Non classifié **DSTI/ICCP(2003)10/FINAL**

Organisation de Coopération et de Développement Economiques
Organisation for Economic Co-operation and Development

09-Feb-2004

Français - Or. Anglais

DIRECTION DE LA SCIENCE, DE LA TECHNOLOGIE ET DE L'INDUSTRIE
COMITE DE LA POLITIQUE DE L'INFORMATION, DE L'INFORMATIQUE ET DES COMMUNICATIONS

NOTE DE SYNTHÈSE POUR L'ATELIER DE L'OCDE SUR LE SPAM

JT00158014

DSTI/ICCP(2003)10/FINAL
Non classifié

Français - Or. Anglais

AVANT-PROPOS

La présente note a été présenté au Groupe de travail sur les politiques en matière de télécommunications et de services de l'information, au Groupe de travail sur la sécurité de l'information et la vie privée et au Comité de la politique à l'égard des consommateurs lors de leurs réunions en 2003. Le Comité de la politique de l'information, de l'informatique et des communications a recommandé la mise en diffusion générale de ce rapport en janvier 2004.

Le rapport a été préparé par M. Sung-il Ahn de la Direction de la science, de la technologie et de l'industrie. Il est publié sous la responsabilité du Secrétaire général de l'OCDE.

NOTE DE SYNTHÈSE POUR L'ATELIER DE L'OCDE SUR LE SPAM

TABLE DES MATIÈRES

INTRODUCTION

Le rôle déterminant de l'Internet et du courrier électronique

Avec la progression de son nombre d'usagers, l'Internet devient peu à peu un élément intégrant de la vie courante. Son expansion devrait se poursuivre. On comptait 213 millions d'usagers du réseau dans la zone de l'OCDE en 2001[1] et plus d 591 millions dans le monde en 2002.[2] Le nombre mondial d'internautes devrait se situer entre 709,1 millions et 945 millions en 2004.[3]

Bon nombre d'analystes du marché ont vu dans le courrier électronique l'une des applications phares qui stimulerait la croissance de l'Internet. Le courrier électronique est en train de s'imposer rapidement, aux côtés du téléphone, comme un outil de communication essentiel dans la vie professionnelle et sociale. Il est devenu un mode de communication puissant, pour l'échange d'idées et d'informations d'une part, mais aussi pour le commerce électronique, notamment le marketing direct. Grâce à sa rapidité et à son coût relativement modique, il est devenu l'un des principaux outils de communication à usage personnel et professionnel.

L'International Data Corporation (IDC) évalue à quelque 700 millions le nombre de boîtes aux lettres électroniques dans le monde, et estime que ce chiffre atteindra 1,2 milliard en 2005.[4] Selon elle, le volume de courriers électroniques va continuer de progresser rapidement. Les estimations suggèrent que quelque 31 milliards de messages auraient été expédiés via l'Internet en 2002, et ce chiffre atteindrait ou dépasserait les 60 milliards en 2006.[5]

Progression du pollupostage (spam)

Le développement de l'Internet et du courrier électronique s'est accompagné d'une croissance spectaculaire des messages électroniques en nombre non sollicités (couramment appelés « spam » ou « pourriels ») ces dernières années. [6] L'Internet étant accessible dans plus de 200 pays, le spam peut émaner de toutes les régions du globe. La facilité avec laquelle les polluposteurs peuvent changer de serveur d'origine pour envoyer leurs messages signifie que même si la culture nationale en matière de commercialisation électronique décourage cette pratique ou s'il existe des restrictions juridiques, les messages spam peuvent aisément être envoyés à partir d'autres endroits. Malgré le déploiement grandissant de services et technologies anti-spam, le nombre de ces messages continue d'augmenter rapidement.

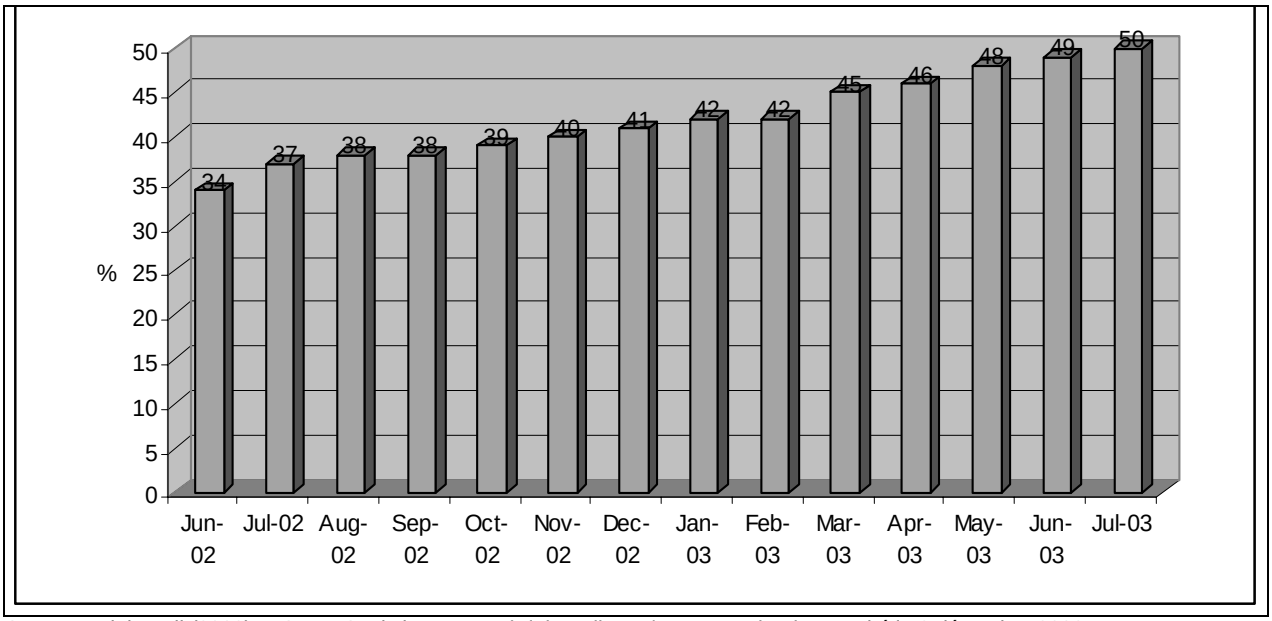
Les statistiques présentées à la figure 1 illustrent la progression rapide du spam ces derniers temps. Selon Brightmail, une société de logiciels anti-spam, le volume de pourriels représentait 50% de l'ensemble du trafic de courrier électronique sur l'Internet en juillet 2003, contre à peine 8 % au milieu de 2001. Une autre société de solutions anti-spam, MessageLabs, a constaté que 55 % des courriers électroniques qu'elle balayait étaient des messages non sollicités en mai 2003. Le groupe Radicati estime que 4,9 billions de messages spam seront envoyés en 2003.[7] Leur taux de croissance devrait augmenter à l'avenir.

Le problème du spam ne concerne pas seulement les comptes de courrier électronique personnels, mais aussi les comptes professionnels. America Online (AOL), un fournisseur de services Internet (FAI) a

notamment bloqué 2,37 milliards de messages spam par jour en avril 2003. Cela signifie une augmentation des coûts et des risques de sécurité pour les entreprises comme pour les consommateurs.

Même si quelques grands prestataires de services de messagerie électronique et sociétés d'études communiquent les données dont ils disposent sur le spam, il serait utile de disposer de plus amples informations quant aux problèmes qu'il provoque, à son taux de croissance, et aux résultats des diverses solutions proposées pour établir un diagnostic plus précis de la situation actuelle et formuler des mesures anti-spam. Il conviendrait par ailleurs d'engager une réflexion pour définir quels organismes seraient compétents pour recueillir des données à cet égard.

Figure 1. **Pourcentages du nombre total des messages électroniques définis comme étant du spam selon Brightmail**



Source : Brightmail (2003), « Spam Statistics », www.brightmail.com/spamstats.html, consulté le 8 décembre 2003.

Effets pernicieux du spam sur la confiance des consommateurs

La croissance et le succès du courrier électronique reposent sur la confiance des consommateurs. Pour que l'expansion commerciale de l'Internet se poursuive et se renforce, il faut que les usagers aient confiance dans la sécurité et la facilité d'utilisation de cet outil électronique. La forte progression du spam risque d'émousser la confiance des consommateurs en ligne, ce qui nuit à son tour au développement de l'économie numérique. Le caractère envahissant du spam, et le fait qu'il est aussi en grande partie associé à des activités commerciales frauduleuses, trompeuses ou pornographiques ont, en portant atteinte à la confiance des consommateurs et à la crédibilité du marketing électronique, compromis le développement du commerce électronique.

Objet et portée du présent document

Ce document a été rédigé pour fournir des informations de référence aux participants à l'atelier de l'OCDE sur le spam qui se tiendra à Bruxelles les 2 et 3 février 2004. Il contient une étude liminaire des problèmes provoqués par le spam ou qui lui sont associés. Il cherche à définir ses caractéristiques, les raisons pour lesquelles il est en expansion et plusieurs des problèmes qu'il soulève, à savoir : les coûts

qu'il induit, son impact sur les infrastructures et marchés de communication, les atteintes à la vie privée et le vol d'informations commerciales, son contenu, et les questions de sécurité du réseau et de protection du consommateur. Le document a aussi pour objectif de présenter un panorama des mesures prises par les pays Membres dans ce domaine afin de faciliter l'échange d'informations quant à l'effet des différentes solutions mises en œuvre. Enfin, il a pour ambition de servir de base à d'autres débats et échanges de renseignements entre les pays Membres afin de lutter contre le spam au niveau national et international.

TOUR D'HORIZON DU SPAM

Qu'est-ce que le spam ?

De la difficulté de définir le spam

Il serait utile de disposer d'une définition du « spam », mais aucune ne semble à ce stade convenir et faire l'unanimité. Une définition exhaustive devrait prendre en compte divers éléments ayant trait au comportement commercial, à la psychologie des destinataires, au contexte juridique global, à des considérations économiques et à des questions techniques. Pour compliquer la situation, le mot « spam » lui-même n'est pas directement lié au phénomène.[8] Enfin, bien évidemment, le phénomène est perçu de manière différente selon les pays. Plusieurs ont toutefois adopté des définitions de travail générales. On trouvera ci-dessous une description des méthodes appliquées en France, en Australie et par la Commission européenne. Grâce à ces définitions et à d'autres analyses du spam, il est possible de définir plusieurs de ses caractéristiques.

En France, la *Commission Nationale de l'Informatique et des Libertés* définit le « spamming » ou « spam » comme l'envoi massif et parfois répété de courriers électroniques non sollicités à des personnes avec lesquelles l'expéditeur n'a jamais eu de contact, et dont il a capté l'adresse électronique de façon irrégulière.

Selon un rapport de la Commission européenne paru en 2001, « Communications commerciales non sollicitées et protection des données », *« le spamming est généralement considéré comme l'envoi massif et répété de messages commerciaux non sollicités provenant d'un expéditeur qui masque ou falsifie son identité.* » En cela, il constitue évidemment une méthode de prospection qui n'a pas été sollicitée. Cependant, il se distingue par son caractère massif, répété et déloyal. En un mot, le spamming est forcément de la prospection commerciale non sollicitée, mais toute prospection commerciale non sollicitée n'est pas du spamming ».[9]

Le « *Final Report of the NOIE (National Office for the Information Economy) Review of the Spam Problem and How It Can Be Countered* » australien, paru en 2003, établit que *« le spam est le terme désormais généralement employé pour désigner les messages électroniques non sollicités, normalement adressés à de nombreux destinataires. »* Ils ont parfois, mais pas nécessairement, un caractère commercial (publicité ou vente de produits ou services) ; ils présentent par ailleurs une ou plusieurs caractéristique(s) commune(s) :

- ils sont envoyés sans discernement, sans cible définie, souvent par des moyens automatisés ;
- ils comportent ou diffusent un contenu illégal ou offensant ;
- ils ont une intention frauduleuse ou autrement trompeuse ;
- ils collectent ou utilisent les renseignements personnels en violation des principes nationaux sur la vie privée stipulés dans la loi sur la vie privée de 1988 ;
- ils sont envoyés de manière à masquer l'identité de l'expéditeur ;
- ils ne contiennent pas d'adresse valable ou fonctionnelle à laquelle les destinataires pourraient envoyer un message pour refuser de recevoir d'autres messages non sollicités ».[10]

Caractéristiques du spam

D'après les commentaires énoncés ci-dessus et ailleurs, on peut associer au spam les caractéristiques suivantes[11] :

- **Messages électroniques :** les messages spam sont envoyés par voie électronique. Si le courrier électronique est de loin le moyen le plus employé, les services de messagerie (SMS) ou SM-Caster (spam messenger, ou services d'affichage des messages) sont aussi utilisés.
- **Envoi en nombre** : les messages spam sont généralement envoyés en masse, mais peuvent être expédiés en plus petit nombre par l'intermédiaire de comptes de messagerie électronique « gratuits ».
- **Non sollicités :** le spam est envoyé sans que le destinataire l'ait demandé ou y ait consenti. Il peut être difficile de définir si un message est non sollicité dans les cas où l'expéditeur et le destinataire ont déjà été en relation.
- **Commercial** : en règle générale, le spam a un objectif commercial : la promotion ou la vente d'un produit ou d'un service. Quelques messages non commerciaux peuvent toutefois être assimilés à du spam, par exemple les messages non sollicités expédiés en nombre qui portent sur un sujet politique ou contiennent un virus.
- **Utilise des adresses recueillies ou vendues sans le consentement du propriétaire** : les polluposteurs utilisent souvent des adresses électroniques qui ont été recueillies sans le consentement explicite des intéressés. Bon nombre d'entre eux font ainsi appel à des listes récoltées par voie électronique auprès de sources publiques, comme les pages web ou les groupes de nouvelles.
- **Indésirés** : le spam est généralement jugé indésiré, voire inutile, par ses destinataires.
- **Non ciblé ou systématique :** le spam est normalement envoyé sans discernement, sans autre renseignement sur le destinataire que son adresse électronique.
- **Répétitif** : beaucoup de messages spam sont répétitifs, et sont soit la reproduction exacte de messages antérieurs, soit le même message très légèrement modifié.
- **Contenu illégal ou offensant :** le spam véhicule souvent un message frauduleux ou trompeur. Certains ont un contenu offensant ou à caractère pornographique, ce qui est illégal dans certains pays.
- **Incontrôlable :** les destinataires du spam ne peuvent bloquer la réception des messages ; en effet, les liens « annuler l'abonnement » ne fonctionnent généralement pas.
- **Anonymes ou déguisés** : les messages spam sont souvent envoyés sous une forme qui masque l'identité de l'expéditeur au moyen d'adresses ou d'informations d'en-tête fausses. Les polluposteurs utilisent souvent des serveurs électroniques tiers non autorisés.

Pour les besoins du présent document, les éléments ci-dessus peuvent être classés en caractéristiques primaires ou secondaires. Les caractéristiques *primaires* concernent les messages commerciaux électroniques non sollicités envoyés en nombre. Nombreux sont ceux qui estimeraient qu'un message réunissant ces particularités est un message spam (voir tableau 1). Les autres caractéristiques mentionnées peuvent être décrites comme *secondaires* ; elles sont fréquemment associées au spam, mais peut-être pas aussi nécessaires. La réglementation de certains pays de l'OCDE s'applique aux messages comprenant plusieurs des caractéristiques dites « primaires » et « secondaires » dans le tableau qui suit.

Tableau 1. **Caractéristiques primaires et secondaires du spam**

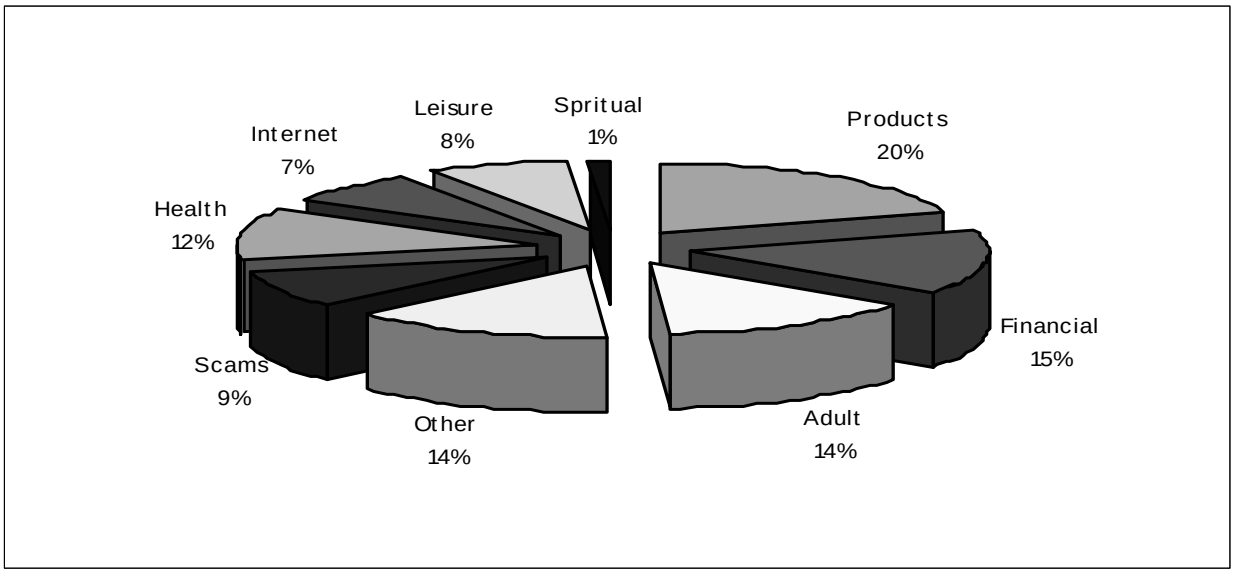
Caractéristiques primaires	Caractéristiques secondaires
Message électronique	Utilise des adresses collectées sans consentement ou connaissance préalable
Expédié en nombre	Indésiré
Non sollicité	Répétitif
Commercial	Non ciblé et systématique
	Incontrôlable
	Anonyme et/ou déguisé
	Contenu illégal ou offensant
	Contenu trompeur ou frauduleux

Source : Secrétariat de l'OCDE.

Catégories de contenu spam

Le contenu des messages spam varie considérablement : publicités de biens et de services, messages à caractère pornographique, informations sur les copies illicites de logiciels, publicités mensongères et/ou sollicitations financières frauduleuses. Pour illustrer cette diversité, la figure 2 présente la répartition chiffrée des données catégorielles sur une période donnée.

Figure 2. **Données catégorielles sur le spam**



Source : Brightmail's Prove Network (2003), « The State of Spam - Impact & Solutions », Brightmail Incorporated, juillet, www.brightmail.com/press/state_of_spam.pdf., consulté le 9 janvier 2004.

Escroqueries Santé Internet Loisirs Spirituel Produits Financier « Adultes » Divers

Aspects économiques du spam

Le spam est devenu l'un des aspects les plus controversés du commerce électronique. Qu'est-ce qui incite les polluposteurs à envoyer des messages électroniques ?

Instrument de commercialisation direct

La mise au point de bases de données évoluées a fait du télémarketing et du cybermarketing des stratégies de prospection directe de plus en plus répandues. Le marketing direct revêt plusieurs formes : courrier postal, téléphone, télécopie, automates d'appel et courrier électronique. Les entreprises y voient un moyen utile d'approcher et de fidéliser les clients, et d'assurer des services de relation avec la clientèle. Les messages électroniques, les courriels notamment, offrent un moyen peu coûteux et facile de contacter un vaste groupe de clients. Le courrier électronique est aussi devenu l'un des outils les plus économiques de soutien et d'assistance à la clientèle. Du fait que l'Internet a, dans de nombreux cas, diminué les coûts du changement pour les usagers, la gestion des relations avec la clientèle et le marketing de permission revêtent une importance nouvelle. Ces avantages ont toutefois été compromis par le flot ininterrompu de spam, qui a porté atteinte à la confiance des consommateurs dans le cybermarketing et dans son efficacité.

Coûts faibles ou transférés

Le courrier électronique est peut-être l'outil de marketing direct le moins onéreux ; les coûts ne varient pas selon la distance et les envois répétés ont un coût supplémentaire très modique. Compte tenu du coût marginal très faible de l'envoi en nombre de messages électroniques à des adresses individuelles, les coûts d'une approche directe particulière sont parfois récupérables même si un seul destinataire devient client. Le courrier électronique peut donc constituer un moyen idéal, économique, de bâtir une relation avec la clientèle. C'est aussi pourquoi le spam progresse à un rythme aussi alarmant. Du fait que les frais d'expédition sont très bas, les polluposteurs peuvent dégager des bénéfices malgré les taux de réponse extrêmement faibles. Plus un polluposteur peut envoyer de messages électroniques, plus ses bénéfices sont élevés, tandis que les coûts restent a peu près stables.

Une enquête réalisée en 2002 sur l'utilisation commerciale du courrier électronique estime que le coût d'expédition d'un courriel unique s'établit en moyenne à USD 0,05, le plus bas étant de USD 0,01.[12] D'autres études ont indiqué qu'il en coûte 0,00032 cents pour obtenir une adresse électronique.[13] Étant donné la diversité des méthodes permettant de collecter ces adresses, il est cependant difficile de fournir des données précises sur les coûts à ce stade. Une chose est toutefois certaine : ils sont très bas.

Le spam diffère sensiblement des autres formes de publicité directe non sollicitée en ce qu'il transfert le coût de la publicité aux entités qui reçoivent et distribuent le courrier électronique, à savoir les FAI, les entreprises et les consommateurs. Avec les autres formes de publicité non sollicitée, l'annonceur paie l'envoi de ses publicités et le consommateur est simplement gêné ou ennuyé de les recevoir. La production et la distribution d'un courrier normal comportent un travail de mise en page, des frais de papier, la mise sous pli et l'affranchissement, tandis que le marketing téléphonique fait intervenir de nombreux effectifs. L'expéditeur de messages électroniques en nombre, en revanche, ne paie souvent qu'une très petite portion des coûts de distribution réels et il semble que la modicité de ces coûts entraîne une utilisation sans discernement de ce moyen. Le seul volume de messages impose des coûts considérables liés au blocage ou à la suppression de grandes quantités de messages indésirés à les FAI, les systèmes d'entreprise et les consommateurs destinataires.

Compte tenu de la modicité des coûts, le spam dégagera des bénéfices même si les taux de réponse sont bas. Selon une enquête réalisée par Mailshell en mars 2003, plus de 8 % des 1 118 personnes interrogées ont admis avoir acheté un produit promu par le spam.[14] Une étude conduite par le Wall Street Journal en 2002[15] a montré qu'avec le courrier électronique, un taux de réponse de 0,001 % à peine peut être rentable. Elle cite le cas d'un publipostage de 3,5 millions de messages qui a produit 81 ventes la première semaine, soit un taux de réponse de 0,0023 %. Chaque vente a rapporté USD 19 à la société de commercialisation, soit USD 1 500 la première semaine. Le coût d'envoi des messages était minime,

probablement moins de USD 100 pour un million de messages. L'étude a estimé que lorsque la société aurait contacté les 100 millions d'adresses de son fichier, elle aurait probablement dégagé plus de USD 25 000 de cette opération.

Qu'est-ce qui explique la prolifération du spam ?

Outre les facteurs économiques évoqués ci-dessus, d'autres éléments peuvent expliquer le volume croissant de spam, par exemple le perfectionnement des stratégies existantes pour obtenir des adresses électroniques. Un autre est la difficulté d'identifier les polluposteurs pour leur faire assumer la responsabilité de leurs pratiques.

Technologies de collecte et de diffusion d'adresses électroniques

Un polluposteur peut se procurer des adresses électroniques auprès des sources suivantes :

1) Clients ou clients prospectifs qui fournissent eux-mêmes leur adresse électronique au polluposteur.

2) Tiers qui ont obtenu les adresses directement auprès des particuliers et les vendent au polluposteur.

3) Espaces publics - pages web, annuaires ou groupes de nouvelles - où les polluposteurs captent les adresses grâce à des progiciels de récolte automatique (« spamware »).

4) Tiers qui font appel aux outils spamware pour recueillir les adresses particulières sur les espaces publics et les vendre au polluposteur.

