2219.

POTASHMAN, Meyer, "International Spam Regulation & Enforcement: Recommendations Following the World Summit on the Information Society", (2006) 29 *Boston College International & Comparative Law Rev.*, 323.

REED STARK, John et Carolyn E. KURR, "Using the Securities and Exchange Commission's Statutory Weaponry to Combat Spam", [2006] 37 *University of Toledo Law Rev.*, 271-305.

REIDENBERG, Joel, « Lex Informatica », (1998) 76 *Texas Law Review*, 553-593.

SCHULTZ, T., « La régulation en réseau du cyberespace », (2005) 55 *R.I.E.J.*, 31

SORKIN, D.E., "Spam Laws", http://www.spamlaws.com/

SORKIN, D.E., "Technical and Legal Approaches to Unsolicited Electronic Mail", (2000-2001) 35 *University of San Fransisco Law Review* 326.

SORKIN, D.E., Spam Legislation in the United States, (2003) 22 *John Marshall Journal of Computer & Information Law* 1.

SULLIVAN, J.D., & M.B. de LEEUW, "Spam After CAN-SPAM: How Inconsistent Thinking Has Made A Hash Out Of Unsolicited Commercial E-Mail Policy," (2003-2004) 20 *Santa Clara Computer & High Tech. L.J.* 888

TRUDEL, P., « Un 'droit en réseau' pour le réseau : le contrôle des communications et la responsabilité sur Internet », dans Institut canadien d'études juridiques supérieures, *Droits de la personne : Éthique et mondialisation*, Cowansville, Éditions Yvon Blais, 2004, 221 p.

TRUDEL, Pierre, "La Lex electronica", dans Charles-Albert MORAND, *Le droit saisi par la mondialisation*, Bruxelles, Éditions Bruylant, 2001, 221.

VERDUN, Franck, *La gestion des risques juridiques*, Paris, Éditions d'organisation, 2006.

WERY, Étienne, « La Commission européenne déclare la guerre totale au spam :elle dévoile un plan d'attaque pluri-annuel », *Droit et Nouvelles technologies*, 30 janvier 2004, http://www.droit-technologie.org/1_2.asp?actu_id=883.

ZHANG, L., "The CAN-SPAM Act: An Insufficient Response to the Growing Spam Problem", (2005) 20 *Berkeley Technology Law Journal* 301.