5) Dans certains cas, il existe aussi des formules (méthodes empiriques automatisées associées au nom ou au prénom) appliquées à un domaine spécifié.

La troisième et la quatrième de ces techniques sont les plus couramment utilisées.[16] Seule la première méthode permettrait au destinataire de se rendre compte que son adresse électronique est utilisée aux fins de spam. Pour collecter les adresses électroniques, les outils spamware naviguent automatiquement sur les sites web et les espaces public, comme Usenet ou les forums de discussion, au moyen d'une liste d'URL qui peut être spécifiée par avance, créée avec des mots-clés introduits dans les moteurs de recherche ou chargée récursivement sur les pages web à la manière d'un moteur de recherche. Ils rassemblent ensuite toutes les adresses électroniques trouvées dans ces espaces. Ils distribuent aussi les messages électroniques à des listes conçues de manière à contourner les filtres mis en place par les FAI.

Certains programmes de spamware ont recours à d'autres techniques pour recueillir les adresses électroniques. L'une d'elles est le générateur aléatoire d'adresses électroniques. Un expéditeur de messages électroniques en nombre inonde un nom de domaine particulier au moyen d'un programme qui génère des millions d'adresses électroniques possibles : aa@cdt.org, ab@cdt.org, etc. Cette « attaque en force » essaie d'envoyer des messages à toutes les combinaisons de lettres susceptibles de composer une adresse électronique. « L'attaque dictionnaire », plus élégante, établit des listes d'adresses par des permutations alphabétiques générées par ordinateur et combinées à des suffixes d'adresse, ou crée des adresses au moyen de patronymes courants et d'initiales de prénoms (autrement dit, les noms forment une séquence, par exemple : bob@msn.com, abob@msn.com, bbob@msn.com, cbob@msn.com, etc.).

Les principaux FAI et réseaux d'entreprise, qui gèrent chaque jour un volume important de courrier électronique sur leurs serveurs, sont très vulnérables aux attaques dictionnaire parce que les polluposteurs les conduisent sans être détectés, dissimulés dans le trafic normal. Ces derniers utilisent parfois des logiciels qui ouvrent des connexions aux autres serveurs et soumettent automatiquement des millions

d'adresses aléatoires, par exemple « anne@hotmail.com », « michael@hotmail.com », et enregistrent les adresses valables, qui sont ensuite automatiquement ajoutées à leur liste.[17] Les polluposteurs ciblent essentiellement les FAI, mais aussi les entreprises, de manière à atteindre les boîtes aux lettres de millions d'employés. Bien que ces attaques n'aient pas pour objet de porter atteinte au fonctionnement des machines visées, leur effet sur les FAI ou sur les entreprises est analogue à celui d'une attaque par saturation, où un trafic illégitime massif empêche l'usage légitime des services du FAI.

Certains polluposteurs établissent des listes d'adresses électroniques valables non pas aux fins de spam, mais pour les revendre en gros à d'autres polluposteurs, partout dans le monde.[18] De fait, bon nombre de polluposteurs n'ont pas pour but de vendre des biens et des services ; ils gagnent de l'argent en vendant des adresses électroniques à d'autres polluposteurs.

De la difficulté d'identifier les polluposteurs

Il est difficile de repérer les polluposteurs. Ceux-ci font appel à plusieurs méthodes pour masquer leur identité. Les adresses sources sont randomisées de manière à ne pas être facilement identifiées. Les programmes de spamware génèrent automatiquement de faux en-têtes et de fausses adresses de retour. Les faux en-têtes permettent aux polluposteurs de ne pas tenir compte de la demande de retrait des listes présentée par les destinataires, et d'occulter leur identité en empêchant tout traçage. D'autres balaient l'Internet pour trouver des serveurs relais ouverts à l'étranger de manière à ce que leurs messages ne puissent être tracés. Selon Spamhaus, les sources directes « sont à l'origine de quelque 50 % des messages spam reçus par les relais de messagerie Internet dans le monde, les 50 % restants étant transmis par des outils tiers comme les serveurs mandataires et les serveurs relais ouverts »[19].

Certains polluposteurs ouvrent des comptes de messagerie électronique gratuits et les abandonnent avant d'être repérés. Ils écrivent aussi des programmes qui utilisent plusieurs comptes de sorte que lorsqu'un compte est résilié, un autre entre automatiquement en fonctionnement. Bon nombre d'entre eux changent simplement de FAI quand leurs comptes sont résiliés pour avoir pratiqué le spam. D'autres se font cependant passer pour de petits fournisseurs d'accès Internet auprès de leur FAI et prétendent que le spam provient de clients non existants.[20] Les polluposteurs peuvent envoyer des centaines de milliers de messages, dont chacun a un contenu personnalisé et des adresses sources, et ferment ensuite rapidement la session.[21] Ils ont aussi recours à l'usurpation d'adresses IP, ce qui suppose l'utilisation de faux noms d'expéditeurs : il peut s'agir de fausses informations ou bien, dans certains cas, de noms d'autres entités commerciales non impliquées dans l'opération de spam.

D'après Spamhaus, qui exploite un « Registre d'opérations spam connues » (ROKSO, *Register of Known Spam Operations*), 90 % des spams reçus par les internautes en Amérique du Nord et en Europe sont envoyés par un groupe restreint de quelque 180 personnes seulement, presque toutes fichées dans la base de données ROKSO. Ces polluposteurs chroniques, professionnels, forment des groupes peu structurés (les « spam gangs ») et se déplacent de réseau en réseau à la recherche de FAI réputés pour ne pas appliquer les mesures anti-spam.

Le spam dans le monde sans fil

Face à l'expansion mondiale des communications hertziennes, au développement des réseaux sans fil de troisième génération, et à l'utilisation grandissante de la messagerie mobile pour envoyer des messages commerciaux non sollicités, une protection anti-spam dans l'environnement hertzien se fait de plus en plus nécessaire. Étant donné la popularité croissante des téléphones cellulaires ou des appareils mobiles tels que les assistants numériques personnels, les polluposteurs vont être de plus en plus tentés de prendre pour cible les abonnés aux réseaux sans fil. Si la messagerie électronique textuelle accuse un certain retard dans

quelques pays Membres (commes les États-Unis), elle est depuis plusieurs années l'une des applications vedette du service téléphonique cellulaire dans d'autres (Finlande, Japon, Corée et Royaume-Uni par exemple) ; dans ces pays, le spam pose déjà un problème sur les réseaux hertziens.

Au Royaume-Uni, la messagerie SMS fait des adeptes de plus en plus nombreux. Plus de 6 milliards de messages textuels ont été envoyés en 2000, et plus de 12 milliards en 2001. Un spam SMS typique demande aux destinataires d'appeler de toute urgence un service kiosque. Les appels à destination de ces services coûtent jusqu'à GBP 1,50 la minute au Royaume-Uni. Ces numéros sont parfois associés à des « services » d'information qui ne proposent aucun renseignement utile et/ou n'ont été établis qu'aux fins d'escroquerie. Une autre pratique trompeuse consiste à envoyer un message SMS énoncé comme suit : « URGENT : veuillez appeler tel numéro », le numéro étant celui d'un service kiosque. D'autres types d'escroquerie SMS font intervenir des tiers qui assurent la promotion de leurs produits et services auprès de clients d'autres entreprises. Dans certains cas, le demandeur n'entendra qu'une tonalité d'occupation enregistrée, et l'appel lui sera facturé. Cette technique a pour objet d'encourager le demandeur à recomposer le numéro de manière à le facturer de nouveau. Des stratagèmes similaires sont appliqués en ligne, une connexion au service kiosque étant générée par un appel informatique au travers d'un lien usurpé.

L'arrivée de la messagerie textuelle a rendu les téléphones cellulaires particulièrement vulnérables aux attaques de type dictionnaire menées par les polluposteurs au moyen de numéros de téléphone. Par ailleurs, plus les appareils mobiles intégreront de fonctions (téléphone, caméra, lecteur MP3 etc.), plus il sera indispensable de les protéger contre les virus répandus par spam.

Les opérateurs de services hertziens doivent aussi faire face au désabonnement de leurs clients et aux remboursements onéreux causés par les spam indésirés. Dans le cadre des modèles de tarification de la messagerie sans fil, qui veulent que les abonnés ou destinataires paient le message et le contenu d'un message, ce sont les clients et les prestataires de services mobiles qui assument le coût des spams. Au Japon, par exemple, le prestataire de services cellulaires DoCoMo, du fait qu'il facture les messages entrants, rembourse à ses clients chaque message spam reçu. Le caractère initialement ouvert du système d'adresse de DoCoMo a aggravé les problèmes pour les usagers en 2001. La société a recommandé à ses abonnés de changer d'adresse électronique, et plus de 90 % d'entre eux l'avaient fait à la fin de janvier 2002. Face au flux massif de messages non sollicités sur les appareils mobiles, certains usagers finaux risquent de juger ces systèmes de communication impraticables.

Les opérateurs hertziens, les organisations apparentées et les usagers ont fait appel à des méthodes diverses pour lutter contre le spam. Aux États-Unis, les opérateurs de services sans fil ont créé des systèmes qui bloquent les messages en nombre et empêchent la diffusion de leurs listes de clients pour décourager le spam. En janvier 2001, la Mobile Marketing Association (MMA) a établi pour ses membres des normes de confidentialité fondées sur le principe selon lequel les campagnes de publicité ne doivent être adressées qu'aux clients qui l'ont demandé. La MMA a également déclaré que le spam diffusé via les réseaux hertziens ne servirait ni les besoins des consommateurs, ni ceux du secteur mobile, et que les systèmes de « consentement préalable explicite confirmé » devaient devenir la norme de fait des campagnes publicitaires sur ces réseaux.[22]

Au Japon, DoCoMo a essayé d'empêcher les annonceurs de créer des listes de cibles précises en bloquant les moyens qui leur permettent d'envoyer des publicités à de nombreuses adresses électroniques de DoCoMo. La société a commencé par utiliser par défaut des adresses électroniques alphanumériques plutôt que des numéros de téléphone, et à fournir gratuitement 400 paquets par mois à titre de compensation, les abonnés étant facturés pour la réception comme pour l'expédition de messages électroniques. Les usagers ont en outre bloqué les messages provenant d'adresses non spécifiées et modifié leurs propres adresses.

Au Royaume-Uni, trois sociétés de téléphonie cellulaire, BT Cellnet, Vodafone et Orange, ont adopté en mars 2001 un code de déontologie qui limite l'envoi de messages textuels non sollicités vers les téléphones mobiles. Ce code, établi par la *Wireless Marketing Association* (WMA), établit que le marketing mobile ne doit être adressé aux abonnés de ces services que si ceux-ci ont préalablement accordé leur permission. Par ailleurs, le gouvernement britannique a mis sur pied un dispositif, le Telephone Preference Service (TPS), qui permet aux clients d'enregistrer leur numéro cellulaire. Il est illégal d'effectuer un appel de marketing direct ou d'envoyer un SMS commercial à tout numéro enregistré sur le TPS (maintenant en partie supplanté par de nouveaux systèmes de consentement préalable explicite - « opt-in » - destinés aux particuliers). Les abonnés peuvent aussi signaler les messages SMS à tarification majorée présumés fallacieux à l'*Independent Committee for the Supervision of Standards of Telephone Information Services* (ICSTIS). Ils peuvent également déposer une plainte à ce sujet auprès du Commissaire à l'information.

Le 19 octobre 2003, le Ministère coréen de l'information et de la communication (MIC) a annoncé qu'il allait instaurer un système de « opt-in » pour les services de téléphonie mobile. Celui-ci sera appliqué dans le cadre d'accords d'utilisation conclus entre les fournisseurs de services mobiles et les prestataires de services d'information. Le MIC interdit également l'envoi de messages publicitaires à certaines heures, entre 21 heures et 8 heures par exemple, même pour les clients ayant donné leur consentement préalable.

QUELS SONT LES PROBLÈMES ASSOCIÉS AU SPAM ?

Le spam suscite un mécontentement grandissant parmi les internautes. Une enquête conduite en 2002 par Harris Interactive auprès d'usagers adultes aux États-Unis indique que 80 % d'entre eux sont « très ennuyés » par le spam, alors qu'ils n'étaient que 49 % à répondre de la sorte deux ans et demi plus tôt. Quelque 74 % seraient partisans de le rendre illégal, 12 % seulement étant opposés à son interdiction.[23] On trouvera ci-après un exposé des raisons qui ont fait du spam un tel problème.

Coûts du spam

Le spam impose des coûts à tous les usagers de l'Internet. Ces coûts augmentent parallèlement au nombre de messages spam qui envahissent le réseau chaque jour. Il ne fait aucun doute que le spam constitue une gêne, et le degré de gêne qu'il provoque a également progressé avec lui. Le point le plus important, toutefois, est que le spam utilise, sans compensation ni approbation, les ressources rares des usagers et des prestataires de services. Il consomme des ressources de réseau et de calcul, le temps de l'administrateur du système de messagerie électronique et du personnel des services d'assistance, et diminue la productivité des travailleurs.

Il est difficile de calculer le coût total du spam à l'échelle mondiale mais, selon les estimations, il serait élevé. Une étude de l'Union européenne (UE) l'évalue par exemple à quelque EUR 10 milliards pour les internautes.[24] Elle estime par ailleurs que si chaque personne reçoit six messages spam par jour, elle perd deux heures chaque année pour les supprimer (en supposant qu'il faut de 3 à 4 secondes pour définir la nature d'un message et l'effacer).[25] Il ressort d'une enquête conduite auprès de 1 000 abonnés par InsightExpress que 65 % d'entre eux passent plus de dix minutes par jour à traiter le spam, et 24% y consacrent plus de vingt minutes[26]

Coûts pour les abonnés particuliers

Les usagers perdent du temps à effacer les messages commerciaux non sollicités répétitifs. D'autres coûts peuvent s'ajouter : le prix des communications supplémentaires des FAI ou des compagnies téléphoniques (ou les deux) ainsi que les coûts additionnels de stockage des données. Par ailleurs, les coûts engagés par les FAI pour résoudre le problème du spam sont généralement répercutés sur les consommateurs.

Coûts pour les entreprises

Les entreprises s'inquiètent également des coûts substantiels liés au spam, qui portent diversement atteinte à l'environnement commercial. Grâce à des techniques de récolte d'adresses électroniques sur l'Internet, les polluposteurs disposent de bases de données d'adresses saisies sur les sites web des entreprises. La fréquence croissante des attaques de spam sur les entreprises soulève en outre des risques sérieux.

Les coûts pour les entreprises peuvent varier selon la méthode utilisée ; l'examen de plusieurs études permet néanmoins de les estimer. Brightmail évalue les coûts annuels du spam pour une entreprise en

supposant que 10 % du nombre total de messages électroniques relèvent du spam, et que chaque employé consacre 30 secondes par jour à les supprimer. Selon ces hypothèses, le coût annuel estimé du spam pour une entreprise de 10 000 personnes s'élève à USD 675 000.[27] Un rapport de juin 2003 du groupe Radicati prévoit que le spam électronique coûtera aux entreprises USD 20,5 milliards en 2003, et près de dix fois plus, soit USD 198 milliards, d'ici à 2007.[28]

Ferris Research, Inc. a également estimé que les messages électroniques commerciaux non sollicités ont coûté USD 8,9 milliards aux entreprises américaines en 2002. Ferris a évalué le coût du spam en calculant son effet de coût dans trois domaines : perte de productivité des travailleurs ; consommation de bande passante et d'autres ressources techniques ; utilisation du temps d'assistance technique. L'estimation ainsi obtenue représentait quelque USD 10 par usager et par mois.[29] Ferris a également prédit que le spam coûtera aux sociétés américaines plus de USD 10 milliards en 2003. En Europe, la société a estimé le coût du spam à USD 2,5 milliards.[30]

Les coûts du spam pour les entreprises peuvent être classés comme suit. Il y a d'abord la perte de productivité des employés qui lui est due, suivie des coûts additionnels en termes de ressources de réseau et de calcul. Troisièmement, le déploiement d'outils techniques pour lutter contre le spam requiert le renforcement des ressources humaines et constitue un fardeau financier supplémentaire. La quatrième catégorie concerne les risques de sécurité dus aux attaques de spam comme les attaques de dictionnaire et les virus et vers transmis par courrier électronique. Vient enfin la responsabilité civile potentielle.

S'agissant de la baisse de productivité des employés, les coûts comprennent le temps consacré par les employés à vérifier leur courrier et à effacer à intervalles réguliers les messages publicitaires non sollicités qu'ils reçoivent chaque jour. Selon un rapport de l'Australian National Office for the Information Economy, le coût du temps passé à ouvrir et à lire les messages spam sur le lieu de travail est estimé en moyenne à AUD 960 (près de USD 620) par employé et par année.[31] Ce chiffre ne comprend ni les coûts de bande passante et de réseau, ni les temps d'arrêt imputables à la surcharge de messages spam.

Les ressources de réseau et de calcul nécessaires pour traiter les messages spam peuvent être considérables. Le spam exige parfois l'emploi de filtres et peut ralentir les réseaux d'entreprise en augmentant la charge de trafic ; il aura en outre des effets fâcheux sur l'espace de stockage informatique et la bande passante de la société. Le spam absorbe le temps de l'administrateur du système de courrier électronique et celui du personnel des services d'assistance, et augmente les frais financiers compte tenu du déploiement de logiciels anti-spam et l'exploitation des systèmes de filtrage.

Les attaques spam de grande ampleur, comme les « attaques d'annuaires », peuvent paralyser ou fermer les réseaux d'une entreprise. Les virus et les vers transmis par courrier électronique constituent aussi une grave menace pour ces réseaux. D'aucuns ont soulevé la question d'une éventuelle responsabilité civile des entreprises quand elles sont incapables d'empêcher que leurs employés soient exposés à des messages obscènes sur le lieu de travail (c'est-à-dire à des messages spam pornographiques).[32]

Le spam a aussi un coût pour les entreprises légitimes de marketing électronique. Du fait que les abonnés, de plus en plus gênés par les messages spam, utilisent plus fréquemment des filtres, les messages de ces sociétés risquent d'être effacés avec les autres. Il s'agit parfois de messages transactionnels ou simplement d'informations sur des produits ou services. Les distributeurs professionnels risquent ainsi de perdre à la fois leurs clients existants et des clients potentiels.

En bloquant les messages légitimes, les mesures anti-spam peuvent imposer des coûts imprévus aux entreprises et aux usagers. Comme les entreprises et les FAI ont de plus en plus recours à des dispositifs de filtrage et à des listes noires, l'incidence des « faux positifs » augmente de manière exponentielle. Les messages commerciaux légitimes filtrés par erreur en tant que spam ne sont pas distribués à leurs

destinataires qui, souvent, ignorent que leur FAI ou leur entreprise a bloqué le message. Cela arrive de plus en plus fréquemment à des messages commerciaux qui ont reçu le consentement préalable de l'abonné.

Coût pour les FAI et pour les prestataires de services de messagerie électronique

Les FAI et les prestataires de services de messagerie électronique supportent également bon nombre des coûts que doivent assumer les entreprises : bande passante de réseau, stockage des données, temps du personnel, disponibilité des lignes téléphoniques, coûts de traitement liés à l'hébergement et à l'acheminement des messages entrants excédentaires, investissements dans les systèmes de filtrage et frais juridiques engagés pour assigner les polluposteurs en justice. Les FAI supportent en outre d'autres coûts puisqu'ils doivent réagir plus rapidement à l'expansion du spam ; en effet, l'augmentation du volume de messages électroniques peut ralentir considérablement le débit de l'Internet, surcharger les serveurs, voire menacer leurs propres opérations. Les FAI et les prestataires de services de messagerie électronique doivent disposer des effectifs adéquats pour s'attaquer au spam au niveau technique et pour répondre aux réclamations des abonnés. Les filtres mis en place par les FAI peuvent bloquer par erreur des messages qui ne sont pas du spam, provoquant des désagréments aux abonnés qui risquent de changer de prestataire. Dans l'ensemble, les FAI et les prestataires de services de messgerie électronique consacrent au problème du spam (filtrage, bande passante et service à la clientèle) nettement plus de temps et d'argent que les autres entreprises.

Ferris Research estime à USD 500 millions les coûts du spam pour les prestataires de services américains et européens. D'autres études indiquent que les coûts pour les FAI représentent 10 % des frais généraux associés à la fourniture d'un accès Internet, qui sont compris dans le prix mensuel facturé aux abonnés.[33]

Problèmes relatifs à la vie privée

La pratique du spam, et notamment la collecte et la vente d'adresses électroniques, soulève diverses préoccupations quant à la protection de la vie privée en vertu des *Lignes directrices de l'OCDE sur la protection de la vie privée et les flux transfrontières de données de caractère personnel* (« Lignes directrices sur la vie privée »). Ces pratiques risquent également de violer les règles internationales et les lois nationales existantes en la matière. Elles risquent notamment de créer des difficultés si les informations personnelles font l'objet d'une utilisation abusive entraînant des conséquences fâcheuses.

Pour les consommateurs, le spam a pour inconvénient majeur de constituer une atteinte substantielle à leur vie privée : ils reçoivent des messages dont ils ne veulent tout simplement pas. Qui plus est, la collecte d'adresses électroniques est fréquemment effectuée sans qu'ils le sachent, sans que soient spécifiés (ou alors, de manière inexacte) l'objet et sans leur consentement. Ces problèmes sont exacerbés quand le spam est envoyé sans discernement. Quelques polluposteurs moissonnent ainsi des adresses électroniques sur les sites web, les groupes de nouvelles et d'autres sources publiques sur l'Internet. D'autres utilisent des « attaques dictionnaire » pour envoyer le spam. D'autres enfin vont jusqu'à pirater les bases de données privées pour obtenir des adresses. La vie privée des internautes peut également être surveillée via l'introduction, à leur insu, de pixels invisibles et/ou de logiciels espions sur leurs ordinateurs.

Problèmes associés au contenu du spam

Fraude et tromperie

Le spam frauduleux ou trompeur peut revêtir des formes diverses. Selon un rapport de la Federal Trade Commission (FTC) américaine, « *False Claims in Spam* », publié le 30 avril 2003, 66% des messages spam sont frauduleux au niveau des lignes « Expéditeur » et/ou « Objet », ou dans le corps même du message.[34] Les polluposteurs masquent l'origine de leurs messages parce que *i)* ils savent qu'ils sont bloqués ou filtrés ; et *ii)* ils cherchent à inciter les particuliers à les ouvrir. Un stratagème courant consiste à falsifier les en-têtes des messages. Les polluposteurs utilisent souvent la fonction relais des serveurs de messagerie administrés par des tiers.[35] Les falsifications auxquelles ils ont notamment recours sont de fausses adresses d'expédition et de réponse, de fausses informations de routage, des lignes « Objet » fallacieuses, et des liens de désabonnement frauduleux. La FTC a récemment engagé un procès contre un polluposteur pour utilisation trompeuse de la ligne « Objet », utilisation déloyale de la ligne « Expéditeur » et utilisation fallacieuse de la demande de retrait de la liste à la fin du message spam.[36]

Le corps du message spam comporte aussi couramment des déclarations trompeuses ou fallacieuses. Un type d'escroquerie répandu, comme « l'escroquerie nigériane », propose un moyen de s'enrichir rapidement[37] : l'expéditeur du message dit vouloir partager un million de dollars avec le destinataire, mais a généralement besoin d'un acompte. Les services secrets américains ont qualifié « d'épidémie » ce type de stratagème, et affirment que les pertes annuelles s'élèvent à des centaines de millions de dollars.[38] Certains messages proposent des investissements pyramide ou soi-disant sans risques. D'autres spams mensongers font de la publicité pour des régimes « miracles » et des produits de santé, offrent des cartes de crédit ou de meilleures conditions de crédit, des voyages à forfait intéressants et/ou des débouchés commerciaux. Il existe aussi plusieurs sortes de messages illicites ou illégaux, notamment ceux qui assurent la promotion de services de prostitution, des jeux d'argent en ligne illégaux, la vente de stupéfiants ou d'armes, etc.[39]

Pornographie

Les messages spam qui contiennent des images pornographiques et diffusent des produits et services destinés à des publics adultes[40] ne sont pas appropriés pour les enfants. Comme de nombreux polluposteurs ne ciblent pas des destinataires particuliers, les jeunes enfants risquent d'être exposés par mégarde à des messages à caractère pornographique ou offensant.

Conséquences en termes de sécurité

Le spam peut bloquer les réseaux informatiques et paralyser temporairement les ordinateurs personnels, voire les endommager de manière permanente, quand il sert à diffuser des virus ou des vers informatiques. D'importants volumes de spam peuvent porter atteinte aux infrastructures informatiques essentielles et compromettre la sécurité publique. Le spam peut aussi être utilisé dans l'intention de nuire sous forme d'attaque par saturation.

Certains spams contiennent également des virus et des vers destructeurs. Les auteurs de virus écrivent généralement des programmes qui téléchargent les carnets d'adresses des usagers et propagent le virus en l'envoyant à tous les correspondants à partir d'une adresse authentique. Ils évitent ainsi les filtres anti-spam. D'aucuns estiment que 90 % des virus sont transmis par courrier électronique. Cinquante et un pour cent des entreprises ont connu des attaques de virus, et des vers informatiques comme Klez et Code Red sont également devenus courants et problématiques.[41] La pratique consistant à diffuser des virus par spam a induit une plus grande méfiance envers la sécurité du courrier électronique en tant que mode de communication.

Outre les virus ou les vers, des fichiers de type pixels invisibles et logiciels espions peuvent être téléchargés avec le contenu de messages électroniques. Les polluposteurs exploitent également les failles inhérentes aux systèmes de transfert de messages comme les serveurs relais et mandataires ouverts. Selon MessageLabs, plus de 60% du spam ils arrêtent chaque mois est envoyé par les mandataires ouverts.[42] Les relais ouverts servent souvent d'intermédiaires pour le spam ; les polluposteurs tentent parfois des intrusions non autorisées pour ouvrir un relais fermé. Certains FAI ont refusé d'accepter du trafic de communications provenant de serveurs mal configurés, voire de pays où de nombreuses installations peuvent être utilisées pour relayer des communications inopportunes.

Les liens entre les polluposteurs et les auteurs de codes malintentionnés semblent se développer. Les premiers emploient des techniques d'écriture de virus pour que leurs messages franchissent les filtres. Les seconds ont aussi fait appel aux techniques d'envoi en masse des polluposteurs pour attaquer des systèmes informatiques. Un exemple récent est le virus connu sous le nom de « Webber », découvert en juillet 2003. La ligne « Objet » contenait l'énoncé suivant : « Réf : votre demande de crédit ». Les usagers qui ouvraient la pièce jointe téléchargeaient un programme malveillant qui faisait du PC un serveur relais ouvert, lequel permet à un tiers d'envoyer ou de recevoir des messages électroniques à distance.

Un autre exemple, plus grave, est celui du virus « Sobig.E », qui saisit les adresses électroniques dans plusieurs fichiers d'un PC, y compris dans le carnet d'adresses de Windows. Il essaie ensuite d'envoyer une copie de lui-même à chaque correspondant, et utilise l'une des adresses volées pour falsifier la source du message. Selon MessageLabs, Sobig.E est un virus de polluposteur conçu pour récolter des adresses authentiques sur les ordinateurs des usagers. Avec de tels virus, les polluposteurs peuvent utiliser à mauvais escient les carnets d'adresses des usagers pour envoyer de grandes quantités de messages spam.

D'autres problèmes de sécurité surgissent quand le spam est utilisé pour attirer à leur insu des usagers sur des pages web où un logiciel espion est téléchargé clandestinement. Le logiciel surveille l'activité d'un internaute et transmet les informations à d'autres. Il peut aussi rassembler des informations sur les adresses électroniques, les mots de passe, et les numéros de carte de crédit.

Vol d'identité

Le vol d'identité est une pratique en expansion qui, parce qu'elle émousse la confiance des consommateurs, constitue une menace pour le commerce électronique. Chaque message électronique contient des renseignements concernant son origine, mais les techniques actuelles ne garantissent pas l'exactitude des informations de l'en-tête. Si les polluposteurs découvrent que tous les messages électroniques émanant d'une entreprise donnée franchissent les filtres anti-spam parce que la société est sur une « liste blanche », ils peuvent falsifier leurs propres messages de manière à ce qu'ils paraissent provenir de cette source. Les polluposteurs se servent généralement d'une autre adresse IP commerciale ou dissimulent leur propre identité derrière des identités commerciales volées ou trompeuses.[43] D'autres modifient l'en-tête de manière à falsifier le nom de l'expéditeur ou créent un relais ouvert par l'intermédiaire de serveurs non sécurisés.

Le vol d'une identité peut porter préjudice à l'image de marque d'une entreprise partout dans le monde. Les sociétés qui en sont victimes doivent consacrer un temps et des moyens considérables à rétablir leur notoriété. De plus, les listes noires des FAI contiennent souvent les noms de domaine de ces victimes ; les abonnés à ces listes ne peuvent donc plus recevoir de messages électroniques des sociétés légitimes. Aujourd'hui, les noms de domaines jouent un rôle de poids dans l'image de marque d'une société. Leur vol à des fins de spam a donc pénalisé plusieurs entreprises, et cette pratique devrait prendre de l'expansion.

Comme les entreprises, les particuliers peuvent être victimes d'un vol d'identité. Bon nombre de polluposteurs envoient leurs messages au travers d'un compte tiers, sans autorisation, parce que le spam constitue un délit ou qu'il est interdit par leur FAI. Les FAI qui opèrent en vertu d'un code de bonne conduite ou de déontologie professionnel sont habilités à résilier les comptes utilisés pour envoyer du spam.

Baisse de confiance du consommateur

Outre les coûts supportés par les FAI et les usagers finaux, un problème majeur du spam est de susciter la méfiance des internautes envers l'économie numérique, ce qui pourrait compromettre le développement du commerce électronique. Le spam peut dissuader les internautes de participer au réseau, autrement dit aux forums en ligne et aux groupes Usenet, ou les inciter à retirer leurs adresses électroniques des pages d'entreprises et des pages d'accueil par crainte qu'elles ne soient collectées et ajoutées à des listes de diffusion. Cela risque de porter préjudice à l'utilité du courrier électronique, l'un des outils les plus populaires de l'Internet.

Depuis plusieurs années, l'OCDE s'emploie à bâtir la confiance du consommateur en ligne. En 1999, ses pays Membres ont adopté les *Lignes directrices régissant la protection des consommateurs dans le contexte du commerce électronique*. Reconnaissant qu'il importe d'appliquer des pratiques loyales en matière de commerce et de marketing pour renforcer la confiance du consommateur, ce document contient des dispositions relatives au spam, et stipule notamment que :

1) Les entreprises devraient mettre au point et appliquer des procédures efficaces et faciles à utiliser qui donnent aux consommateurs la possibilité d'accepter ou de refuser de recevoir des messages électroniques commerciaux non sollicités.

2) Lorsque les consommateurs ont indiqué qu'ils ne souhaitent pas recevoir de tels messages électroniques commerciaux non sollicités, ce choix devrait être respecté.[44]

MESURES DESTINÉES A RÉDUIRE LE SPAM

Diverses mesures de lutte contre le spam ont été mises en place par les pouvoirs publics, les FAI et les prestataires de services de messagerie électronique, les professionnels du marketing électronique, les entreprises, les organisations anti-spam, les associations de protection du consommateur, les fournisseurs de solutions anti-spam, etc. Le présent chapitre les classe selon qu'il s'agit de dispositions juridiques et réglementaires, d'approches autoréglementaires, de campagnes d'éducation et de sensibilisation, ou de mesures techniques.

Dispositions juridiques et réglementaires des pays Membres

Il existe fondamentalement deux sortes d'approches juridiques et réglementaires au problème du spam aujourd'hui. La première suppose l'application des lois et règlements existants qui, quoique non spécifiques au pollupostage, peuvent le concerner à divers égards. Ainsi, les lois visant à protéger les consommateurs des opérations commerciales trompeuses ou à empêcher la diffusion d'images pornographiques peuvent s'appliquer aux messages spam.[45] La seconde fait intervenir l'amendement des lois et règlements existants ou la création de nouveaux règlements portant particulièrement sur le spam.[46]

Types de dispositions réglementaires

Le résumé qui suit présente une vue d'ensemble des principaux éléments observables dans les pays Membres de l'OCDE qui ont retenu la seconde approche et adopté des règlements particuliers.

Système de consentement préalable explicite (opt-in)

- Le régime « opt-in » interdit l'envoi de messages électroniques non sollicités à moins qu'une relation n'existe déjà avec le destinataire ou que celui-ci n'ait donné son consentement.

Système de liste de refus (opt-out)

Le régime « opt-out » peut imposer toute mesure parmi les suivantes :

- L'intégration d'un texte explicite sur le « opt-out » ou de demandes de retrait de la liste de diffusion (exclusion spécifique).
- La création d'une « *Do Not Spam List* » (liste de non-diffusion, ou liste d'exclusion universelle). Ce type de liste permet aux expéditeurs de messages électroniques (aux opérateurs de marketing direct en particulier) de retirer de la liste de leurs clients ou prospects les personnes qui ont demandé à ne pas recevoir de messages électroniques non sollicités (« opt-out » général).
- Une identification claire et authentique de l'expéditeur - nom, numéro vert, adresse électronique de retour valide opérée par l'expéditeur, boîte postale ou adresse postale pour permettre de demander facilement à être rayé d'une liste de diffusion.[47]

- Le respect de la demande des destinataires de cesser de leur adresser des messages spam par l'interruption immédiate de cette diffusion.

Droit et responsabilité des FAI

- Les FAI peuvent se voir attribuer le droit de refuser leurs services aux polluposteurs. Les prestataires de services informatiques interactifs peuvent être autorisés à bloquer les messages électroniques commerciaux d'une manière donnée.[48]

Identité véritable et impartialité ; transparence accrue

Les règlements peuvent interdire :

- les fausses identités ou adresses d'expédition ;
- les faux en-têtes ou les informations mensongères à la ligne « Objet », ou la non prise en compte d'une demande d'exclusion par le biais d'une manipulation technique ;
- l'accès non autorisé ou la falsification des informations de routage, ou des déclarations inexactes quant à l'identification du point d'origine ou du trajet de transmission ;
- l'utilisation du nom de domaine Internet d'un tiers sans permission.

Labélisation

- La labélisation consiste à afficher des labels d'identification standard à la ligne « Objet » ou dans l'en-tête, par exemple « ADV » pour les publicités, « ADLT » pour les messages réservés aux adultes (si ceux-ci contiennent des informations destinées aux personnes de plus de 18 ans).

Spamware

- Il est possible d'interdire la récolte d'adresses électroniques sur les sites web[49] et de prohiber ou contrôler les progiciels utilisés pour collecter les adresses, diffuser les messages électroniques en nombre et falsifier les adresses de retour (spamware).

Délimitation du spam

- Le champ d'application des lois et règlements sur le spam peut être limité au courrier électronique, ou élargi aux autres messages électroniques (SMS et autres formes de messagerie électronique).

Divulgation ou vente de données personnelles

- La vente, la location ou l'échange de certaines informations circonstancielles personnelles obtenues en ligne à l'insu du consommateur ou sans son consentement explicite peuvent être interdits.

Synthèse des mesures adoptées par les pays de l'OCDE

L'annexe I décrit la legislation anti-spam des pays Membres de l'OCDE et l'annexe II présente ces lois sous forme de matrice. Dix-huit pays Membres disposent de lois ou de décrets portant spécifiquement sur le spam. Le Canada, la République tchèque et le Mexique lui appliquent les lois et règlements en vigueur. Quelques pays, comme la Nouvelle-Zélande et la Turquie, n'ont pas encore adopté de lois ou règlements particuliers à cet égard. Les sections qui suivent donnent un aperçu des méthodes retenues par les pays Membres de l'OCDE.

« Opt-in » ou « opt-out »

Les paragraphes ci-dessous présentent d'abord la démarche des pays membres de l'Union européenne sous une forme collective car ils ont adopté des dispositions législatives similaires en matière de protection de la vie privée.

États membres de l'Union européenne

L'UE a adopté un système de consentement préalable explicite pour les communications commerciales par courrier électronique (SMS compris), au travers de la Directive 2002/58/CE 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 communications électroniques), qui forme partie intégrante du nouveau cadre réglementaire sur les communications électroniques, plus ample, de la CE. Auparavant, le régime de « opt-in » était applicable aux télécopies et aux systèmes automatisés d'appel.

La directive énonce trois principes fondamentaux en ce qui concerne les messages commerciaux non sollicités. Premièrement, aux termes de son article 13(1), les États membres sont priés d'interdire l'envoi de messages commerciaux non sollicités au moyen de télécopieurs, de courrier électronique ou d'autres systèmes de messagerie électronique tels que le SMS et le MMS (service de messagerie multimédia) à moins que les personnes visées n'aient donné leur consentement préalable (« opt-in »). Ce régime est applicable à la prospection commerciale auprès des particuliers (personnes physiques), mais les États membres peuvent élargir son application aux communications commerciales destinées aux entreprises. L'article 13(2) comporte une exception restreinte à ce système, qui concerne les clients existants et porte sur l'utilisation des coordonnées obtenues auprès d'eux dans le cadre d'une vente ; ces informations ne peuvent toutefois être utilisées que par la même personne morale pour la commercialisation de produits ou services « analogues » et sous réserve qu'il soit explicitement proposé aux clients de s'y opposer au moment de la collecte et à chaque message ultérieur. Deuxièmement, il est interdit à l'expéditeur de masquer son identité. Troisièmement, les messages de prospection directe doivent comporter une adresse de retour valable permettant au destinataire de demander que ces communications cessent (« sans frais et de manière simple »).

L'expression « messagerie électronique » est vaste et neutre sur le plan technique. Elle englobe toutes les formes de communications électroniques qui n'exigent pas la participation simultanée de l'expéditeur et du destinataire. Sa définition ne recouvre pas seulement le traditionnel « courrier électronique », mais aussi le SMS, le MMS, etc.

L'application de cette directive établit un modèle législatif similaire dans tous les États membres de l'UE. Le tableau 2 indique lesquels d'entre eux ont déjà adopté le système de consentement préalable explicite.[50] On relèvera que la Finlande, la France et le Royaume-Uni n'exigent pas ce consentement quand le destinataire est une personne morale enregistrée.

Cette directive doit être interprétée en association avec la Directive « générale » relative à la protection des données 95/46/CE qui définit les notions de consentement, etc. Outre ce qui précède, d'autres dispositions juridiques de la CE peuvent s'appliquer aux messages non sollicités, en rapport, par exemple, avec la publicité mensongère, la récolte d'adresses et le piratage.[51]

Tableau 2. **Mesures législatives adoptées en matière de spam dans les États membres de l'UE (« opt-in » / « opt-out »)**

Pays	Messages électroniques non sollicités
Allemagne	Opt-in
Autriche	Opt-in
Belgique	Opt-in
Danemark	Opt-in
Espagne	Opt-in
Finlande	Opt-in
France	Projet de loi Opt-in
Grèce	Opt-in
Irlande	Opt-in
Italie	Opt-in
Luxembourg	Projet de loi Opt-in (document parlementaire 5181)
Pays-Bas	Projet de loi Opt-in
Portugal	Opt-out
Royaume-Uni	Opt-in
Suède	Opt-in

Source : Secrétariat de l'OCDE et Commission européenne (2003), « Neuvième rapport sur la mise en œuvre de la réglementation de l'Union européenne en matière de communications électroniques », 19 novembre, Annexe 2, p. 29, http://europa.eu.int/information_society/topics/ecomm/doc/all_about/implementation_enforcement/annualreports/9threport/annex2181103.pdf, consulté le 9 décembre 2003.

Autres pays européens Membres de l'OCDE

Parmi les huit pays européens Membres de l'OCDE qui ne font pas actuellement partie de l'Union européenne, quatre vont accéder au statut de membre de l'UE en 2004 et devront transposer ses directives : la République tchèque, la Hongrie, la Pologne et la République slovaque. La République tchèque et la Pologne ont déjà opté pour le régime « opt-in », et la Hongrie suit actuellement cette voie. La République tchèque a adopté ce système pour les communications commerciales en général, mais ses lois ne traitent pas spécifiquement du spam. Aucune information n'est actuellement disponible en ce qui concerne la République slovaque.

En ce qui concerne les quatre autres pays, la Norvège a adopté le régime « opt-in ». En Suisse, suite à une consultation publique en octobre 2002, le gouvernement est en train d'amender la réglementation de manière à appliquer le système de consentement préalable à toutes les formes de pollupostage (téléphone, courrier électronique, télécopie, SMS, etc.) et à obliger les prestataires de services de télécommunications à combattre le spam. Il n'existe pas de loi sur le spam en Turquie, et on ne dispose pas de renseignements sur la situation en Islande à ce stade.

Pays de l'OCDE dans la région Asie-Pacifique

L'Australie a été le premier des sept pays Membres de la région Asie-Pacifique à intégrer explicitement le régime de « opt-in » à sa législation. Le « *Final Report of NOIE Review of the Spam Problem and How It Can Be Countered* » d'avril 2003, qui recommandait ce régime, a été suivi le 2 décembre 2003 par le vote du Parlement australien en faveur de la Spam Bill 2003. L'Australie dispense les organismes publics, les partis politiques, les organisations religieuses, les institutions caritatives et les établissements d'enseignement de respecter cette obligation. A ce jour, il n'existe pas de règlement régissant spécifiquement le spam au Canada, bien qu'un régime de « opt-in » ait été adopté dans le cadre de l'application des lois existantes. Aux termes de la loi canadienne sur la protection des renseignements personnels et les documents électroniques, entrée en vigueur en janvier 2001, les adresses électroniques sont assimilées à des informations personnelles. De ce fait, la collecte et l'exploitation non autorisées d'informations à caractère personnel, comme les adresses électroniques, pourraient enfreindre les dispositions de la loi.[52] Au Mexique, des amendements récents à la loi fédérale sur la protection des consommateurs témoignent de l'adoption d'un régime de « opt-out ». Les consommateurs mexicains ont le droit d'empêcher certaines sociétés de les déranger chez eux ou sur leur lieu de travail, ou par courrier électronique, et de transmettre sans autorisation des données personnelles à des tiers.

A ce jour, la Corée et le Japon ont retenu un régime de « opt-out ». Le 19 octobre 2003, le Ministère coréen de l'information et de la communication (MIC) a cependant annoncé l'instauration d'un système de « opt-in » pour les services de téléphonie mobile. La Nouvelle-Zélande n'a pas encore légiféré à ce propos.

Les États-Unis ont récemment voté une loi sur le spam, qui adopte un régime de « opt-out ». Elle exige des expéditeurs de messages électroniques commerciaux non sollicités qu'ils fournissent un mécanisme de refus et qu'ils respectent la demande des destinataires de ne plus recevoir de messages. La loi leur impose d'annoncer clairement et visiblement le caractère publicitaire du message. Les expéditeurs doivent mentionner une adresse postale valable dans le message et avoir une adresse électronique valable.

Autres dispositions relatives au spam

Tous les pays de l'OCDE n'ont pas adopté une démarche analogue à l'égard de la labélisation et de l'utilisation du spamware dans leurs lois et règlements. Dans le cas de la labélisation, la Finlande, le Japon, la Corée, la Norvège, la Pologne, le Royaume-Uni et les États-Unis exigent que les expéditeurs labélisent certains types de messages, mais d'autres (Australie, Danemark, France, Allemagne et Italie) ne le demandent pas. S'agissant des outils spamware, l'Australie, la France, l'Italie, le Japon, la Corée et l'Espagne ont établi un règlement qui interdit leur utilisation aux fins de spam ; ce n'est par contre pas le cas du Danemark, de la Finlande, de l'Allemagne et du Royaume-Uni. Les États-Unis interdisent la récolte d'adresses électroniques, les attaques de type dictionnaire et l'usurpation d'adresses IP.

En revanche, en ce qui concerne l'identité réelle des expéditeurs, l'offre d'une option de « opt-out » dans les messages et les fausses informations dans les en-têtes et les messages, bon nombre de pays Membres ont retenu des approches similaires. Tout d'abord, presque tous les pays examinés disposant de règlements en matière de spam, à savoir l'Australie, la Belgique, l'Italie, le Mexique, les Pays-Bas et la Pologne, ont signalé exiger que l'identité et l'adresse réelles des expéditeurs figurent dans leurs messages. La Finlande fait exception. La situation est analogue pour les options de « opt-out » dans les messages. Quelques pays, comme le Danemark, la Finlande, l'Allemagne, l'Italie, la Corée et le Royaume-Uni, ont un règlement qui exige cette option de manière à ce que les destinataires puissent s'opposer à ce que l'expéditeur leur envoie d'autres messages, ce que la France, le Mexique, la Norvège et la Pologne

n'imposent pas. Plusieurs pays interdisent les fausses informations dans les en-têtes et les messages : l'Australie, le Danemark, la France, l'Italie, la Pologne et les États-Unis.

A l'inverse, la plupart des pays examinés, à l'exception de l'Autriche et de la Corée, n'exigent pas l'établissement de listes « do-not-spam ». Au Royaume-Uni néanmoins, même s'il ne s'agit pas d'une obligation légale, des registres de « opt-out » ont été mis en place en vertu de codes de déontologie sectoriels. La loi américaine sur le spam exige de la FTC qu'elle élabore un programme et un calendrier de mise en œuvre d'un registre « do-no-e-mail » (ne pas envoyer de courriel) et signale tout problème concernant ce registre au Congrès dans les six mois suivant la promulgation de la loi.

Dernier point à relever : les sanctions pour violation des lois et règlements sur le spam se durcissent. Des pays comme la Corée ont amendé les règlements en vigueur de manière à augmenter considérablement les amendes imposées aux polluposteurs. D'autres, comme l'Italie, ne leur imposent pas seulement des amendes, mais aussi des peines de prison.

Mécanismes de réclamation

Pour traiter les réclamations avec plus d'efficacité, les autorités de certains pays, comme la Belgique, la France et les États-Unis,[53] ont mis en place des boîtes aux lettres spécialisées auxquelles les usagers peuvent faire suivre le spam. Les pouvoirs publics peuvent ainsi engager des poursuites judiciaires dans des cas précis, et fournir par ailleurs aux consommateurs des statistiques essentielles sur l'ampleur et la nature du spam.

Les limites de la réglementation : le problème de leur application effective

Plusieurs éléments viennent limiter l'efficacité de l'application des lois anti-spam : le faible rapport coût-efficacité, la difficulté à localiser les polluposteurs, la difficulté à recueillir des preuves à l'étranger, la diversité des réglementations selon les États et/ou pays, etc. Certaines interprétations des lois relatives à la protection de la vie privée en vigueur peuvent aussi créer des obstacles à une application efficace des lois si elles n'autorisent pas l'accès aux informations sur les polluposteurs présumés.

Le nombre de mesures législatives dans les pays Membres tend à indiquer que la loi est l'instrument stratégique de la lutte contre le spam. Il est toutefois évident qu'elle ne peut à elle seule résoudre le problème. De plus, certains règlements, comme la mention d'un label « ADV » dans l'en-tête des messages (que plusieurs lois nationales exigent), ne se sont pas avérés efficaces, 2 % des polluposteurs seulement s'y étant conformés.[54] Quelques organismes, comme la *Direct Marketing Association* (DMA), soutiennent que seuls des opérateurs de marketing direct respectueux de la loi utiliseraient effectivement ce label qui les assujettit volontairement à un filtrage massif. D'autres mettent aussi en doute l'efficacité des « registres do-not-e-mail » nationaux administrés par les pouvoirs publics, parce que ces listes sanctionneraient uniquement les distributeurs professionnels dignes de confiance qui s'y conforment. Par contre, il ressort d'un rapport d'enquête publié par ePrivacy en juillet 2003 que 37 % des consommateurs à peine utilisent l'option de « opt-out », essentiellement pour les raisons suivantes : crainte que l'opt-out ne confirme leur adresse au polluposteur ; incertitude quant à son efficacité ; doutes quant au respect de leur demande.[55]

Le spam est un problème mondial, puisque les courriels sont diffusés dans le monde entier. Compte tenu des problèmes pratiques rencontrés pour découvrir les fautifs, établir les compétences et appliquer les voies de droit, il est extrêmement difficile d'instruire les affaires concernant le spam et d'engager des poursuites judiciaires. Étant donné la nature universelle de l'Internet, les différentes mesures appliquées par les pays risquent de compliquer encore la mise en œuvre de solutions efficaces au niveau planétaire. Le spam produit hors de leur territoire sera hors de leur portée.

Plusieurs mesures ont cependant été prises à l'échelle internationale pour lutter contre le problème des escroqueries internationales. En juin 2003, notamment, l'OCDE a adopté de nouvelles lignes directrices pour encourager la coopération internationale dans la lutte contre les pratiques frauduleuses et trompeuses transfrontières *(Lignes directrices de l'OCDE régissant la protection des consommateurs contre les pratiques commerciales transfrontières frauduleuses et trompeuses)*. Les messages de spam contenant des informations trompeuses ou frauduleuses peuvent s'inscrire dans le cadre de ces lignes directrices, ce qui permet d'envisager la mise en œuvre du cadre de coopération pour la répression qu'elles décrivent.

Mesures d'autoréglementation

Plusieurs actions autoréglementaires visant à réduire le spam ont été engagées. Quelques-unes des mesures actuellement appliquées par le secteur privé sont présentées ci-dessous, notamment celles des organismes anti-spam, des FAI, des prestataires de services de messagerie électronique, du secteur de l'Internet, des sociétés de marketing par courriel, des organismes de protection du consommateur et des usagers finaux.

Activités autoréglementaires des principaux participants

Interventions des organismes de lutte contre le spam ou des organisations d'internautes

Bon nombre d'organismes de lutte contre le pollupostage affichent sur leur site web une liste des autres organismes anti-spam ou établissent des liens avec eux. L'annexe IV présente la liste de la SpamCon Foundation. Ces organismes essaient de sensibiliser les internautes au problème en publiant des informations, des documents, des statistiques et des lois relatifs au spam, et en leur proposant des moyens de l'identifier et de le combattre. L'un d'eux, Spamhaus,[56] fournit des outils techniques qui permettent de bloquer le spam, de localiser les polluposteurs et d'établir une liste noire des polluposteurs bien connus. D'autres organismes, comme la *Coalition contre les courriels publicitaires non sollicités* (CAUCE), participent activement aux débats législatifs.[57] D'autres encore, comme la SpamCon Foundation Law Center et SpamLaws.com, offrent des informations sur les lois relatives au spam en vigueur et/ou sur la façon d'engager une action juridique contre les polluposteurs. Certains gèrent des centres de notification qui reçoivent des réclamations sur le spam, et analysent ou font suivre les pourriels aux autorités compétentes aux fins d'enquête. D'autres organismes présentent des pratiques exemplaires ou encouragent les FAI et les distributeurs en ligne à appliquer des conditions rigoureuses qui interdisent le spam.

Les organisations d'internautes s'emploient aussi à lutter contre le pollupostage. L'association espagnole des internautes administre un site web anti-spam (http://aui.es/contraelspam), qui vient compléter d'autres mesures qu'elle a prises dans le cadre de son action : suivi de l'évolution du spam, campagnes de sensibilisation, établissement d'un centre de coordination des FAI, mise au moins de logiciels permettant aux usagers d'analyser et de filtrer les pourriels.

Les organismes de protection des consommateurs ont aussi pris des dispositions. Ainsi, le Dialogue transatlantique avec les consommateurs (DTAC), une coalition de plus de 60 organismes de consommateurs des États-Unis et des États membres de l'UE, a adopté une résolution[58] qui appelle à des actions collectives pour lutter contre le problème international du spam. Cette résolution préconise un régime de « opt-in » et recommande que les messages électroniques commerciaux ne soient envoyés qu'avec le consentement préalable explicite des destinataires.

Mesures appliquées par les FAI, les prestataires de services de messagerie électronique, et le secteur de l'Internet

Les FAI et les prestataires de services de messagerie électronique, premières victimes du spam, ont pris quelques dispositions préventives et punitives à son égard. La plupart ont appliqué des mesures techniques, comme les filtres de détection du spam entrant, et établi des listes noires produites par les usagers pour endiguer les flux de messages.[59] Ils essaient ainsi de prévenir l'épuisement des ressources de réseau et en bande passante, et d'appuyer les efforts des consommateurs en vue de réduire le spam. L'emploi de logiciels de filtrage soulève toutefois le problème de la légitimité d'une décision prise par un FAI privé de bloquer les messages en provenance d'un expéditeur donné. De plus, les filtres ne fonctionnent pas quand l'adresse électronique de l'expéditeur est masquée ou falsifiée. En revanche, dans le cadre de leurs contrats de service, les FAI se réservent le droit de résilier le compte d'un abonné qui se livre à des pratiques abusives.[60] Un FAI américain a intégré à son contrat une clause établissant qu'il pourrait facturer à un abonné jusqu'à USD 50 par message spam transmis. [61]

L'Association canadienne des fournisseurs Internet (ACFI) a élaboré un code de conduite fondé sur les pratiques optimales de ses membres. Dans le cadre de leur rivalité commerciale, les FAI sont libres d'établir leurs propres politiques d'utilisation admissible et de les appliquer aux termes de leurs accords de service. Selon l'ACFI, la vaste majorité de ses membres interdisent déjà l'utilisation de leurs réseaux pour l'envoi de messages électroniques en nombre et se réservent le droit de résilier le compte de tout abonné se livrant à cette activité.[62] Quelques FAI essaient de diminuer la capacité des polluposteurs à utiliser des comptes anonymes par la mise en œuvre de technologies adaptées, comme l'identification de la ligne appelante (ILA), et encouragent les normes d'identification pour les comptes prépayés. D'autres associations du secteur de l'Internet, comme l'Association mexicaine de l'industrie publicitaire et commerciale sur l'Internet, ont établi des codes déontologiques qui couvrent l'utilisation des données personnelles à des fins de commercialisation.

L'un des plus grands avantages du spam est la modicité de son coût pour l'expéditeur. Quelques prestataires de services de messagerie électronique ont tenté de traiter ce problème sur le plan commercial ; ils ont ainsi essayé de réduire le spam et d'en dégager des compensations financières. Le prestataire coréen de services de messagerie électronique Daum a par exemple mis en place, en avril 2002, un « mécanisme d'affranchissement en ligne » qui vise à limiter le spam envoyé à ses abonnés.[63] Cette démarche se fonde sur la théorie selon laquelle le pollupostage enregistrerait un recul spectaculaire si les expéditeurs de messages commerciaux en nombre étaient obligés de payer leur expédition. Il a été suggéré qu'en tant que bénéficiaire du spam, l'expéditeur devrait partager le coût de l'infrastructure de réseau.

Le secteur de l'Internet a également lancé des campagnes de sensibilisation pour aider les usagers à comprendre le spam et à le réduire. La *Internet Industry Association* australienne a ainsi donné le coup d'envoi d'un programme auxquels participent 11 fournisseurs de logiciels anti-spam qui ont accepté, le 16 avril 2000, d'offrir pendant un mois des essais gratuits de leurs produits à tous les internautes australiens.[64] Le secteur australien des télécommunications a aussi élaboré en 2002 un code de déontologie concernant le spam SMS. Enfin, des services publics comme GetNetWise (http://spam.getnetwise.org), administrés par des sociétés Internet et des organismes d'intérêt public, aident les usagers à lutter contre le spam en leur communiquant des solutions et des renseignements utiles.

Par ailleurs, le nombre de poursuites engagées contre les polluposteurs augmente. Ces derniers temps, les entreprises ont été plus nombreuses à essayer d'intenter contre eux des poursuites au civil pour les pertes subies à cause du spam. Le géant de l'industrie logicielle Microsoft Corp. a ainsi pris la décision, en 2003, de mettre un frein aux messages non sollicités en engageant aux États-Unis et au Royaume-Uni une douzaine d'actions en justice contre des sociétés qui ont envoyé plus de deux milliards de messages spam à ses clients, et dont beaucoup utilisent son service gratuit Hotmail. EarthLink a récemment engagé

des poursuites pour USD 5 millions contre 100 polluposteurs présumés. Ce type d'actions judiciaires intentées par les FAI pourrait avoir un effet dissuasif sur les polluposteurs.

Mesures prises par les sociétés de marketing électronique (ou en ligne, direct)

Prolifération des listes de refus. Le souhait exprimé par un particulier de ne pas recevoir de spam constitue en soi une information utile qui, lorsqu'elle est diffusée aux détaillants, leur permet de réduire les frais de commercialisation improductifs et d'éviter des réactions négatives et des plaintes. Dans quelques pays européens, les fédérations nationales du secteur du marketing direct, la FEDMA (Fédération du marketing direct européen) ou des organisations plus récentes représentant l'industrie en ligne sont en train de mettre en place des listes de refus. Créées en France en 1998, ces listes sont activement promues par la Fédération des Entreprises de Vente à Distance (FEVAD) depuis l'été 1999. Elle constitue un modèle dont pourraient s'inspirer d'autres pays, et un accord a été signé avec la Fédération allemande du marketing direct à cet effet. L'Association Belge du Marketing Direct (ABMD) a aussi établi une liste générale de refus à l'échelon national.

Presque toutes ces dispositions ont été prises par suite de l'adoption de la Directive 2000/31/CE sur le commerce électronique et de son article 7(2).[65] Il ressort d'une enquête exhaustive que la Commission européenne a conduite auprès des fédérations industrielles européennes de mai à octobre 2000 que des listes de refus ont été établies en Finlande, en Allemagne, en Italie, aux Pays-Bas, en Norvège, en Espagne, en Suède et au Royaume-Uni. Elles ne devaient initialement couvrir que l'État membre concerné, mais la plupart des fédérations à l'origine de leur création prévoient de les élargir prochainement à l'ensemble de l'UE, voire à des pays non-membres de l'UE.[66] Néanmoins, du fait que les pays membres de l'UE ont opté pour le régime de « opt-in » dans les lois transposant la directive 2002/58/CE, on ne sait si les listes de refus continueront tout de même de se développer dans ces pays.

Aux États-Unis, la *Direct Marketing Association* (DMA) a également instauré à l'intention des consommateurs un dispositif de préférences autoréglementaire (système de « opt-out ») qu'elle administre elle-même. Les consommateurs peuvent enregistrer leur souhait de ne pas recevoir de spam dans le *e-Mail Preference Service* (e-MPS), géré par la DMA, après quoi tous les membres de la DMA désireux d'envoyer un courriel commercial non sollicité doivent retirer les personnes enregistrées de leurs listes de clients potentiels.[67] Les numéros de téléphone mobile peuvent aussi être enregistrés gratuitement auprès du *Telephone Preference Service* britannique (quoique celui-ci soit maintenant supplanté par les nouveaux droits de « opt-in » pour les SMS).[68]

Marketing direct par « opt-in » (autorisation ou consentement préalables). Un nombre grandissant de sociétés de marketing direct et électronique ont adopté les principes de l'autorisation préalable et du courriel avec consentement explicite. En octobre 2002, la Fédération finlandaise de marketing direct a ainsi adopté un code de conduite qui exige un système de « opt-in ». Le modèle de collecte des adresses électroniques consiste à afficher des formulaires de consentement préalable sur les sites web. Les visiteurs remplissent les formulaires en ligne pour s'abonner à une lettre d'information, participer à un concours ou à une opération promotionnelle, ou recevoir des offres spéciales en ligne en fonction des centres d'intérêt qu'ils précisent. Bon nombre de sites web donnent maintenant à leurs visiteurs deux possibilités : *i)* indiquer s'ils souhaitent recevoir des messages commerciaux ou pas ; *ii)* signaler si leurs données peuvent ou ne peuvent pas être communiquées à des tiers. Les pratiques de marketing direct par consentement préalable, surtout quand elles sont le fait de distributeurs professionnels, semblent connaître une progression foudroyante dans les pays Membres qui ont adopté un régime de « opt-in » ou sont en train de le faire (l'Australie et les pays membres de l'UE par exemple).

Codes, lignes directrices et/ou autres engagements de principe. Les associations de marketing direct ont aussi rédigé des lignes directrices, comme les *Commercial Solicitations Online Guidelines* de la DMA, qui couvrent l'envoi de courriels commerciaux, et notamment dans quelles circonstances ces messages peuvent être envoyés, l'utilisation du *e-Mail Preference Service*, et la définition claire de l'identité de l'expéditeur.[69] Des associations comme l'Association canadienne de marketing (ACM) ont établi des codes et des lignes directrices destinés à ceux de leurs membres qui distribuent du matériel promotionnel par l'intermédiaire de l'Internet.[70] Certaines, telle la *Network Advertising Initiative* (NAI), un groupe coopératif de publicitaires de réseau, et l'*Association for Interactive Marketing* (AIM), un organisme commercial à but non lucratif, ont élaboré un ensemble de principes portant sur la protection de la vie privée.[71] Ils fournissent également aux particuliers et aux entreprises des conseils sur la façon de réduire la quantité de spam. Certaines sociétés ont adopté des mesures qui permettent au destinataire d'un courriel identifié comme étant commercial de s'inscrire sur un registre de refus en cliquant simplement sur un lien figurant à la fin du message.

Inconvénients des mesures autoréglementaires

Les mesures autoréglementaires, bien qu'elles puissent s'avérer essentielles dans la prévention du spam, présentent plusieurs inconvénients. Peu de polluposteurs sont membres de l'*Internet Industry Association* ou sont susceptibles d'adhérer volontairement à son code. Malheureusement, un code de conduite n'assure qu'une protection limitée contre les « mauvais » polluposteurs. Ceux-ci trouvent facilement le moyen d'éviter les systèmes et/ou les mesures autoréglementaires punitives ; ils peuvent par exemple faire un usage créatif de la programmation, changer de FAI, falsifier leurs identités, etc.

Éducation et sensibilisation

L'éducation et la sensibilisation des consommateurs, conjuguées à d'autres mesures, peuvent concourir à diminuer substantiellement le spam. La sensibilisation permettrait à de nombreuses victimes du spam (qui diffusent sans le savoir leurs adresses sur des espaces publics ouverts aux polluposteurs) de s'en libérer, mais pourrait aussi augmenter les frais de collecte d'adresses électroniques pour les polluposteurs, diminuant ainsi la rentabilité du spam. L'éducation est aussi une solution qui transcende les frontières géographiques. La loi a une capacité restreinte à protéger un usager d'un polluposteur étranger, mais les mesures prises par un utilisateur informé seront utiles où que le polluposteur soit localisé.

A cet égard, beaucoup d'organisations de protection des consommateurs ont organisé des programmes de formation et de sensibilisation pour permettre aux usagers de prendre en connaissance de cause des décisions en matière de stratégies et de techniques anti-spam. Ces activités et programmes, dans la plupart des cas, ont été conduits en conjugaison avec d'autres programmes de sécurité électronique qui portaient notamment sur la lutte contre les virus, la confidentialité des données en ligne ou la protection du consommateur.

Bon nombre d'organismes de protection des consommateurs ont sensibilisé le public en l'informant des stratégies du spam et en lui suggérant des moyens d'empêcher ce phénomène. Ainsi, le *Center for Democracy and Technology* (CDT) a récemment publié un rapport sur les méthodes les plus efficaces pour bloquer la réception de messages non sollicités, par exemple en masquant les adresses électroniques ou en les dissimulant.[72] Le rapport soulignait que les consommateurs devaient être conscients que certains domaines de l'Internet, comme les groupes de nouvelles, ne présentent pas ou peu de sécurité. D'autres organismes ont pris des mesures pour aider techniquement les usagers, en ligne ou sur place, à empêcher le spam. Ainsi, la *Korea Information Security Agency* a, dès 2002, mis sur pied des stratégies visant à contrôler les points faibles du secteur privé, et a aidé les usagers à réaliser des opérations d'autovérification

de manière à fermer les serveurs relais ouverts. Une autre opération intéressante est la mise au point d'un outil appelé « signal vérifié », comme le message *Trusted Sender*, qui vise à authentifier l'expéditeur, l'intégrité du message, etc.[73] Certaines associations de consommateurs fournissent une liste noire des polluposteurs. On peut citer pour exemple la liste publiée par l'Union Fédérale des Consommateurs de Quimper, une association française, dans son bulletin « *Arnaques-infos* ».

Les instances de réglementation et les pouvoirs publics, qui jouent un rôle essentiel en matière de sensibilisation et d'information du public en matière de spam, ont aussi élaboré à l'intention des entreprises et des particuliers des guides exhaustifs qui expliquent comment empêcher le spam et comment les lois en vigueur peuvent être appliquées pour le combattre. Beaucoup de gouvernements encouragent les acteurs du secteur à s'y attaquer par l'adoption volontaire de codes et de pratiques sectoriels. Ainsi, le Département du Trésor australien a établi un « Modèle australien des pratiques optimales en matière de commerce électronique », destiné à toutes les entreprises en ligne, qui contient des dispositions particulières au marketing direct sur l'Internet.[74]

Aux États-Unis, la FTC administre un site web spécialisé dans la sensibilisation au spam, qui fournit aux usagers des informations sur la façon de réagir au pollupostage. L'autorité française de protection des données a affiché sur son site des informations fournies sur les divers aspects du spam. La Commission européenne prévoit également de publier prochainement des renseignements sur son site EUROPA, notamment les règlements des États membres, des hyperliens aux sites nationaux, ainsi que des chiffres relatifs au spam et son évolution dans l'UE. Elle va aussi élaborer un plan d'action pour un Internet plus sûr afin de favoriser la coordination des opérations et programmes de sensibilisation à cet égard dans les États membres.

Les FAI et entreprises d'Internet ont également favorisé la sensibilisation et l'éducation d'utilisateur. Par exemple, Microsoft a lancé le MSN Spam Buster[75], un site Web d'éducation sur le spam qui conseille des utilisateurs d'Internet comment se protéger contre le spam, y compris l'utilisation des filtres.

Solutions techniques

Compte tenu de l'augmentation rapide du volume de spam et de la modicité des coûts d'entrée pour les fournisseurs, les produits anti-spam se sont multipliés. De nombreux services et nouveaux produits destinés à fournir des solutions techniques aux utilisateurs, prestataires de services et aux entreprises ont été mis sur le marché récemment. Certains des outils techniques susceptibles d'aider à filtrer ou à bloquer les messages électroniques non sollicités sont présentés ci-dessous.

Structure actuelle du courrier électronique

L'une des raisons techniques essentielles à la prévalence du spam est que le SMTP (protocole de transfert de courrier simple), le protocole utilisé pour transmettre les messages entre les serveurs (ou d'un client à un serveur), ne vérifie pas la validité de l'identifiant de l'expéditeur, par exemple le « serveur expéditeur » ou l'adresse d'origine. Ces deux identifiants sont les seules informations d'identité reçues avant que le message ne soit transmis au travers du SMTP, et tous deux sont falsifiables. Il n'existe en outre aucun mécanisme permettant de vérifier l'intégrité du corps du message. Le contenu d'un courriel, à savoir l'objet et d'autres informations, sont transmis dans un bloc de données et ne sont pas jugés constituer une partie utile de l'échange SMTP. [76] Dans ce cas, le fait de ne pas tenir compte du contenu accroît substantiellement la performance (lecture de volumes importants du trafic mondial de messages électroniques) mais, en l'absence d'automatismes régulateurs, il soulève aussi des problèmes de confiance et d'obligation de rendre compte. En l'absence d'une obligation de rendre compte, le spam prospère.

Déploiement de services et de technologies anti-spam

Les solutions anti-spam protègent les entreprises, les FAI et les particuliers et les aident à réduire le temps passé à lire et à gérer les courriels indésirés en filtrant le contenu inapproprié et offensant. L'une d'elles fait appel à des filtres qui utilisent des « listes noires » constituées de noms de domaines ou d'adresses IP (protocole Internet) de polluposteurs connus. Ces listes peuvent être établies de manière collective. Dès lors qu'un nombre suffisant de destinataires à l'intérieur d'une communauté d'usagers objecte à un message donné, celui-ci est automatiquement transféré aux répertoires « spam » de futurs usagers. Une autre solution technique, la « liste blanche » ou « liste des expéditeurs agréés », permet aux usagers d'identifier le courriel provenant d'expéditeurs agréés et reconnus. Si ces listes améliorent parfois le filtrage du spam, elles sont actuellement exposées à l'usurpation d'adresses IP ou à la falsification des données sources des courriels. Un autre outil technique efficace consisterait à configurer le système du client de manière à ce qu'il n'accepte que les messages signés par des certificats numériques sécurisés émis par une autorité de certification. Les dispositifs de signature numérique, comme les infrastructures à clé publique, peuvent être utilisés à cette fin.

Il existe en outre d'autres techniques anti-spam, dont les outils d'analyse comportementale qui recherchent certaines structures, un grand nombre de destinataires par exemple. Les logiciels de validation d'adresses inversent les paramètres des systèmes de noms de domaine pour vérifier que l'expéditeur n'essaie pas de masquer son identité. Les empreintes numériques mises au point au moyen d'algorithmes et d'heuristiques servent aussi à identifier et à bloquer ou filtrer les structures courantes de spam.

De nouveaux produits arrivent sur le marché qui sont capables de rechercher des graphiques (tons de chair par exemple) pour combattre la pornographie, mais ils sont encore à un stade embryonnaire de développement.[77] Une autre technique nouvelle, le filtrage bayesien, apprend et réapprend comment repérer le spam en balayant les courriels que les usagers ont lus et ceux qu'ils ont rejetés sans adhérer à un jeu de règles particulier. Il effectue ensuite un calcul des probabilités d'après les caractéristiques inhabituelles de chaque message et décide quel type de courriels livrer et refuser. Cette solution est peut-être viable car seuls les destinataires savent ce qui les intéresse. Ce dispositif devrait être précis à 99 %. Sa sortie commerciale est prévue en 2004. Un autre dispositif récemment introduit est le protocole défi-réponse : il oblige l'expéditeur à confirmer son identité avant d'être ajouté à une « liste blanche » qui lui permet d'envoyer librement des messages par la suite.

La plupart des solutions anti-spam associent généralement plusieurs composantes techniques : balayage basé sur des règles heuristiques, listes noires et blanches, outils d'analyse du contenu, autres dispositifs de sécurité essentiels comme l'authentification SMTP,[78] et mises à jour des moteurs heuristiques configurables au niveau du réseau[79] à mesure que de nouveaux filtres permettent aux dispositifs de s'adapter à ceux des polluposteurs. En règle générale, pour identifier le spam, ces techniques ne se limitent pas à comparer les adresses électroniques à une liste de polluposteurs connus, mais analysent intégralement le contenu du message électronique en recherchant des publicités courantes et des modèles de textes pornographiques. Elles appliquent aussi des filtres à « logique floue » à chaque courriel examiné sous le contrôle de l'usager. Elles sont en outre automatiquement mises à jour, car les techniques de spam évoluent rapidement.

Travaux des groupes d'experts techniques

Des travaux visant à trouver des solutions techniques de prévention/réduction du spam ont été réalisés au niveau des entreprises individuelles et par de nombreuses sociétés dans le cadre d'une démarche collective et coopérative. Face à l'ampleur croissante du problème du pollupostage, les entreprises de technologie sont de plus en plus nombreuses à discuter des moyens de le combattre. Une conférence

sectorielle anti-spam s'est tenue le 27 février 2003 pour coordonner une approche sectorielle à cet égard. Des participants de tous les secteurs commerciaux et technologiques concernés par le spam ont envisagé une solution plus globale au problème. L'idée serait que les entreprises du secteur unissent leurs efforts pour produire un protocole anti-spam ouvert, interopérable, qui fonctionnerait entre tous les systèmes de messagerie électronique d'origine hétérogène et arrêterait le spam tout en garantissant la transmission sûre du courrier légitime.[80]

Par ailleurs, plusieurs grandes entreprises technologiques, dont Yahoo, Dell Computer, Oracle, Microsoft et Sun Microsystems, se sont réunies le 14 mars 2003 à San Francisco pour évoquer les solutions anti-spam. L'objectif du forum, appelé « JamSpam », était de créer une spécification anti-spam ouverte, interopérable, qui servirait de solution universelle au spam. Les discussions ont notamment porté sur l'élaboration de normes d'authentification du courriel de manière à ce que les messages légitimes soient reconnus et transmis en toute sécurité. Lors d'une réunion spéciale des FAI et des prestataires de services de messagerie électronique, les différentes entreprises ont discuté de solutions techniques visant à fermer les relais ouverts. Elles souhaitaient par ailleurs construire un système assurant une plus grande transparence des messages légitimes envoyés, à savoir l'identification de la nature d'un courriel - qu'il s'agisse d'une lettre d'information, d'une facture émanant d'un site de commerce électronique, ou du message d'un ami.

En avril 2003, les sociétés Microsoft, AOL et Yahoo ont annoncé avoir engagé une collaboration dans le but de bloquer les messages non-identifiés et d'empêcher les polluposteurs de créer des comptes de messagerie frauduleux. Par ailleurs, quelques FAI se sont aussi rassemblés pour trouver des solutions techniques au spam. En Pologne, par exemple, les plus grands portails Internet et les principaux prestataires de services de messagerie électronique - Onet, Wirtualna Polska et Interia - ont formé en mai 2003 une coalition pour tenter de mettre un terme au spam envoyé par l'intermédiaire de leurs systèmes. Les trois sociétés ont élaboré un plan d'action commun afin de mettre au point une nouvelle technologie qui empêcherait les particuliers et les entreprises d'envoyer du spam.

Les débats sur les technologies anti-spam se poursuivent. Un influent organisme de normalisation de l'Internet a entrepris un examen minutieux du problème grandissant du spam électronique, dans le cadre d'une opération qui pourrait avoir de vastes retombées sur l'utilisation et la sécurité futures du courrier électronique. Un Groupe de recherche anti-spam officiel[81] a été réuni sous les auspices de l'*Internet Research Task Force*, un organisme non officiel affilié à l'*Internet Engineering Task Force* (IETF). Ce nouveau groupe est un organisme d'études ouvert, qui n'est pas habilité à prendre des mesures, mais ses conclusions pourrait à terme changer la façon dont les FAI et les réseaux gèrent le courrier électronique. Par ailleurs, le 16 septembre 2003, les directeurs généraux et les cadres dirigeants de quarante entreprises (FAI, sociétés de filtrage du spam, et sociétés de messagerie électronique) ont organisé à San Francisco un *E-Mail Deliverability Summit* pour examiner le problème des faux positifs et améliorer les taux de livrabilité des messages légitimes tout en permettant aux systèmes récepteurs d'identifier le spam. Certaines normes relatives à la gestion des messages retournés, aux demandes de désabonnement, à la publication des règles en matière de permission et à la communication entre les entreprises expéditrices et destinataires ont été présentées.[82]

Imperfections des solutions techniques

La plupart des systèmes anti-spam font actuellement appel au blocage par mot-clé ou par liste noire, qui produit un nombre important de faux positifs. Ces derniers se produisent quand un courriel légitime est traité par erreur comme du spam et filtré. Il est toujours possible que l'ensemble des messages provenant d'un site inscrit sur une liste noire soient systématiquement supprimés sans être livrés.[83] Par ailleurs, les listes noires anti-spam bloquent souvent d'innocents internautes connectés au réseau par l'intermédiaire de

FAI bloqués. Il est arrivé que des domaines nationaux entiers soient paralysés. Si certains usagers se sont sentis sécurisés par ces filtres, bon nombre de FAI soutiennent qu'ils ont eu pour effet de victimiser des « innocents », y compris des FAI qui hébergent à leur insu des polluposteurs, des internautes dont l'adresse IP a pu être usurpée par un polluposteur, et les adresses attenantes à celles du polluposteur présumé.

Pour neutraliser ce problème, les fournisseurs de solution anti-spam proposent plusieurs méthodes, comme le balayage fondé sur des règles heuristiques et les filtres à logique floue. Quoi qu'il en soit, il est très difficile de déterminer par des moyens purement automatisés si un message particulier est du spam ou pas. Les algorithmes informatiques destinés à identifier le spam ne sont pas parfaits, loin s'en faut. Par ailleurs, les techniques assez nouvelles, comme les protocoles défi-réponse, ont pour inconvénient d'imposer un fardeau supplémentaire aux expéditeurs légitimes. De plus, les propriétaires de listes comprenant de nombreux abonnés, ceux qui envoient des lettres d'information par exemple (systèmes de réponse automatisé), ont du mal à répondre personnellement aux courriers défi-réponse, de sorte que les abonnés cessent parfois de recevoir leur lettre. Cela équivaut à un faux positif.

Une autre solution au filtrage du spam est le modèle consensuel, selon lequel les personnes qui reçoivent des messages qu'elles jugent être du spam le signalent à une entité coordinatrice. Un programme informatique coordonne ensuite toutes les données reçues. Une liste convenablement compilée des polluposteurs connus constituerait aussi une amélioration substantielle aux listes noires non réglementées en usage actuellement. Quoiqu'il en soit, il est quasiment impossible de produire des systèmes de filtrage parfaits.

Beaucoup de polluposteurs maîtrisent suffisamment la technologie pour dissimuler leurs traces, régler leurs systèmes de manière à passer au travers des filtres et franchir d'autres obstacles techniques. Ils peuvent contrôler électroniquement les ordinateurs non protégés, et en faire ainsi un outil pour envoyer leur spam. Tant que le coût des envois en nombre sera aussi modique, les polluposteurs auront tout intérêt à trouver les moyens de défier les limites technologiques.

Les solutions anti-spam augmentent inévitablement les coûts et les temps d'attente des FAI, des prestataires de services de messagerie électronique, et des consommateurs. Des services efficaces de filtrage des courriels peuvent entraîner des coûts supplémentaires considérables pour les prestataires de services, et ils ont souvent des effets secondaires sur la performance des communications. Le filtrage des messages coûte du temps et de l'argent aux FAI, et ralentit le fonctionnement du réseau. Quelques FAI estiment que les filtres sont utiles, au moins au niveau du consommateur, mais ils ne sont pas toujours souhaitables ou faciles à concevoir, configurer ou installer à celui du FAI.[84]

CONCLUSION

Le faible coût et la portée mondiale du courriel et autres messages électroniques en ont fait un moyen de communication d'une grande importance, qui rencontre un immense succès. Cependant, la forte croissance du pollupostage (« spam ») est une menace pour la commodité et l'efficience des messages électroniques et elle sape plus généralement la confiance de l'utilisateur à l'égard des réseaux. Diverses mesures et initiatives ont été prises dans les pays de l'OCDE pour répondre aux accroissements de volume récents du spam et pour renforcer la confiance des consommateurs à l'égard des réseaux. Il ne semble pas, toutefois, que ces mesures de réglementation, d'autorégulation ou les remèdes techniques aient pour le moment réussi à ralentir la croissance du spam. Les efforts renouvelés pour résoudre ce problème devront tenir compte du fait que l'on ne peut se limiter à une seule voie d'approche, quelle qu'elle soit, si l'on veut faire barrage au spam, et qu'une coordination internationale sera nécessaire pour traiter un problème qui ne connaît pas les frontières nationales.

Nécessité d'une approche pluridimensionnelle

Aucune voie d'approche actuelle à l'égard du spam n'est exempte de limites. Les approches juridiques se heurtent au fait que les polluposteurs sont souvent habiles à cacher leur identité et à opérer à travers les frontières. Pour l'autorégulation, la grande difficulté est d'assurer la participation volontaire des expéditeurs de spam et leur observance des codes de bonnes pratiques professionnels. Une plus grande sensibilisation et une éducation accrue du public sont nécessaires pour répandre des pratiques informatiques plus sûres. A cet égard, on pourrait joindre les stratégies anti-spam aux campagnes générales sur la sécurité électronique. Du côté technique, un soutien continu à la mise au point et au déploiement des outils techniques visant à combattre le spam est nécessaire pour contribuer à faire en sorte que celui-ci ne déjoue pas les filtres des FAI ou autres parties. Globalement, une approche mixte associant les solutions réglementaires, autorégulatoires et techniques et la sensibilisation des utilisateurs offre les meilleures perspectives pour réduire le spam.

La coopération internationale est aussi un facteur essentiel

Le spam n'est pas le problème d'un seul pays, ni même des seuls pays de l'OCDE. C'est un problème mondial. Ce caractère mondial du spam pourrait encore s'affirmer davantage avec l'accès à l'Internet et son utilisation dans les pays en développement, qui augmentent continûment. Il est de plus en plus évident que les efforts nationaux doivent être complétés par des stratégies coordonnées à l'échelle internationale, afin de relever les défis transfrontaliers que pose le spam.

ANNEXE I. LEGISLATIONS NATIONALES

Australie - "Opt-in"

Le SPAM Bill 2003 a été voté par le Parlement australien le 2 décembre 2003. Cette loi adopte un régime de "opt-in" pour les messages électroniques commerciaux. Ces messages électroniques comprennent le courrier électronique, la messagerie instantanée, la messagerie de texte ou de vidéo à destination des téléphones mobiles et autres messages définis dans la réglementation. La loi exige aussi que les messages indiquent l'adresse exacte de l'expéditeur et qu'ils offrent un moyen de désinscription fonctionnel ; elle interdit la distribution et l'utilisation d'outils permettant de moissonner les adresses électroniques et de listes d'adresses moissonnées ; elle encourage la création de codes professionnels appropriés. La loi prévoit aussi un régime de sanctions civiles flexible et évolutif avec des avertissements, des avis de contravention et des peines infligées par les tribunaux. Les personnes physiques qui contreviennent à la législation en expédiant du spam s'exposeront à une amende totale de 44 000 AUD au maximum, pour les infractions commises un jour donné ; l'amende maximale applicable à une organisation est de 220 000 AUD pour un jour donné. Cette législation interdit aussi le moissonnage de répertoires et les attaques de type dictionnaire, quand ces agissements ont pour but le spam ou autres activités connexes. L'Australian Communications Authority (ACA) aura le pouvoir de mener des investigations, de délivrer des avis de contravention et d'intenter des actions en justice. Quand une personne ou une société a subi des pertes ou dommages dus à l'activité d'un polluposteur, l'ACA peut demander en leur nom une indemnisation au tribunal.

Autriche - "Opt-in"

La section 101 de la loi de régulation des télécommunications (Journal officiel autrichien n° 100/1997) exige un consentement préalable des destinataires pour l'envoi en masse de messages électroniques à des fins commerciales.[85] Conformément à l'article 7(2) de la loi sur le commerce électronique ("*Bundesgesetz, mit dem bestimmte rechtliche Aspekte des elektronischen Geschäfts-und Rechtsverkehr geregelt werden")*, la *Rundfunk und Telekom Regulierungs* a établi une liste de refus ("opt-out"), ouverte à tous les utilisateurs, énumérant les personnes qui ne souhaitent pas recevoir une correspondance commerciale par courrier électronique.[86]

Belgique - "Opt-in"

La Belgique a adopté un régime de "opt-in" pour le "courrier électronique à des fins de publicité" dans la loi du 11 mars 2003 sur la commerce électronique. Cette loi exige que l'expéditeur fournisse une information sur le droit qu'a le destinataire de s'opposer, pour l'avenir, à recevoir les publicités par courrier électronique. Elle interdit aussi à l'expéditeur d'utiliser l'adresse électronique ou l'identité d'un tiers et de falsifier ou de masquer toute information permettant d'identifier l'origine du message. La preuve que les courriers électroniques publicitaires ont été sollicités incombe à l'expéditeur.

Canada – régime de "opt-in" en appliquant la loi existante

Avant la Loi sur la protection des renseignements personnels et les documents électroniques, le gouvernement canadien avait adopté une position suivant laquelle la distribution de matériel promotionnel et informatif non sollicité concernant des produits, sous forme imprimée ou par voie électronique, n'était ni illégale ni réglementée au Canada.[87] Cependant, aux termes de cette loi entrée en vigueur en janvier 2001, les adresses électroniques sont considérées comme des informations à caractère personnel et sont ainsi soumises aux dispositions de la loi. La collecte et l'utilisation d'informations à caractère personnel (telles que les adresses électroniques) sans le consentement de la personne concernée pourraient être contraires aux exigences de la loi. Le Commissaire à la protection de la vie privée du Canada est chargé de veiller à l'application de cette loi.

Cette loi oblige aussi les entreprises et autres parties qui conservent des adresses électroniques à assurer une sécurité appropriée à ces renseignements personnels. Elle s'applique, durant les trois premières années qui suivent son adoption, aux organisations assujetties à la réglementation fédérale et aux entreprises du secteur privé qui s'adonnent au commerce interprovincial et international des renseignements personnels. Après cette période, toute organisation utilisant des renseignements personnels pour la conduite d'activités commerciales sera assujettie à la loi. Ainsi les entreprises qui achètent, vendent, louent ou troquent des listes d'adresses électroniques – qui sont à la base du courrier électronique en vrac non sollicité - par-delà des frontières provinciales et nationales, seront visées par la nouvelle loi.[88] Toutefois, il n'existe pas de réglementation spécifique sur le spam pour le moment.

En outre, bien qu'il n'existe pas de législation spécifique traitant du spam au Canada, les messages qui véhiculent des assertions fallacieuses ou des pratiques de marketing trompeuses pourrait enfreindre certains articles de la Loi sur la concurrence ou autres textes de loi dont l'application est confiée au Bureau de la concurrence au Canada.

République tchèque –régime de "opt-in" en appliquant la loi existante

Le problème du spam est décrit de manière générale dans l'article 2 de la loi n° 40/1995 Coll. sur la réglementation de la publicité. Il est interdit d'envoyer une communication commerciale non sollicitée si elle tend à une dépense quelconque de la part du destinataire ou si elle dérange le destinataire. La recommandation concernant le spam dans la version provisoire du Livre blanc sur le commerce électronique devait être soumise à l'approbation du gouvernement au cours du deuxième trimestre 2003. La plupart des objectifs définis par la Directive 2000/31/CE ont été transposés dans le cadre juridique tchèque. Le gouvernement se penche maintenant sur les exigences qui n'ont pas encore été satisfaites.[89]

Danemark - "Opt-in"

Le Danemark a adopté un modèle de "opt-in" avec des modifications. La loi danoise sur les pratiques de marketing exige que le consommateur, avant de recevoir un "appel par courrier électronique,…" , ait *demandé* celui-ci. Une nouvelle section en vigueur depuis le 25 juillet 2003 modifie cette règle, en permettant un fournisseur qui a eu l'adresse électronique d'un consommateur en connexion avec une vente d'un bien ou service à envoyer le courrier électronique non sollicité sans que le consommateur l'ait explicitement demandé, quand un certain nombre de conditions bien définies sont remplies. Le consommateur doit être en mesure de manifester son refus facilement et gratuitement à tout moment. Ce nouveau paragraphe ne s'applique qu'au courrier électronique. La législation danoise exige aussi dans les messages une identité et une adresse véridiques ainsi que l'offre d'un moyen de refus ("opt-out"), et elle interdit la falsification des informations dans les en-têtes et les messages.

Finlande - "Opt-in"

La nouvelle Directive 2002/58/CE du Parlement européen et du Conseil concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques a été adoptée le 12 juillet 2002. Sa transposition nationale dans la législation finlandaise est entrée dans une phase finale. La Directive entrera en vigueur avec la nouvelle loi finlandaise sur la protection de la vie privée dans les communications électroniques. Le gouvernement a pris sa décision sur le contenu de la loi sur la protection de la vie privée et la sécurité des données dans les communications électroniques le 15 octobre 2003. Le projet de loi a été présenté au Parlement le 24 octobre. Il est actuellement en cours d'examen par les diverses commissions parlementaires. La commission parlementaire pour les transports et les communications présentera probablement en mars 2004 son avis sur la proposition gouvernementale. Ce projet de loi pourrait être voté au printemps ou au début de l'été 2004.

Aux termes de ce nouveau projet de loi, la prospection directe au moyen d'automates d'appel, de télécopieurs, de courrier électronique, de mini-messages SMS, de messages sous forme de texte, de voix, de son ou d'image n'est autorisée à destination d'une personne physique que si celle-ci a donné préalablement son consentement. (Cependant, quand un fournisseur de service ou le vendeur d'un produit obtient d'un de ses clients, qui est une personne physique, dans le cadre de la vente d'un produit ou service, des renseignements permettant de le joindre par courrier électronique ou messages sous forme de texte, de voix, de son ou d'image, ce même fournisseur de service ou vendeur de produit peut utiliser ces renseignements pour le marketing direct de ses propres produits dans le même groupe de produits, ou de produits ou services similaires. Le fournisseur de service ou vendeur de produit doit donner à toute personne physique qui est son client la possibilité de s'opposer, sans frais et de manière simple, à l'utilisation de ces renseignements lorsqu'ils sont recueillis et lors de chaque message de courrier électronique ou autre message sous forme de texte, de voix, de son ou d'image).

La nouvelle loi n'exige pas le "opt-in" pour les personnes morales, mais elle demande l'étiquetage des messages et l'offre d'un moyen de refus ("opt-out")dans les messages. Elle interdit les informations fausses dans les en-têtes et les messages. Elle interdit l'envoi de messages de marketing direct qui déguisent ou cachent l'identité de l'expéditeur ou qui ont des adresses invalides. Selon ce projet, les opérateurs de télécommunications et les entreprises ou associations abonnées des télécommunications auraient le droit de filtrer les messages électroniques de marketing illicites et les programmes malveillants, afin de sécuriser les services de communication. Avec le consentement de l'utilisateur, cela permettrait de mieux filtrer le courrier électronique nuisible.

Le système de "opt-in" en ce qui concerne les personnes physiques est obligatoire depuis 1999 en vertu de la loi n°1999/565 sur la protection de la vie privée et la sécurité des données dans les télécommunications. Cette loi n'exige pas le "opt-in" pour les personnes morales. Un abonné qui n'est pas une personne physique peut notifier son refus. Cette loi stipule aussi que le marketing direct destiné aux consommateurs est en outre soumis aux dispositions de la loi de protection des consommateurs (n° 1978/38). En vertu de la loi de protection des consommateurs, l'envoi de messages de marketing direct par voie électronique sans le consentement préalable du consommateur est aussi considéré comme une pratique déloyale.

La nouvelle loi finlandaise sur la protection de la vie privée dans les communications électroniques, mentionnée ci-dessus remplacera la loi n° 1999/565 sur la protection de la vie privée et la sécurité des données dans les télécommunications.

France – Projet de loi de "opt-in" en cours d'adoption

Le gouvernement français a présenté en janvier 2003 un projet de loi intitulé *Pour la confiance dans l'économie numérique*. En première lecture, l'Assemblée nationale l'a voté le 26 février 2003 et le Sénat le 25 juin 2003 ; le projet de loi est actuellement en deuxième lecture. L'article 12 du projet de loi adopte le régime de "opt-in" pour le courrier électronique destiné aux personnes physiques. Cependant, on continue à débattre du choix entre "opt-in" et "opt-out" en ce qui concerne les personnes morales inscrites au registre du commerce. Néanmoins, l'envoi de courrier électronique à des fins commerciales sans le consentement préalable du destinataire est autorisé si les coordonnées du destinataire ont été recueillies directement auprès de lui, dans le contexte d'une relation commerciale existante. Dans tous les cas, une stricte conformité à la législation française de protection des données est obligatoire et l'expéditeur de messages électroniques commerciaux doit offrir à la personne concernée un moyen clair et aisé de s'opposer à l'utilisation de son adresse électronique.

Le projet de loi exige aussi des expéditeurs une identité et une adresse véridiques et il interdit les informations fausses dans les en-têtes et les messages. Il prévoit que la Commission nationale de l'informatique et des libertés (CNIL) recueille les plaintes des personnes relatives au non-respect de ces dispositions.[90]

Allemagne - Projet de loi de "opt-in" en cours d'adoption

En Allemagne, un projet de loi de "opt-in" est en cours d'adoption, sous la forme d'une modification de la loi sur la concurrence déloyale *(Gesetz gegen unlauteren Wettbewerb §7 UWG)*. Il a pour objet de mettre en œuvre l'article 13 de la Directive de l'Union européenne concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (2002/58/CE du 12 juillet 2002). Aux termes de ce projet de loi – en particulier d'une nouvelle section 7 de la loi sur la concurrence déloyale – l'envoi de messages publicitaires non sollicités par courrier électronique, télécopie ou automates d'appel sans consentement préalable du destinataire constitue une concurrence déloyale. Cette disposition sera applicable aussi bien quand le destinataire est une personne physique que quand c'est une personne morale, protégeant ainsi de la même manière les entreprises et les consommateurs. Une plainte contre le concurrent déloyal peut être déposée par un de ses concurrents, par des associations représentant les intérêts d'entreprises offrant des produits ou services comparables, par les chambres de commerce ainsi que par les organisations de consommateurs. Ils peuvent demander que le concurrent déloyal mette fin à ses pratiques et s'en abstienne à l'avenir. Le cas échéant, les organisations susnommées peuvent aussi demander que les profits réalisés leur soient reversés. Les concurrents lésés par les pratiques déloyales peuvent réclamer des indemnités.

Si une entreprise a acquis une adresse électronique dans le cadre d'une relation commerciale antérieure, cette entreprise a le droit d'utiliser l'adresse pour envoyer des publicités concernant des biens ou services comparables, sauf si le client lui interdit d'utiliser son adresse ("opt-out"). Lors de l'acquisition de l'adresse et chaque fois que l'adresse est utilisée, le consommateur doit être informé qu'il peut à tout moment s'opposer à l'utilisation de son adresse. Toute violation de cette règle constitue aussi une concurrence déloyale.

Avant ce projet de loi, il existait déjà en Allemagne une obligation de type "opt-in". Les appels téléphoniques à des fins commerciales non sollicités sont interdits en vertu de la loi sur la concurrence déloyale. D'après un certain nombre de décisions de justice, cela s'applique aussi aux messages électroniques non sollicités, mais il n'y a encore eu de décision de la cour suprême sur cette question.

Grèce - "Opt-in"

Le "opt-in" est requis pour les messages électroniques, appels téléphoniques et télécopies publicitaires non sollicités.

Hongrie - "Opt-out"

Sans traiter spécifiquement de l'Internet, la législation hongroise prévoit quelques limitations concernant les communications commerciales non sollicitées. Le décret gouvernemental n° 17/1999 (II. 5.) sur la vente à distance stipule que, si le consommateur ne s'y oppose pas explicitement, une entreprise peut utiliser un moyen de télécommunication permettant aux parties de prendre directement contact, mais sans entrer dans le cadre d'une une offre faite par téléphone ou télécopieur. En conséquence, l'utilisation du spam n'est pas admissible si le consommateur s'y oppose explicitement.

D'après la loi sur la publicité, une annonce ne peut être publiée que si sa nature publicitaire est clairement indiquée et séparable du reste de la communication.[91]

Irlande - "Opt-in"

Le décret n° 535 de 2003, "European Communities (Electronic Communications Networks and Services) (Data Protection and Privacy) Regulations", est entré en vigueur le 6 novembre 2003. Les points saillants de cette réglementation sont les suivants :

Droit des abonnés de déterminer, parmi leurs données à caractère personnel, celles qui figureront dans les annuaires d'abonnés mis à la disposition du public.

Obligation d'informer les abonnés, avant qu'ils y soient inclus, sur les usages auxquels sont destinés les annuaires publics et de leur donner des renseignements complets sur la façon dont leurs données à caractère personnel pourront ensuite être utilisées ou consultées.

Possibilité du traitement des données de localisation des mobiles, avec le consentement des abonnés, pour fournir de nouveaux services à valeur ajoutée.

Dispositions en matière de confidentialité étendues à l'utilisation des réseaux de communications électroniques pour stocker des informations ou accéder à des informations stockées dans l'équipement terminal d'un abonné. L'utilisation de cookies (témoins) et autres dispositifs comme les logiciels destinés à espionner l'activité de l'utilisateur est soumis à réglementation et exige le consentement des utilisateurs.

Restrictions touchant le marketing direct non sollicité par téléphone, télécopie, automates d'appel, courrier électronique, messages SMS et MMS. Le spam (originaire de l'Union européenne) envoyé à des abonnés qui sont des personnes physiques sera illégal. Les abonnés professionnels et autres entités auront aussi des droits renforcés concernant la prévention du spam.

Dispositions facilitant la mise à exécution des décisions de la Comreg et du Data Protection Commissioner, avec des pouvoirs d'investigation sur les violations présumées de la réglementation.

Le multipostage à destination des personnes physiques, avec une exception limitée (couvrant les relations client-fournisseur existantes) n'est autorisé qu'avec un consentement préalable. Cette régime de "opt-in" couvre également les mini-messages (SMS) et autres messages électroniques envoyés à tout terminal fixe ou mobile. Aux termes de cette réglementation, les personnes physiques jugées responsables

de la création de spam ou de courrier électronique ou autres messages de texte non sollicités s'exposeraient à des amendes pouvant atteindre 3 000 EUR par message, et peut-être, dans l'avenir, à une peine de prison.

Italie - "Opt-in"

En Italie, le consentement préalable pour l'envoi de communications non sollicitées, y compris par courrier électronique, est obligatoire depuis 1998 en vertu de la section 10 du Décret n° 171/1998, pris en application de la Directive européenne 97/66/CE, ainsi qu'en vertu de la section 10 du Décret n° 185/1999, pris en application de la Directive 97/7/CE concernant la protection des consommateurs en matière de contrats à distance.

Le nouveau Code de protection des données à caractère personnel, qui transpose la Directive 2002/58/CE dans la législation italienne, confirme le régime de "opt-in" déjà établi dans les décrets susmentionnés. En outre, ce nouveau code (en particulier la section 130) régit les communications non sollicitées de manière beaucoup plus détaillée, en couvrant explicitement toutes les sortes de communications non sollicitées (courrier électronique, télécopie, MMS, SMS, etc.) et en instituant des sanctions qui peuvent même être de nature pénale.

Le nouveau code interdit la pratique consistant à envoyer des messages à des fins commerciales ou promotionnelles en déguisant ou en cachant l'identité de l'expéditeur, ou sans adresse valide à laquelle la personne concernée puisse envoyer une demande pour exercer ses droits. La section 130 permet aussi au *Garante per la protezione dei dati personali* (l'autorité italienne chargée de la protection des données à caractère personnel), dans les cas de violation persistante de cette disposition, d'ordonner au fournisseur de service de communications de mettre en œuvre des mesures de filtrage ou autres mesures applicables à l'égard des coordonnées électroniques utilisées pour envoyer les messages. Concernant l'autorégulation, la section 133 permet au *Garante* d'encourager l'adoption d'un code de conduite et de pratique professionnelle régissant le traitement des données à caractère personnel par les fournisseurs de services de communication et d'information assurés au moyen de réseaux de communications électroniques.

Le *Garante* a pris de nombreuses dispositions concernant le spam, bloquant souvent le traitement de données à caractère personnel stockées dans les bases de données d'entreprises qui utilisaient illégalement des adresses électroniques. En outre, le 29 mai 2003, le *Garante* a adopté une mesure générale concernant les messages non sollicités envoyés à des fins de marketing direct, de publicité ou de promotion. Cette disposition réaffirme le principe de "opt-in" en déclarant que les adresses électroniques qui sont affichées sur le Web, dans des groupes de discussions ou dans des répertoires d'abonnés, ne doivent pas servir à envoyer des messages non sollicités, à moins que le destinataire n'ait donné son consentement préalable et n'ait été informé des droits que lui garantit la législation de protection des données. En conséquence, le *Garante* a interdit la poursuite de pratiques illégales de traitement de données visant soit à envoyer des publicités ou à mener des activités de marketing direct, soit à réaliser des sondages ou entretenir des communications commerciales interactives.

Japon - "Opt-out"

En juillet 2002, deux lois régissant le spam sont entrées en vigueur. L'une est la Loi sur la régulation de l'envoi de certains courriers électroniques (loi n° 26 de 2002), qui vise à régir l'envoi de courriels commerciaux non sollicités. Cette loi oblige les expéditeurs de messages électroniques non sollicités à afficher leur nom, leurs coordonnées et, si c'est le cas, à déclarer au début de la ligne indiquant l'objet du message que le message est une publicité qui n'a fait l'objet d'aucun consentement ni demande, de telle sorte que les utilisateurs aient la possibilité de bloquer automatiquement tout le courrier électronique contenant de la publicité non sollicitée. La loi interdit aussi l'envoi de courriels vers des adresses

électroniques générées de manière aléatoire. En outre, la loi interdit aux expéditeurs d'envoyer des courriels à des destinataires qui les ont informés par téléphone ou par courrier électronique qu'ils ne souhaitent pas recevoir des messages de leur part. Le Ministre de la Gestion publique, des Affaires intérieures et des Postes et télécommunications prononce des décisions administratives pour contraindre les expéditeurs en infraction à se conformer à la loi. Si un expéditeur continue à violer la loi après avoir reçu l'avis de décision, il s'expose à une amende de 500 000 JPN (4 180 USD). La loi permet aux opérateurs de télécommunications de refuser le courrier électronique des expéditeurs de spam si celui-ci engendre des problèmes dans leurs réseaux. Le Ministre a prononcé plusieurs décisions administratives depuis l'entrée en vigueur de la loi en juillet 2002.

L'autre loi est une mise à jour de la Loi régissant certaines transactions commerciales de 1976 (loi n° 28 de 2002), qui régit la vente par correspondance et qui a été établie pour protéger les consommateurs des techniques de vente abusives, comme dans le marketing direct. Elle offre aux utilisateurs une possibilité de refus ("opt-out"), en exigeant que les vendeurs de produits ou fournisseurs de services qui font de la publicité par courrier électronique affichent leur nom et leurs coordonnées et, si c'est le cas, déclarent au début de la ligne indiquant l'objet du message que le message est une publicité qui n'a fait l'objet d'aucun consentement ni demande, de telle sorte que les utilisateurs aient la possibilité de bloquer automatiquement tout le courrier électronique contenant de la publicité non sollicitée. La loi les oblige aussi à y joindre des messages informant les destinataires sur la façon dont ils peuvent refuser les publicités futures. Quand le destinataire a ainsi exprimé son refus, il est interdit aux vendeurs de produits ou fournisseurs de services d'envoyer à nouveau des publicités. Le Ministère de l'Economie, du Commerce et de l'Industrie envoie des messages d'avertissement aux vendeurs de produits ou fournisseurs de services présumés en infraction avec la loi (3 700 messages ont été envoyés en 2002) et prononce contre eux des décisions gouvernementales s'ils n'obéissent pas aux messages d'avertissement (deux sociétés ont fait l'objet de telles décisions en octobre 2003). Les infractions à cette nouvelle loi seront punies d'une peine de deux ans de prison maximum ou d'amendes pouvant atteindre 3 millions JPN (24 000 USD).[92]

Corée - "Opt-out"

La Loi sur la promotion de l'information et de la communication, l'utilisation des réseaux et la protection de l'information interdit l'envoi de spam si le destinataire a exprimé explicitement son refus. Elle interdit aussi de passer outre à une demande de refus au moyen d'une manipulation technique. La loi interdit l'envoi aux mineurs de messages tels que des publicités pour adultes par courrier électronique, téléphone, télécopie, etc. Le spam est défini comme l'envoi de toute publicité commerciale par courrier électronique, téléphone, télécopie, etc. à un utilisateur qui l'a expressément refusé, en violation de la loi. La loi exige aussi que l'expéditeur indique expressément l'objet du message et l'essentiel de son contenu, son nom et ses coordonnées, et qu'il offre une possibilité d'exprimer le refus. La loi exige un étiquetage par "ADV" ou "ADLT" dans les en-têtes et une description claire des moyens permettant au destinataire de refuser les messages à l'avenir (nom, numéro de téléphone, etc. pour communiquer facilement le refus). Il est interdit aux expéditeurs d'utiliser des étiquettes non conformes dans les en-têtes.

En outre, le spam généré par un programme informatique ou la collecte d'adresses électroniques par des moyens techniques sont interdits. Il est aussi interdit de partager ou échanger avec d'autres personnes, ou leur vendre ou fournir une liste d'adresses électroniques moissonnées dans des groupes de discussion qui interdisent qu'on enregistre leurs adresses. En outre, la loi stipule que les FAI peuvent refuser de fournir leurs services de transmission d'information si ils sont fondés à craindre, immédiatement ou ultérieurement, de sérieux encombrements résultant de grands afflux de spam. Actuellement, c'est le régime de "opt-out" qui est adopté en Corée. Toutefois, le 19 octobre 2003, le Ministère de l'Information et de la Communication (MIC) de Corée a annoncé qu'il instaurerait un régime de "opt-in" pour le service de téléphonie mobile. Il faudra un certain temps pour modifier la législation existante, si bien que, pour

commencer, le "opt-in" sera mis en œuvre par des accords d'utilisation entre les fournisseurs de services mobiles et les fournisseurs de services d'information avant la fin de 2003. Le MIC interdit aussi l'envoi des messages publicitaires à certaines heures, par exemple entre 21 heures et 8 heures, même si les clients ont accepté d'en recevoir. Le MIC modifiera la législation en la matière au début de l'année prochaine.

Luxembourg – Projet de loi de "opt-in" en cours d'adoption

A l'heure actuelle, il n'existe pas de règles concernant le courrier électronique non sollicité, ni même les télécopies ou les appels téléphoniques. Le gouvernement essaie maintenant d'établir une nouvelle réglementation transposant la Directive vie privée et communications électroniques 2002/58/CE, en proposant par exemple la solution de "opt-in" pour les appels téléphoniques, les télécopies et le courrier électronique non sollicités.

Mexique – "Opt-out"

Le 11 décembre 2003, le Congrès mexicain a approuvé des réformes et ajouts importants à la Loi fédérale pour la protection des consommateurs. Parmi ces modifications, quelques articles ont été introduits pour assurer certains aspects de la protection des données à caractère personnel :

- Article 17 – Les messages commerciaux ou la publicité envoyés aux consommateurs doivent indiquer le nom, l'adresse, le téléphone et, le cas échéant, l'adresse électronique du fournisseur et de l'entreprise qui envoie les publicités pour le compte des fournisseurs.

  Le consommateur a le droit d'informer directement un fournisseur ou une entreprise qui utilise ses données à caractère personnel à des fins de marketing ou de publicité qu'il ne souhaite pas être dérangé à son domicile, à son lieu de travail, à son adresse électronique ni par quelque autre voie par des propositions de biens ou services, et le consommateur peut notifier au fournisseur qu'il ne veut pas recevoir de publicité. De même, le consommateur a le droit d'informer à tout moment les fournisseurs ou entreprises qui utilisent ses données à caractère personnel à des fins de marketing ou de publicité que ses données à caractère personnel ne doivent pas être transmises à des tiers ni partagées avec des tiers, sauf si une autorité judiciaire a ordonné une telle transmission.

- Article 18 - La *Procuraduría* pourra établir, le cas échéant, un registre public des consommateurs qui ne souhaitent pas que leurs données à caractère personnel servent à des fins de marketing ou de publicité. Les consommateurs pourront notifier à la *Procuraduría*, par lettre ou par courrier électronique, leurs demandes d'inscription à ce registre, qui aura lieu gratuitement.

- Article 18*bis* – Il est interdit aux fournisseurs et aux entreprises qui utilisent les données à caractère personnel des consommateurs à des fins de marketing ou de publicité, ainsi qu'à leurs clients, d'utiliser ces informations à des fins différentes du marketing et de la publicité, ainsi que d'envoyer des publicités aux consommateurs qui ont expressément demandé de n'en pas recevoir ou qui se sont inscrits au registre mentionné dans l'article précédent. Les fournisseurs qui font l'objet de la publicité sont co-responsables de la gestion des données à caractère personnel des consommateurs quand la publicité est envoyé par l'intermédiaire de tiers.

Pays-Bas – "Opt-out", mais projet de loi de "opt-in" en cours d'adoption

La Loi sur les télécommunications du 19 octobre 1998 doit être remplacée à la fin de 2003. La nouvelle loi exige le "opt-in" pour les messages électroniques à des fins commerciales et institue un régime de "opt-out souple" dans le cas de l'utilisation de coordonnées recueillies au cours de la vente de produits ou services, pour le courrier électronique commercial. Elle exige aussi dans les messages l'identité et l'adresse véridiques de l'expéditeur et l'offre d'un moyen de refus ("opt-out") ; elle interdit les informations fausses dans les en-têtes et dans les messages.

Nouvelle-Zélande – Pas de réglementation

A l'heure actuelle, la Nouvelle-Zélande n'a pas de législation sur le spam mais des projets de loi sont à l'étude.

Norvège - "Opt-in"

Un régime de "opt-in" pour le courrier électronique et le SMS s'applique en vertu de la section 2b de la Loi de contrôle du marketing qui est entrée en vigueur en mars 2001. Aux termes de cette loi, il est interdit d'effectuer une prospection directe auprès des consommateurs en utilisant des moyens de télécommunication qui permettent une communication individuelle, comme le courrier électronique, les services de messages de texte à destination des téléphones mobiles, la télécopie ou les automates d'appel, sans le consentement préalable du destinataire.

Pologne - "Opt-in"

La Loi du 18 juillet 2002 sur la fourniture de services par des moyens électroniques, qui régit les activités en ligne, notamment sur l'Internet, a pris effet le 10 mars 2003. Aux termes de cette loi, les fournisseurs de services doivent avoir le consentement des acheteurs pour envoyer des informations commerciales non sollicitées au moyen de systèmes de communication électroniques, notamment le courrier électronique et les messages SMS. Les agissements en infraction avec cette règle sont considérés comme des pratiques de concurrence déloyale. Cela s'applique non seulement aux envois en masse d'informations non sollicitées (multipostage), mais aussi aux messages isolés (communications non sollicitées).[93]

Portugal - "Opt-out", mais projet de loi de "opt-in" en cours d'adoption

Il existe un régime de "opt-out" pour le courrier électronique, mais pas d'interdiction sur les appels téléphoniques non sollicités. Un régime de "opt-in" est en vigueur pour la télécopie. Un projet de loi de "opt-in" plus large est en cours d'adoption.

République slovaque – Pas de réglementation

A l'heure actuelle, la République slovaque n'a pas de législation sur le spam.

Espagne - "Opt-in"

Concernant le courrier électronique, les appels téléphoniques ou d'autres communications électroniques (comme le SMS) non sollicités utilisés à des fins de marketing direct, un régime de "opt-in" a été adopté aussi bien pour les personnes physiques que pour les personnes morales. La Loi sur les services pour la société de l'information interdit la distribution de courrier électronique en masse non sollicité et stipule que les transactions sur l'Internet ont la même valeur en justice que les contrats signés sur papier. Cette loi a été adoptée le 27 juin 2002.[94] En novembre 2003, la Loi sur les télécommunications a été adoptée en application de la directive européenne 2002/58/CE. Cette loi, qui modifie la Loi sur les services pour la société de l'information, prévoit une exception au modèle de "opt-in" dans le cas des relations client-fournisseur existantes.

Suède – Évolution de la réglementation concernant l'acceptation préalable de la prospection commerciale non sollicitée

Actuellement, la Loi suédoise relative à la prospection (1995:450) prévoit deux régimes différents applicables à la prospection commerciale non sollicitée : l'acceptation préalable (« *opt-in* ») pour les télécopieurs et les automates d'appel ; et l'acceptation tacite (« *opt-out* ») pour le courrier électronique et d'autres supports de marketing à distance. Toutefois, le 27 novembre 2003, un projet de loi gouvernemental portant amendement à cette législation pour la mettre en conformité avec les dispositions de l'article 13 de la directive 2002/58/CE a été présenté au Parlement. Les auteurs de ce projet proposés étendent le régime d'acceptation préalable aux courriels en intégrant au premier alinéa de la section 13b de la Loi suédoise relative à la prospection une exigence de consentement en cas d'utilisation du courrier électronique pour des opérations de prospection directe auprès de personnes physiques. Une exception dite d'« acceptation préalable allégée » est prévue lorsque préexiste une relation commerciale avec le destinataire, que l'objet de la prospection directe concerne des biens ou des services similaires et que le destinataire bénéficie d'un moyen simple et sans frais de refuser de nouvelles communications par courriel. La règle de « consentement préalable » ne s'appliquera qu'aux destinataires personnes physiques, les personnes morales n'étant pas concernées. L'acception du mot « courriel », ou de l'expression « courrier électronique », est large : elle englobe tout message textuel, vocal, sonore ou graphique transmis via un réseau public de communications électroniques et stockable sur le réseau ou sur le terminal du destinataire jusqu'à ce que ce dernier le relève (courriel, minimessage ou SMS, minimessage multimédia ou MMS, etc.). Le gouvernement propose en outre d'incorporer à la section 13c de la Loi suédoise relative à la prospection une interdiction visant à empêcher les prospections directes dans lesquelles le destinataire, faute d'adresse de retour valide, ne peut signifier le cas échéant qu'il refuse tout autre publipostage. Cette disposition sera, elle, applicable à toutes les sortes de destinataires, qu'ils soient personnes physiques ou morales. Si une prospection contrevenait à cette disposition, il serait possible d'imposer à son auteur une sanction financière pour perturbation du marché.

Le Parlement devrait procéder au vote formel de ce projet début 2004. S'il était entériné, les amendements à la loi sur la prospection entreraient en vigueur le 1er avril 2004.

Suisse - Projet de loi de "opt-in" en cours d'adoption

42. Les règles concernant le spam relevant de l'article 45a de la Loi sur les télécommunications : LTC) et de l'article 3 de la Loi contre la concurrence déloyale, sont en cours d'adoption au Parlement.[95] Elles correspondront essentiellement à la nouvelle législation de l'Union européenne (Directive concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques). Le régime de "opt-in" s'appliquera ainsi au spam dans toutes les formes de

messages (par exemple, téléphone, courrier électronique, télécopie, SMS), envoyé aussi bien aux entreprises qu'aux consommateurs. Les fournisseurs de services de télécommunications seront tenus de combattre le spam. En d'autres mots, si une personne envoie des messages publicitaires soit en masse, soit individuellement, sans le consentement préalable du destinataire, ou bien si ce n'est pas sur la base d'une relation commerciale préexistante avec le destinataire, cette pratique est alors considérée comme déloyale et des poursuites peuvent être engagées en vertu de la Loi contre la concurrence déloyale. La Loi sur les télécommunications oblige tous les fournisseurs de services de télécommunications à employer les moyens appropriés et proportionnés pour s'opposer au spam.

Turquie – Pas de réglementation

A l'heure actuelle, il n'existe pas de réglementation contre le spam. Cependant, des discussions sont en cours entre les administrateurs de systèmes informatiques et les ingénieurs des FAI, ainsi que certains travaux expérimentaux, pour explorer les solutions techniques, par exemple les listes noires de type RBL, etc. pour réduire les effets nuisibles du spam sur le trafic Internet.

Royaume-Uni – "Opt-in"

Quand les adresses de courrier électronique constituent des données à caractère personnel parce qu'elle contiennent le nom d'une personne, tout traitement doit s'effectuer conformément aux exigences du Data Protection Act de 1998. Cela signifie que si une entreprise continue de traiter une adresse électronique contenant des données à caractère personnel afin d'envoyer des messages de prospection non sollicités après que la personne concernée lui a demandé de cesser, cette entreprise viole les dispositions de la Loi en matière de loyauté du traitement de données.

En mars 2003, le ministère britannique du Commerce et de l'Industrie a présenté de nouvelles règles anti-spam, avec un régime de "opt-in". Cette loi a été votée en septembre 2003 et est entrée en vigueur le 11 décembre 2003. Aux termes de cette nouvelle loi, les entreprises doivent obtenir la permission explicite des destinataires de courrier électronique avant d'envoyer leurs offres. La loi permet aux personnes physiques d'intenter des actions en justice contre les entreprises qui envoient par courrier électronique des offres non sollicitées. Elle oblige aussi les sites Web à donner aux consommateurs la possibilité de refuser les cookies (témoins) avant de les placer dans l'ordinateur de l'utilisateur et elle interdit les messages de texte non sollicités à destination des mobiles. L'Information Commissioner aura des pouvoirs accrus pour donner suite aux plaintes. Suivant ces nouvelles règles, le régime de "opt-in" ne s'applique pas aux adresses électroniques des entreprises, ce qui implique que la loi n'impose pas l'obligation de consentement préalable pour la plupart des adresses professionnelles.

Etats-Unis - "Opt-out"

Le 16 décembre 2003, les Etats-Unis ont adopté une loi sur le spam (« CAN-SPAM Act ») qui se caractérise par un régime "opt-out" à partir de 1 janvier 2004. Cette loi interdit les données d'en-tête fausses ou trompeuses et les informations fallacieuses dans la ligne indiquant l'objet du message. Les expéditeurs de courrier électronique commercial non sollicité sont tenus de fournir un mécanisme de refus ("opt-out") et d'obéir aux demandes des destinataires qui notifient leur refus. La législation exige aussi une déclaration claire et visible indiquant que le message est publicitaire. Les expéditeurs doivent inclure une adresse postale véridique dans le courrier électronique et avoir une adresse électronique qui fonctionne. La loi interdit aussi le moissonnage d'adresses électroniques, les attaques de type dictionnaire, et le déguisement de l'origine du message. La législation crée aussi de nouvelles infractions pénales. Par exemple, aux termes de la loi, le fait d'envoyer sciemment des messages électroniques commerciaux non sollicités avec un en-tête substantiellement falsifié est une infraction pénale. Enfin, la loi ordonne à la FTC

d'établir un plan et un calendrier pour la mise en œuvre d'un registre des personnes refusant les messages électroniques non sollicités et de rendre compte au Congrès de tout ce qui concerne l'établissement de ce registre dans un délai de 6 mois à compter de la promulgation de la loi.

ANNEXE II. TABLEAU DU SPAM - PARTIE I

	1. Lois ou décrets sur le spam ?	2. Titre/ date d'effet des lois ou décrets ?	3. Définition / délimitation du spam ?	4. "Opt-in", "opt-out" ou ni l'un ni l'autre ?	5. Exceptions aux régimes "opt-in" ou "opt-out"?	Commentaires?
Australie	Oui – Voté par le Parlement australien le 2 décembre 2003	Spam Bill 2003	Messages électroniques commerciaux non sollicités	"Opt-in"	Organes gouvernementaux, partis politiques, organisations religieuses, œuvres et institutions charitables, institutions éducatives	Cette loi a un délai de mise en conformité de 120 jours ; elle entre en vigueur en avril 2004.
Autriche	Oui	Loi de régulation des télécommunications	Envoi en masse de messages électroniques à des fins commerciales	"Opt-in"		
Belgique	Oui	Loi sur la commerce électronique, 11/3/2003	Courrier électronique commercial non sollicité	"Opt-in"		
Canada	Application de la loi existante	Loi sur la protection des renseignements personnels et les documents électroniques, janvier 2001	Les adresses électroniques sont considérées comme des données à caractère personnel	"Opt-in"		
République tchèque	Application de la loi existante	Loi n° 40/1995 Coll. sur la réglementation de la publicité	Communications commerciales non sollicitées	"Opt-in"		
Danemark	Oui	Loi sur les pratiques de marketing	Courrier électronique non sollicité	"Opt-in"	Relation préexistante	
Finlande	Oui	Loi sur la protection de la vie privée et la sécurité des données dans les télécommunications. 1999/565	Courrier électronique, télécopies, etc., non sollicités	"Opt-in"	Personnes morales	Nouveau projet de loi en cours d'adoption
France	Non, projet de loi de "opt-in" en cours d'adoption	Pour la confiance dans l'économie numérique	Courrier électronique non sollicité	"Opt-in"	Personnes morales inscrites au registre du commerce / Relation préexistante	
Allemagne	Non, application de la loi existante par les tribunaux ; projet de loi de "opt-in" en cours d'adoption	Projet de loi modifiant la Loi sur la concurrence déloyale *(Gesetz gegen unlauteren Wettbewerb §7 UWG)*	Communication commerciale non sollicitée par téléphone, automate d'appel, télécopie ou courrier électronique	"Opt-in"	Dans le cas d'une relation préexistante : "opt-out"	
Grèce	Oui		Messages électroniques, appels téléphoniques et télécopies publicitaires non sollicités	"Opt-in"		

	1. Lois ou décrets sur le spam ?	2. Titre/ date d'effet des lois ou décrets ?	3. Définition / délimitation du spam ?	4. "Opt-in", "opt-out" ou ni l'un ni l'autre ?	5. Exceptions aux régimes "opt-in" ou "opt-out"?	Commentaires?
Hongrie	Oui (décret)	Décret gouvernemental n° 17/1999 (II. 5.) sur la vente à distance	Moyens de télécommunication	"Opt-out"		
Islande						
Irlande	Oui	Décret n° 535 de 2003, "European Communities (Electronic Communications Networks and Services) (Data Protection and Privacy) Regulations, 2003"		"Opt-in"	Relation préexistante	
Italie	Oui (décret)	Décret n° 171 du 13 mai 1998. Le Code de protection des données à caractère personnel (décret législatif n° 196 du 30 juin 2003), qui transpose la Directive 2002/58/CE dans la législation italienne, entrera en vigueur le 1er janvier 2004	Communications non sollicitées à des fins de marketing direct ou pour envoyer des publicités, ou encore pour réaliser des sondages ou entretenir des communications commerciales interactives. Cela inclut l'utilisation d'automates d'appel sans intervention humaine, le courrier électronique, la télécopie, les messages de type MMS ou SMS	"Opt-in"	Relation préexistante	
Japon	Oui	Loi sur la régulation de l'envoi de certains courriers électroniques, juillet 2002 ; Loi régissant certaines transactions commerciales, juillet 2002	Courrier électronique commercial non sollicité	"Opt-out"		
Corée	Oui	Loi sur la promotion de l'information et de la communication, l'utilisation des réseaux et la protection de l'information, juillet 2001	Toute publicité commerciale par des moyens électroniques	"Opt-out"		
Luxembourg	Non, projet de loi de "opt-in" en cours d'adoption					

	1. Lois ou décrets sur le spam ?	2. Titre/ date d'effet des lois ou décrets ?	3. Définition / délimitation du spam ?	4. "Opt-in", "opt-out" ou ni l'un ni l'autre ?	5. Exceptions aux régimes "opt-in" ou "opt-out"?	Commentaires?
Mexique	Il n'y a pas de loi spécifique sur le spam, mais la Loi fédérale pour la protection des consommateurs couvre certains aspects du courrier électronique.	Loi fédérale pour la protection des consommateurs (LFPC) avec les modifications apportées en mai 2000 et celles attendues en janvier 2004.	Pas de définition spécifique dans la LFPC, mais "messages électroniques commerciaux non sollicités" est une définition généralement admise du spam.	Les modifications sont de type "opt-out".		Le Parlement analyse actuellement un projet de texte pour régir la protection des données à caractère personnel.
Pays-Bas	Oui	Loi sur les télécommunications, 19 octobre 1998 (doit être remplacée à la fin de 2003)	Automates d'appel et télécopies Autres appels non sollicités à fins commerciales	"Opt-in" "Opt-out"	Des facultés de "opt-in" et de "opt-out" doivent être offertes aux abonnés des télécommunications (personnes morales aussi bien que personnes physiques)	Après la mise en application de 2002/58/CE : "opt-in" pour les automates d'appel, télécopies ou messages électroniques à des fins commerciales ; "opt-out" quand d'autres moyens sont utilisés ; "opt-out souple" dans le cas de l'utilisation de coordonnées recueillies au cours de la vente de produits ou services, pour le courrier électronique commercial.
Nouvelle-Zélande	Non					Document de travail en préparation qui examinera l'hypothèse de l'introduction d'une législation anti-spam qui pourrait apporter un complément aux mesures législatives prises par l'Union européenne et l'Australie.
Norvège	Oui	Loi de contrôle du marketing, mars 2001	Conduite de relations commerciales en utilisant les moyens de télécommunication	"Opt-in"	Régime "opt-out" en cas de relation commerciale préexistante	
Pologne	Oui	Loi du 18 juillet 2002 sur la fourniture de services par des moyens électroniques	Informations commerciales non sollicitées au moyen de systèmes de communication électroniques (y compris les messages isolés)	"Opt-in"		

	1. Lois ou décrets sur le spam ?	2. Titre/ date d'effet des lois ou décrets ?	3. Définition / délimitation du spam ?	4. "Opt-in", "opt-out" ou ni l'un ni l'autre ?	5. Exceptions aux régimes "opt-in" ou "opt-out"?	Commentaires?
Portugal	Non, projet de loi de "opt-in" en cours d'adoption			Projet de loi de "opt-in" et "opt-out" en cours d'adoption		
République slovaque						
Espagne	Oui	Loi sur les services pour la société de l'information, juin 2002 ; Loi sur les télécommunications, novembre 2003	Communications électroniques non sollicitées	"Opt-in"	Relation préexistante	
Suède	Oui	Loi sur les télécommunications		"Opt-in"		
Suisse	Non, projet de loi de "opt-in" en cours d'adoption	Loi sur les télécommunications, Loi contre la concurrence déloyale	Toutes les formes de messages électroniques	"Opt-in"	Relation préexistante	
Turquie	Non					
Royaume-Uni	Oui - régime de "opt-in" en vigueur depuis le 11 décembre 2003	Privacy and Electronic Communications (EC Directive) Regulations 2003	Les règles s'appliquent au courrier électronique commercial non sollicité, y compris aux messages de texte à destination des téléphones mobiles	"Opt-in"	Exception de type "opt-out" pour les relations client-fournisseur existantes. Les personnes morales ne bénéficient pas des nouvelles règles "opt-in" pour le courrier électronique	Mise en application de la directive européenne "vie privée et communications électroniques" (Directive 2002/58/EC)
Etats-Unis	Oui	CAN SPAM Act, 1er janvier 2004	Courrier électronique commercial non sollicité	"Opt-out"		La loi s'applique à tout "message commercial par courrier électronique" ayant essentiellement pour objet la publicité ou promotion commerciale d'un produit ou service marchand. Cette définition n'inclut pas les "messages de transaction ou de relation."

ANNEXE II. TABLEAU DU SPAM - PARTIE II

	6. Etiquetage obligatoire ?	7. Identité et adresse véridiques obligatoires ?	8. Faculté d'exprimer son refus ("opt-out") dans les messages ?	9. Liste des personnes refusant le publipostage ?	10. Interdiction des informations fausses dans les en-têtes et les messages ?	11. Interdiction de l'utilisation de logiciels facilitant le spam (spamware) ?	Commentaires?
Australie	Non	Oui	Oui	Non	Oui	Oui	Le SPAM Bill 2003, voté par le Parlement australien le 2 décembre 2003, entrera en vigueur en avril 2004
Autriche				Oui (aux termes de la RTR)			
Belgique		Oui	Oui				
Canada							
République tchèque							
Danemark	Non	Oui	Oui	Non	Oui	Non	
Finlande	Oui	Non	Oui	Non	Oui	Non	Nouveau projet de loi en cours d'adoption
France	Non	Oui	Non	Non	Oui	Oui	11. loi du 8 janvier 1978
Allemagne	Non	Oui	Oui	Non	Dans l'en-tête (adresse) : Oui Dans le message : pas de règle spécifique pour le spam	Non	Sous réserve de l'approbation du Parlement
Grèce							
Hongrie							
Islande							
Irlande							
Italie	Non	Oui	Oui	Non	Oui	Oui	
Japon	Oui	Oui	Oui	Non	Oui	Oui	
Corée	Oui	Oui	Oui	Oui	Oui	Oui	
Luxembourg							
Mexique	Non	Oui	Non	Oui	Oui	Non	

	6. Etiquetage obligatoire ?	7. Identité et adresse véridiques obligatoires ?	8. Faculté d'exprimer son refus ("opt-out") dans les messages ?	9. Liste des personnes refusant le publipostage ?	10. Interdiction des informations fausses dans les en-têtes et les messages ?	11. Interdiction de l'utilisation de logiciels facilitant le spam (spamware) ?	Commentaires?
Pays-Bas	Non	Oui	Oui	Non	Oui		Après la mise en application de 2002/58/CE : "opt-in" pour les automates d'appel, télécopies ou messages électroniques à des fins commerciales ; "opt-out" quand d'autres moyens sont utilisés ; "opt-out souple" dans le cas de l'utilisation de coordonnées recueillies au cours de la vente de produits ou services, pour le courrier électronique commercial.
Nouvelle-Zélande							Les responsables publics examinent actuellement la législation existante pour vérifier si certaines de ces options législatives y sont déjà incluses.
Norvège	Oui	Oui	Non	Non	Oui, en relation avec les activités de marketing	Non	
Pologne	Oui	Oui	Non	Non	Oui	Non	
Portugal							
République slovaque							
Espagne						Oui	
Suède							
Suisse	Non	Oui	Oui	Non	Non	Non	
Turquie							

	6. Etiquetage obligatoire ?	7. Identité et adresse véridiques obligatoires ?	8. Faculté d'exprimer son refus ("opt-out") dans les messages ?	9. Liste des personnes refusant le publipostage ?	10. Interdiction des informations fausses dans les en-têtes et les messages ?	11. Interdiction de l'utilisation de logiciels facilitant le spam (spamware) ?	Commentaires?
Royaume-Uni	Oui	Oui	Oui	Ce n'est pas une obligation légale mais des registres de refus ("opt-out") sont requis par les codes de bonne pratique de certains branches professionnelles	Oui	Non	Les réglementations applicables sont celles du commerce électronique de 2002 et de protection de la vie privée de 2003
Etats-Unis	Oui	Oui	Oui	LA FTC doit rendre compte au Congrès en juin 2004 sur de l'établissement d'un tel registre pour le courrier électronique.	Oui	La loi interdit l'utilisation de logiciels pour moissonner des adresses électroniques, générer des attaques de type dictionnaire ou créer automatiquement un grand nombre de comptes de courrier électronique pour faire du spam.	

ANNEXE III. REGLES EN RAPPORT AVEC LE SPAM DANS LA *DIRECTIVE EUROPÉENNE 2002/58/CE DU 12 JUILLET 2002*

Article 2 - Définitions

(h) "courrier électronique" : tout message sous forme de texte, de voix, de son ou d'image envoyé par un réseau public de communications qui peut être stocké dans le réseau ou dans l'équipement terminal du destinataire jusqu'à ce que ce dernier le récupère.

Communications non sollicitées

Article 13.1

L'utilisation de systèmes automatisés d'appel sans intervention humaine (automates d'appel), de télécopieurs ou de courrier électronique à des fins de prospection directe ne peut être autorisée que si elle vise des abonnés ayant donné leur consentement préalable.

Article 13.2

Nonobstant le paragraphe 1, lorsque, dans le respect de la directive 95/46/CE, une personne physique ou morale a, dans le cadre d'une vente d'un produit ou d'un service, obtenu directement de ses clients leurs coordonnées électroniques en vue d'un courrier électronique, ladite personne physique ou morale peut exploiter ces coordonnées électroniques à des fins de prospection directe pour des produits ou services analogues qu'elle-même fournit pour autant que lesdits clients se voient donner clairement et expressément la faculté de s'opposer, sans frais et de manière simple, à une telle exploitation des coordonnées électroniques lorsqu'elles sont recueillies et lors de chaque message, au cas où ils n'auraient pas refusé d'emblée une telle exploitation.

Article 13.3

Les Etats membres prennent les mesures appropriées pour que, sans frais pour l'abonné, les communications non sollicitées par celui-ci et effectuées à des fins de prospection directe, dans les cas autres que ceux visés aux paragraphes 1 et 2 ne soient pas autorisées, soit sans le consentement des abonnés concernés, soit à l'égard des abonnés qui ne souhaitent pas recevoir ces communications, le choix entre ces deux solutions étant régi par la législation nationale.

Article 13.4

Dans tous les cas, il est interdit d'émettre des messages électroniques à des fins de prospection directe en camouflant ou en dissimulant l'identité de l'émetteur au nom duquel la communication est faite, ou sans indiquer d'adresse valable à laquelle le destinataire peut transmettre une demande visant à obtenir que ces communications cessent.

Il existe cependant une exception autorisant la prospection directe dans le cadre d'une relation client-fournisseur existante. Il sera permis aux entreprises d'envoyer des messages commerciaux non sollicités si elles ont obtenu directement du consommateur son adresse électronique dans le cadre d'un achat et à condition que :

- le message électronique non sollicité ne concerne que des produits analogues qu'elle-même fournit ; et
- que le consommateur se voie donner la faculté de s'opposer sans frais et de manière simple.

La Directive ne s'appliquera toutefois qu'à l'envoi de messages en Europe.

ANNEXE IV. ORGANISATIONS ANTI-SPAM

www.irtf.org/charters/asrg.html (Internet Research Task Force - Anti-Spam Research Group)
www.cauce.org/ (Campaign against Unsolicited Commercial E-mail)
www.euro.cauce.org/ (Euro CAUCE)
www.spamcon.org/
www.mail-abuse.org/
http://mail-abuse.org/swat/
http://spam.abuse.net/
www.junkbusters.com/junke-mail.html
www.spamrecycle.com/
www.junke-mail.org/
www.sputum.com/
www.nanae.org/
www.spamsites.org/
www.spamhaus.org/
www.fmp.com/spam_patrol/
www.natsma.com/
http://sims.net/massacre/
www.gssnet.com/antispam/spam_index.htm
www.stop-spam.org/
www.caspam.org/
www.ripe.net/ripe/wg/anti-spam/
www.cauce.org/orgmember/org_list.shtml
www.caube.org.au/ (CAUCE Australia)
http://cauce.ca/ (CAUCE Canada) (anciennement http://cauce-canada.org/)
http://india.cauce.org/ (CAUCE India)
www.spambr.org/ (Brazilian Spam Fighters)
www.antispam.ru/ (site anti-spam russe)
http://nospam.spb.ru/ (russe)
www.aui.es/contraelspam/ (association espagnole des utilisateurs de l'Internet)
www.fabel.dk/ (site danois)
www.spam.org.tr/ (site anti-spam turc)
www.antispam-argentina.8m.net/ (site anti-spam argentin)
www.spamstop.net/ (japonais)
www.cauce.nl/ (néerlandais)
www.ihatespam.biz/ (coréen)
www.iajapan.org/hotline/ (japonais)
www.spamstop.net/ (japonais)
www.nospamware.it/ (italien)
www.uzice.net/yasi/ (Yugoslav Anti-Spam Initiative)

Source : SpamCon Foundation, 2003.

NOTES

1. *Perspectives des communications de l'OCDE, 2003*.

2. Voir « Internet indicators: Hosts, Users and Number of PCs », Union internationale des télécommunications, disponible à l'adresse suivante : www.itu.int/ITU-D/ict/statistics/at_glance/Internet02.pdf.

3. Voir « Population explosion », des services de CyberAtlas, 14 mars 2003, disponible à l'adresse suivante : http://cyberatlas.internet.com/big_picture/geographics/article/0,,5911_151151,00.html

4. Voir « Start-up aims to end spam », de John Markoff, 24 mars 2003, disponible à l'adresse suivante : www.nytimes.com/2003/03/24/technology/24PHIL.html

5. Voir « E-mail marketing: Consumer choices and business opportunities - Discussion paper » , Industrie Canada, Janvier 2003, disponible à l'adresse suivante : http://e-com.ic.gc.ca/english/strat/e-mail_marketing.html

6. Une enquête menée en 2002 auprès de consommateurs par InsightExpress pour Symantec Corp fournit plusieurs données intéressantes :

   - 37 % des personnes interrogées reçoivent plus de 100 courriels spam par semaine, à domicile et sur leur lieu de travail.
   - 63 % reçoivent plus de 50 messages spam par semaine, à domicile et sur leur lieu de travail.
   - 69 % se sont déclarées d'accord ou tout à fait d'accord pour dire que le spam nuit en général aux utilisateurs du courrier électronique. MessageLabs signale une interception de virus tous les 212 courriels en 2002 (contre une sur 380 en 2001) - « Klez » étant le virus le plus répandu en 2002 (5 millions de copies saisies).
   - 77 % de celles qui ont des enfants de moins de 18 ans se disent inquiètes ou très inquiètes de voir leurs enfants lire les messages spam.
   - 38 % ont indiqué que les messages pornographiques et autres contenus inappropriés étaient pour elles les plus préoccupants. Le seul « spam nigérian » s'est répandu dans le monde entier, et MessageLabs prévoit que cette opération rapportera plus de deux milliards de dollars en 2003, devenant ainsi le deuxième secteur d'activité du pays, si les usagers du courrier électronique continuent d'être trompés.
   - 84 % sont d'accord ou tout à fait d'accord pour dire que les messages spam leur font perdre du temps.
   - 36 % ont répondu que la suppression ou le désabonnement aux messages spam leur prend trop de temps.
   - 42 % n'utilisaient pas de filtre spam.
   - 18 % ont signalé que le spam occupe des ressources informatiques et de messagerie électronique limitées.

   Voir « Spam Expected to Outnumber Non-Spam », de Robyn Greenspan et Brian Morrissey, Jupitermedia Corporation, 12 décembre 2002, disponible à l'adresse suivante : http://cyberatlas.internet.com/big_picture/applications/article/ 0,1323,1301_1555831,00.html

7. Groupe Radicati, « Anti-spam Market Trends, 2003-2007 », www.radicati.com/cgi-local/ brochure.pl?pub_id=202&subscr=&back_link=/single_report/, consulté le 8 décembre 2003.

8. Il s'agit de la marque déposée d'un produit américain de « jambon épicé » en boîte. Le terme « spam » est utilisé dans notre contexte à cause d'un sketch des humoristes britanniques Monty Python qui met en

scène un homme et sa femme, attablés dans un restaurant où la serveuse propose du spam avec tous les plats, même si le client n'en veut pas.

9 Voir « Communications commerciales non sollicitées et protection des données », Commission des Communautés européennes, Janvier 2001, disponible à l'adresse suivante : http://europa.eu.int/comm/internal_market/ privacy/docs/studies/spamsum_fr.pdf

10. Voir www.noie.gov.au/publications/NOIE/spam/final_report/SPAMreport.pdf.

11. Cette liste n'est pas exhaustive.

12 . Voir « Survey on the commercial use of e-mail », Association for Interactive Marketing », 2002, disponible à l'adresse suivante : www.interactivehq.org/councils/CRE/valuesurvey.asp

13. Voir « Spam: Can It Be Stopped? », de Vinton Cerf et Orson Swindle, 18 juin 2002, disponible à l'adresse suivante :
www.gip.org/publications/papers/Spam061802.asp

14. Voir « SpamCatcher Attitude Survey », publié le 1er mai 2003 sur le Forum Spam de la FTC par Mailshell.

15. *Wall Street Journal*, 13 novembre 2002.

16. Un rapport de la FTC (États-Unis) montre que les pages web, les groupes de nouvelles et les forums de discussion sont plus vulnérables aux polluposteurs que d'autres sources. Selon le rapport, les enquêteurs ont semé 250 nouvelles adresses électroniques banalisées sur 175 emplacements différents sur l'Internet pour observer quels domaines les polluposteurs jugent les plus fructueux à la collecte d'adresses. Ces emplacements comprenaient des pages web, des groupes de nouvelles, des forums de discussion, des tableaux d'affichage, des annuaires de pages web en ligne, des usagers de messagerie instantanée, des noms de domaine, des CV, et des services de rendez-vous. Dans les six semaines qui ont suivi leur affichage, ces comptes ont reçu 3 349 messages spam. Les enquêteurs ont constaté que :

- 86 % des adresses affichées sur des pages web et des groupes de nouvelles recevaient du spam.
- Les forums de discussion sont des aimants virtuels pour les logiciels de collecte d'adresses.

Voir « E-mail Address Harvesting: How Spammers Reap What You Sow », FTC (États-Unis), novembre 2002, disponible à l'adresse suivante : www.ftc.gov/bcp/conline/pubs/alerts/spamalrt.htm

17. Selon Spamhouse, les polluposteurs ont mené pendant cinq mois une attaque dictionnaire massive contre les serveurs de messagerie de Hotmail et de MSN pour s'emparer des adresses électroniques de millions d'abonnés à ces deux sociétés. Spamhouse recommande aux usagers de FAI d'utiliser un nom d'usager long, contenant des caractères aléatoires, pour éviter que leur adresse ne soit aspirée par les polluposteurs. Voir « spammers grab MSN Hotmail addresses », Spamhouse, 5 janvier 2003, disponible à l'adresse suivante :
www.spamhaus.org/news.lasso?-database=sbl_news&-layout=detail&-response=newsstory.lasso&-recordID=13&-search

18. Il existe deux sortes de services de messagerie en nombre sur le marché. Les sociétés qui hébergent les campagnes de spam offrent toute la gamme de services nécessaires à l'organisation d'une telle campagne, tandis que les courtiers d'adresse fournissent de nombreuses listes ou adresses électroniques. En réponse aux anti-polluposteurs, ces courtiers proposent aussi le retrait de listes de « opt-in » contenant l'adresse de militants anti-spam connus, ainsi que des domaines .gov, .mil et .edu.

Voir p. 33, « Communications commerciales non sollicitées et protection des données », Serge Gauthronet, Etienne Drouard, Commission des Communautés européennes, Janvier 2001, disponible à l'adresse suivante : http://europa.eu.int/comm/internal_market/ privacy/docs/studies/spamsum_fr.pdf

19. Voir www.spamhaus.org/sbl/sbl-rationale.html

20. Voir www.spamhaus.org/sbl/sbl-rationale.html

21. Voir « Spam Wars », de Melissa Solomon, Computerworld Inc., 11 novembre 2002, disponible à l'adresse suivante : http://computerworld.com/softwaretopics/software/groupware/story/0,10801,75737,00.html

22. Le texte des lignes directrices volontaires est disponible à l'adresse suivante : www.wirelessadassociation.org.

23. Voir « Net users want law to can spam », de Stefanie Olsen, Oaxaca Lending Library, 3 janvier 2003, disponible à l'adresse suivante : www.oaxlib.org/spamcost.html

24. Commission des Communautés européennes, « Communications commerciales non sollicitées et protection des données », Résumé des conclusions de l'étude – Janvier 2001 Serge Gauthronet et Etienne Drouard.

25. Voir p. 66-67, « Communications commerciales non sollicitées et protection des données », Serge Gauthronet, Etienne Drouard, Commission des Communautés européennes, janvier 2001, disponible à l'adresse suivante : http://europa.eu.int/comm/internal_market/privacy/docs/studies/spamsum_fr.pdf

L'extrait ci-dessous montre comment les coûts sont calculés dans ce rapport :

« En partant de l'idée qu'un internaute moyen, disposant d'un abonnement forfaitaire de 12 € pour 10 heures de connexion par mois (communications téléphoniques comprises) et d'un équipement standard (hors Internet rapide), parvient à charger environ 180 Ko à la minute, on obtient un coût qui peut représenter dans le pire des cas jusqu'à 30 € par an pour le chargement d'une petite quinzaine de messages quotidiens représentant entre 500 et 800 Ko au total. Cela revient à une dépense globale très significative si l'on raisonne à l'échelle du parc utilisateur de toute une nation. Au plan mondial et en se projetant dans l'avenir, sur une base de 400 millions d'internautes, le chargement de messages publicitaires dans le contexte technologique actuel donnerait une dépense globale que l'on peut situer au bas mot autour de € 10 milliards pour les seuls coûts supportés par les internautes. »

26. Voir « Spam Expected to Outnumber Non-Spam », de Robyn Greenspan et Brian Morrissey, Jupitermedia Corporation, 12 décembre 2002, disponible à l'adresse suivante : http://cyberatlas.internet.com/big_picture/applications/ article/0,1323,1301_1555831,00.html

27. Voir p. 7, « The state of spam – impact & solutions », Brightmail, janvier 2003, disponible à l'adresse suivante : www.brightmail.com/press-vpk.html

28. Groupe Radicati, « Anti-spam Market Trends, 2003-2007 », www.radicati.com/cgi-local/brochure.pl?pub_id=202&subscr=&back_link=/single_report/, consulté le 8 décembre 2003.

29. Voir « Spam Cost Corporate America $9B in 2002 » de Brian Morrissey, Jupitermedia Corporation, 7 janvier 2003, disponible à l'adresse suivante : http://cyberatlas.internet.com/big_picture/applications/article/0,,1301_1565721,00.html

30. Voir « Spam's Cost To Business Escalates », Jonathan Krim, Washington Post, 13 mars 2003, disponible à l'adresse suivante : www.washingtonpost.com/wp-dyn/articles/A17754-2003Mar12.html?referrer=e-mail

31. Voir p. 11, « The spam problem and how it can be countered – an interim report by NOIE », The National Office for the Information Economy, Australie, 1er août 2002.

32. Voir p. 7, « The state of spam – impact & solutions », Brightmail, janvier 2003, disponible à l'adresse suivante : www.brightmail.com/press-vpk.html

33. Voir « How to Can Spam », de Randolph H. Court et Robert D. Atkinson, 1er novembre 1999, disponible à l'adresse suivante : www.ppionline.org/ndol/print.cfm?contentid=1349

34. Voir « False Claims in Spam », Division of Marketing Practices de la FTC, 30 avril 2003.

35. Il ressort des réponses des fédérations de FAI européennes qu'aujourd'hui encore, plus de 40 % des serveurs de messagerie en exploitation en Europe ont une fonction de relais et sont donc incapables d'empêcher le spam d'être relayé à toutes les adresses électroniques qu'ils gèrent.

Voir. 98, « Communications commerciales non sollicitées et protection des données », Serge Gauthronet, Etienne Drouard, Commission des Communautés européennes, janvier 2001, disponible à l'adresse suivante : http://europa.eu.int/comm/internal_market/privacy/docs/studies/spamsum_fr.pdf

36. Voir Brian D. Westby, FTC V., FTC, File N° 032 3030, soumis le 15 avril 2003, www.ftc.gov/opa/2003/04/westby.htm, consulté le 19 janvier 2004.

37. En janvier 2003, Brightmail a évalué à 5 % les messages spam qui étaient des escroqueries, d'après la définition suivante : « attaques par courrier électronique reconnues comme étant frauduleuses, intentionnellement trompeuses, ou connues pour conduire à une activité frauduleuse de la part de l'expéditeur ». Une lettre d'une personne prétendant être un citoyen nigérian invite le destinataire à envoyer une certaine somme pour l'aider à libérer un compte bancaire de plusieurs millions de dollars. Cette escroquerie paraîtra ridicule à certains, mais elle rencontre un tel succès qu'elle continue de circuler au travers de millions de boîtes aux lettres..

38. www.secretservice.gov/alert419.shtml

39. En mars 2003, des messages demandaient aux abonnés de PayPal, usagers du service de paiement en ligne d'eBay, de communiquer des données bancaires et de cartes de crédit. Ces messages frauduleux, simulant des messages authentiques d'eBay et de PayPal, affichaient le logo de PayPal, des liens à son site et des clauses apparemment officielles en petits caractères qui avaient l'air particulièrement convaincantes. Les messages disaient aux destinataires que leur compte PayPal avait été sélectionné au hasard aux fins de maintenance et mis en état « d'accès limité ». Ce message, qui semblait provenir de l'adresse info@paypal.com, priait le détenteur du compte d'inscrire les numéros de sa carte de crédit et de son compte bancaire sur un formulaire en ligne intégré au courriel. Les polluposteurs ont été arrêtés et condamnés à des peines de prison pour ne pas avoir livré le produit promis.

40. Selon le livre blanc de Brightmail co. paru en 2003, 18 % du spam consiste aujourd'hui en messages à caractère pornographique. Des femmes nues pratiquant le sexe oral, une arme contre la tête ; des femmes nues, de gros chiens accrochés à leurs dos, des femmes nues déguisées en petites filles, portant des couettes, qui feignent d'avoir des rapports sexuels avec leur père. Ce sont là quelques-unes des images explicites qui ont commencé à s'introduire dans les boîtes aux lettres ces derniers temps, les polluposteurs essayant d'orienter le trafic sur les sites de plus en plus nombreux qui affichent différentes pratiques pornographiques : viol, bestialité, inceste.

41. Voir p. 6, « The state of spam – impact and solutions », janvier 2003, Brightmail, Livre blanc, Document Version 1.0. www.brightmail.com/press-vpk.html

42 Voir « Sobig may be working for spammers », pcworld.com, 29 août 2003, disponible à l'adresse suivante : www.pcworld.com/news/article/0,aid,112261,00.asp

43. Selon la FTC américaine, un défendeur utilisait en novembre 2002 des messages spam trompeurs, notamment par l'utilisation non autorisée de logos d'institutions financières réputées dont Radian Bank, Prudential et Fannie Mae, pour inciter ses victimes à divulguer des renseignements financiers délicats, comme leurs revenus, le solde de leurs prêts hypothécaires, la valeur de leur domicile,. Les polluposteurs prétendaient offrir aux consommateurs des prêts de financement et de refinancement compétitifs. Les défendeurs auraient aussi falsifié les en-têtes des courriels (une technique connue sous le nom de « spoofing », ou « usurpation d'adresse IP »), de sorte que les messages qui ne pouvaient être livrés allaient à des adresses électroniques qui ne leur étaient pas apparentées.

Voir « Federal, State, and Local Law Enforcers Tackle Deceptive Spam and Internet Scams », Federal Trade Commission, 13 novembre 2002, disponible à l'adresse suivante : www.ftc.gov/opa/2002/11/netforce.htm

44. Les lignes directrices sont disponibles à l'adresse suivante : www.oecd.org/dataoecd/5/34/1824782.pdf.

45. Par exemple, les autorités australiennes ont appliqué les lois civiles et pénales pertinentes suivantes pour prévenir ou sanctionner l'envoi de communications électroniques en Australie :

- Manquement aux principes nationaux de protection de la vie privée contenus dans la loi sur la vie privée (Privacy Act).
- Violation des interdictions relatives à la promotion du contenu réservé aux adultes sur les sites web ou à la plupart des formes de jeux d'argent interactifs.

- Non-respect des dispositions sur le commerce loyal, la lutte contre la fraude et la protection des investisseurs contenues dans la loi sur les pratiques commerciales (*Trade Practices Act*) et la loi sur les sociétés (*Corporations Law*).
- Violation de la loi sur la cybercriminalité par le biais du piratage et éventuellement de l'usurpation d'adresses IP.

46. Les adresses électroniques qui ne comportent pas le nom d'un individu ne peuvent être assimilées à des informations personnelles aux termes de la loi sur la vie privée, et ne sont donc pas couvertes par ses dispositions. Dans ce cas, l'adoption d'une nouvelle loi ou l'amendement de la loi apparentée en vigueur peuvent être envisagés.

47. Quelques organismes, comme la GEMA, s'inquiètent de ce type de réglementation à cause des menaces de mort qu'elles ont reçues. Selon la GEMA, bon nombre de ses membres sont de petites entreprises et travaillent à domicile ; dans ce cas, la divulgation de leur adresse les mettrait en danger, ainsi que leur famille. Elle estime donc que l'intention législative peut être satisfaite si le distributeur mentionne soit son adresse, soit son numéro de téléphone. Voir « "Statement of Marie Monroe, President of GEMA », communiqué de presse sur le forum spam de la FTC, mai 2003.

48. La Global E-mail Marketing Association (GEMA) s'inquiète des pratiques commerciales trompeuses et déloyales et recommande qu'une instance de réglementation comme la FTC surveille le marché pour vérifier que les FAI n'exploitent pas leur position de force sur le marché pour éliminer les concurrents dans l'environnement du marketing électronique.

49. La GEMA soutient que les robots Internet, des programmes logiciels utilisés pour recueillir les adresses électroniques affichées sur les sites web publics, ne doivent pas être interdits comme le propose la législation en vigueur. Elle estime qu'ils n'ont rien de pernicieux et qu'ils n'entraînent pas le piratage d'ordinateurs ou de bases de données. Voir « Statement of Marie Monroe, President of GEMA », communiqué de presse sur le forum spam de la FTC, 2 mai 2003.

Par ailleurs, la Direct Marketing Association (DMA) s'oppose à la collecte subreptice d'adresses électroniques et aux « attaques de dictionnaire ». Elle estime que ces deux pratiques constituent des abus du droit d'envoyer légitimement des courriels et pourrait, à terme, porter préjudice à l'utilité du courriel en tant qu'outil de communication commerciale. Voir « The DMA opposes surreptitious harvesting and 'dictionary attacks' of e-mail addresses » publié par la DMA sur le Forum spam de la FTC, 30 avril 2003.

50. Les États membres devaient transposer les nouvelles règles dans la législation nationale avant le 31 octobre 2003. La Commission européenne a engagé des procédures d'infraction contre plusieurs États membres qui n'ont pas notifié ces mesures de transposition.

51. Voir par exemple la *Directive 2000/31/CE du 8 juin 2000 sur le commerce électronique* qui comporte des dispositions relatives à la transparence dans le cadre du marketing électronique, et exigent notamment que les communications commerciales soient identifiables en tant que telles.

52. Voir « Internet and Bulk Unsolicited Electronic Mail (SPAM) Policy », Industrie Canada, juillet 1999, disponible à l'adresse suivante : http://e-com.ic.gc.ca/english/strat/spam.html#Consumer.

53 . La FTC a invité les consommateurs à faire suivre les messages spam à une adresse spéciale (uce@ftc.gov) et a établi une base de données sur le spam qui sert de source d'informations aux enquêteurs. En mai 2002, les consommateurs faisaient suivre leur message à la FTC au rythme d'environ 105 000 courriels par jour.

54. Voir « False Claims in Spam », Division of Marketing Practices de la FTC, 30 avril 2003.

55. Voir « 2003 Consumer Spam Study », ePrivacy Group, juillet 2003, disponible à l'adresse suivante : www.eprivacygroup.net/ spamstudy

56. Spamhaus(//spamhouse.org) suit à la trace les polluposteurs les plus nocifs de l'Internet, les gangs de polluposteurs et les services d'appui au spam connus, et travaille en collaboration avec les FAI et les organismes d'application de la loi pour identifier et éliminer les polluposteurs persistants du réseau. La société fournit gratuitement à ses abonnés « "The Spamhaus Block List (SBL) », une base de données en temps réel, basée sur le DNS, d'adresses IP de polluposteurs, gangs et services de spam confirmés.

57. CAUCE participe activement à la soumission de projets de loi visant à limiter ou à interdire les messages électroniques commerciaux non sollicités. Euro-CAUCE a lancé une pétition contre le spam qui doit être adressée aux membres du Parlement européen et des parlements nationaux.

58. Voir www.tacd.org

59. Aux États-Unis, les FAI ont organisé un réseau d'administrateurs volontaires connus sous le nom de *The Mail Abuse Prevention System* qui exploite la *Realtime Blackhole List* (RBL). Cette liste est un instrument de boycott de masse utilisé par les administrateurs de systèmes des FAI pour mettre à l'index les adresses IP et les noms de domaines des polluposteurs. Voir « Communications commerciales non sollicitées et protection des données », Serge Gauthronet, Etienne Drouard, Commission des Communautés européennes, janvier 2001, disponible à l'adresse suivante : http://europa.eu.int/comm/internal_market/en/dataprot/studies/spamstudyen.pdf

60. Par exemple, dans son Acceptable Usage Policy (AUP), « *Telstra BigPond Direct* », le plus important fournisseur de réseau principal en Australie, énonce clairement que le pollupostage est inacceptable et qu'il mettra fin au service des abonnés qui recourent à cette pratique.

Conditions d'utilisation de Telstra Bigpond concernant le spam :

2.1 Vous ne devez pas:

- Utiliser telstra.com pour envoyer des messages électroniques non sollicités à qui que ce soit.
- Effectuer des enquêtes, des réservations ou des demandes frauduleuses ou spéculatives par l'intermédiaire de telstra.com.
- Utiliser sans permission le nom, le nom d'utilisateur ou le mot de passe d'un autre abonné.
- Envoyer, ou transmettre, par l'intermédiaire de telstra.com, de documents obscènes, indécents, outrageux ou pornographiques, ou des document qui pourraient entraîner des poursuites au civil ou au pénal.
- Gêner ou empêcher le fonctionnement de telstra.com ou lui apporter des modifications non autorisées.
- Transmettre en toute connaissance de cause des virus ou autres programmes nocifs à telstra.com.

61. Voir « Internet and Bulk Unsolicited Electronic Mail (SPAM) Policy », Industrie Canada, juillet 1999, disponible à l'adresse suivante : http://e-com.ic.gc.ca/english/strat/spam.html#Consumer

62. Voir « Internet and Bulk Unsolicited Electronic Mail (SPAM) Policy », Industrie Canada, juillet 1999, disponible à l'adresse suivante : http://e-com.ic.gc.ca/english/strat/spam.html#Consumer

Voir « The spam problem and how it can be countered – an interim report by NOIE », The National Office for the Information Economy, Australie, 1er août 2002.

En Australie, la section 10 du code de déontologie de l'Internet Industry Association (cinquième version) énonce les restrictions suivantes au spam :

- Les membres de l'IIA et les abonnés au code ne doivent ni pratiquer le pollupostage, ni l'encourager, sauf exceptions dans le cas de relations préexistantes.
- Les membres de l'IIA et les abonnés au code qui pratiquent le pollupostage envers leurs connaissances doivent donner aux destinataires le moyen de le refuser, et doivent fournir des instructions à cet égard dans le message spam.
- Les membres de l'IIA et les abonnés au code ne doivent envoyer à personne, pas même à leurs connaissances, du spam dont le contenu est interdit.

- Les prestataires de services Internet des membres de l'IIA et des abonnés au code doivent avoir une politique d'utilisation acceptable qui interdit le spam ainsi que les services qui dépendent du spam.
- Les FAI devraient mettre en place une adresse de contact permettant le dépôt de plaintes sur le spam, autrement dit une adresse électronique de type « abuse@ ».

- Les FAI devraient installer des systèmes anti-relais sur leurs serveurs de messagerie électronique pour empêcher les polluposteurs d'utiliser le relais pour éviter toute détection ou sanction.

63. Dans le cadre du système d'affranchissement en ligne, les expéditeurs de messages commerciaux en nombre qui souhaitent envoyer plus de 1 000 courriels par jour doivent payer l'expédition et enregistrer au préalable leur nom réel auprès de Daum, faute de quoi Daum bloquera leurs messages. Dans le cas où les destinataires du message répondent par voie de vote que celui-ci n'est pas commercial mais qu'il contient des informations utiles, Daum rembourse l'expéditeur, si celui-ci a déjà payé, sur une base différentielle selon le ratio d'information préétabli dans son barème de remboursement (système de points de récompense de Daum). Bien entendu, Daum vend les timbres en ligne et administre les expéditeurs inscrits en ligne, ou sur son site web. La société a également mis en place un « indice de réclamations relatives au spam » qui comporte quatre niveaux : « bon », « attention », « avertissement », « restriction ». Les FAI inscrits au niveau « restriction » sont ceux qui ont reçu le plus grand nombre de réclamations, et ils risquent de voir leurs envois en masse limités.

    Selon un sondage réalisé par Daum auprès du public en 2002, 76,6% des personnes interrogées estimaient que le spam avait diminué après l'instauration du système d'affranchissement en ligne, 23,4 % jugeaient que rien n'avait changé, et 83,5 % se déclaraient en faveur du système. Bien que les expéditeurs aient demandé aux abonnés à Daum de transférer leur adresse électronique à d'autres prestataires de services de messagerie électronique, 88,4 % des personnes ont déclaré qu'elles continueraient de faire essentiellement appel aux services de Daum. On trouvera des précisions sur le système d'affranchissement en ligne de Daum aux adresses suivantes : http://onlinestamp.daum.net/intro.jsp, http://onlinestamp.daum.net/focus/focus2.jsp

64. Voir www.iia.net.au/nospam.

65. « Les États membres prennent des mesures visant à garantir que les prestataires qui envoient par courrier électronique des communications commerciales non sollicitées consultent régulièrement les registres « opt-out » dans lesquels les personnes physiques qui ne souhaitent pas recevoir ce type de communications peuvent s'inscrire, et respectent le souhait de ces dernières. »

66. p. 91, « Communications commerciales non sollicitées et protection des données », Serge Gauthronet, Etienne Drouard, Commission des Communautés européennes, janvier 2001, disponible à l'adresse suivante : http://europa.eu.int/comm/internal_market/privacy/docs/studies/spamsum_fr.pdf

67. Voir http://preference.the-dma.org/products/empssubscription.shtml

68. Voir www.tpsonline.org.uk/.

69. Voir « Direct Marketing Association's Online Marketing Guidelines and Do the Right Thing Commentary », janvier 2002, disponible à l'adresse suivante : www.the-dma.org/guidelines/onlineguidelines.shtml#2

70. Aux termes de ce code, les consommateurs sollicités doivent avoir la possibilité de refuser toute communication ultérieure du distributeur. Un distributeur qui ne respecte pas le code est radié de l'Association.

71. Voir www.networkadvertising.org

72. Le CDT a proposé aux usagers quelques méthodes pour cacher leur adresse aux polluposteurs :

    - Déguiser les messages envoyés à un espace public ou ne pas afficher leur adresse électronique dans les annuaires publics.
    - Veiller tout particulièrement à cocher les cases demandant le droit de diffuser leur adresse électronique.
    - Utiliser plusieurs adresses électroniques.
    - Utiliser un filtre.
    - Ne pas utiliser une adresse électronique courte.

[73]. En cours de développement par le groupe ePrivacy. Contient des timbres de confiance, clairement visibles dans la partie supérieure droite du message, qui permettent aux destinataires de vérifier, en temps réel, l'authenticité de l'expéditeur, l'intégrité du message et la conformité de l'expéditeur aux principes de protection des données à caractère privé et aux pratiques exemplaires en matière de messagerie électronique fondées sur le consensus des entreprises du secteur et des défenseurs de ces principes.

74. Voir www.ecommerce.treasury.gov.au

75. Voir www.msn.co.uk/spambuster

76. Voir p. 2-3, « Trusted E-mail Open Standard », Livre blanc du groupe ePrivacy, mai 2003..

77. Voir « Spam Wars », de Melissa Solomon, Computerworld Inc., 11 novembre 2002, disponible à l'adresse suivante : http://computerworld.com/softwaretopics/software/groupware/story/0,10801,75737,00.html

78. L'une de ces solutions est le « Trusted E-mail Open Standard », proposé par le groupe ePrivacy sur le Forum spam de la FTC le 2 mai 2003 ; ce dispositif permet aux expéditeurs d'un courriel de présenter dans l'en-tête du message des informations vérifiables quant à leur identité et au contenu du message. Cette proposition a reçu le soutien de CAUCE, de la SpamCon Foundation et de CAUCE Canada. Les participants au forum de la FTC (distributeurs, FAI, défenseurs des consommateurs et entreprises de technologie) ont convenu qu'un effort consensuel s'imposait pour déployer des outils grâce auxquels les expéditeurs pourront intégrer des données plus vérifiables à leurs messages. Un *Trusted E-mail Oversight Board* a été proposé pour créer des programmes qui certifieront les messages électroniques en fonction d'un ensemble de normes que les participants à ces programmes accepteront de respecter. Voir « Trusted E-mail Open Standard », Livre blanc du groupe ePrivacy, mai 2003, et http://eprivacygroup.net/toes

79. Les logiciels d'analyse heuristique recherchent les identités de message non valables, les bogues et autres caractéristiques des messages spam, et établissent une notation numérique pour chaque message entrant. Si cette notation atteint une limite prédéfinie, le courriel est bloqué.

80. Voir « First industry-wide antispam conference shows promise », de David Berlind, Oaxaca Lending Library, 27 février 2003, disponible à l'adresse suivante : www.oaxlib.org/v-37.html

81. Voir www.irtf.org/charters/asrg.html.

82. Voir http://www.isipp.com/news.html, et http://www.internetnews.com/IAR/article.php/3-78481

83. Au Royaume-Uni, un membre du Parlement a appelé en février 2003 le gouvernement à repenser le système de filtrage qui avait pour but de protéger les boîtes aux lettres des parlementaires de tout message spam ou pornographique, mais qui avait également paralysé des débats ordinaires sur le projet de loi relatif à la criminalité sexuelle. Voir « MPs call for anti-spam rethink », BBC News, 10 février 2003, disponible à l'adresse suivante : http://news.bbc.co.uk/2/hi/technology/2737221.stm

84. Une enquête de AC Nielsen consult portant sur les FAI australiens a constaté qu'un seul des cinq principaux FAI filtrait le spam avant que ses serveurs ne fassent suivre les messages aux abonnés. L'un des quatre autres a dit encourager activement ses clients à employer des filtres (fournis par le FAI à prix réduit). Parmi les plus petits FAI australiens, la plupart employaient des filtres avant de faire suivre le courrier, mais beaucoup ne filtraient pas tous les spams.

Voir p. 23, « The spam problem and how it can be countered – an interim report by NOIE" », The National Office for the Information Economy, Australie, 1er août 2002.

NOTES DE L'ANNEXE I

85. Voir p. 80, "Communications commerciales non sollicitées et protection des données", Serge Gauthronet, Etienne Drouard, Commission des Communautés européennes, janvier 2001, disponible à http://europa.eu.int/comm/internal_market/privacy/docs/studies/spamstudy_fr.pdf .

86. Voir Annex 3, "Overview of implementation in the Member States" du "Eighth report from the commission on the implementation of the telecommunications regulatory package", European telecoms regulation and markets 2002, 3 décembre 2003, disponible

à http://europa.eu.int/information_society/topics/telecoms/implementation/annual_report/8threport/index_en.htm

87. Voir "L'internet et le courrier électronique en vrac non sollicité (MULTIPOSTAGE)", Industrie Canada, juillet 1999, disponible à http://e-com.ic.gc.ca/francais/strat/multipostage.html

88. Voir "L'internet et le courrier électronique en vrac non sollicité (MULTIPOSTAGE)", Industrie Canada, juillet 1999, disponible à http://e-com.ic.gc.ca/francais/strat/multipostage.html

89. Par exemple, le gouvernement essaie d'adapter la réglementation de l'envoi de communications non sollicitées (spamming) prévue par l'article 7 de la Directive (identification de l'expéditeur par le destinataire, mise en place de registres des personnes qui refusent le spam, et obligation pour l'expéditeur de consulter ces registres) étant donné que la loi n° 40/1995 Coll. sur la réglementation de la publicité est trop générale sur cette question (elle ne prévoit pas de sanctions) et, en même temps, sa formulation est trop restrictive.

90. En outre, le projet de loi appelle aussi les hébergeurs de sites Internet à exercer un "minimum de surveillance" sur les pages qu'ils stockent, pour empêcher la diffusion de messages ou d'images racistes, pédophiles ou faisant l'apologie de crimes contre l'humanité. Le commerce électronique serait aussi soumis à des règles plus strictes, une "responsabilité globale" étant imposée aux marchands en ligne.

91. Voir "Overview of Electronic Commerce", Judit Budai, International Law Office Internet Publication, septembre 2000, disponible à www.szecskay.hu/publikaciok/jbuy010.pdf

92. Voir "The Future of the wireless spam", Duke law and technology review, 28.10.2002, disponible à www.law.duke.edu/journals/dltr/articles/2002dltr0021.html. .

93. Voir "Spam Slammed", The Warsaw Voice news, 13 mars 2003, disponible à www.warsawvoice.pl/view/1593

94. Les opposants à la nouvelle loi espagnole sur le commerce électronique, qui impose aux fournisseurs d'accès Internet (FAI) d'exercer une surveillance sur les utilisateurs, veulent la contester devant les tribunaux au motif qu'elle viole les droits constitutionnels. Source : "Spain's New E-Commerce Law Worries Privacy Advocates", Jerome Socolovsky, Associated Press, 28/6/02.

95. Voir l'article 45a et l'annexe (*Modification du droit en vigueur*) du *"Projet de loi sur les télécommunications"*, disponible à www.bakom.ch/imperia/md/content/francais/telecomdienste/principesetconsultations/consultations/ProjetdeloiLTC.pdf

Voir aussi les commentaires dans les paragraphes 2.1.7 (Art. 45a de la LTC), 2.2.1 (Art. 3 de la LCD) du *"Message relatif à la modification de la loi sur les télécommunications"*, disponible à www.bakom.ch/imperia/md/content/francais/telecomdienste/principesetconsultations/consultations/MessageLTC.pdf